LECTURE NOTES FOR 428

CHARLES REZK

1. Solving the quadratic

Everyone here knows how to solve \( aX^2 + bX + c = 0 \).

- If \( a = 0 \), it’s not actually a quadratic, and you know what to do.
- If \( a \neq 0 \), then its the same to divide out by \( a \) and solve the monic quadratic

\[
X^2 + \frac{b}{a}X + \frac{c}{a} = 0.
\]

- Then “complete the square” in the LHS:

\[
X^2 + \frac{b}{a}X + \frac{c}{a} = X^2 + \frac{b^2}{4a^2} - \frac{b^2}{4a^2} + \frac{c}{a} = \left( X + \frac{b}{2a} \right)^2 - \left( \frac{b^2}{4a^2} - \frac{c}{a} \right).
\]

- Set equal to 0 to get

\[
\left( X + \frac{b}{2a} \right)^2 = \frac{b^2 - 4ac}{4a^2},
\]

- then take square-root to get:

\[
X + \frac{b}{2a} = \pm \frac{\sqrt{b^2 - 4ac}}{2a} \implies X = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.
\]

Notably, there can be up to two roots. If \( a, b, c \in \mathbb{R} \), then real roots exist iff \( b^2 - 4ac \geq 0 \); if not, the roots are complex. When \( a, b, c \in \mathbb{C} \) there are always roots, since every complex number has a square root.

Not that there is a “repeated root” if and only if the “discriminant” \( \Delta := b^2 - 4ac = 0 \). That is, a factorization of the form

\[
aX^2 + bX + c = a(X - \gamma)^2 = aX^2 - 2a\gamma X + a\gamma^2
\]

exists iff \( b = -2a\gamma \) and \( c = a\gamma^2 \), i.e., iff

\[
\gamma = -\frac{b}{2a} \quad \text{and} \quad b^2 = 4ac.
\]

2. Solving the cubic: Cardano’s method

Let \( aX^3 + bX^2 + cX + d = 0 \) be a general cubic equation. I’m eventually going to want to consider \( a, b, c, d \in \mathbb{C} \) being arbitrary complex numbers, but right now you should think of the case of real coefficients, which is what Cardano was interested in solving.

Remark. We know that every cubic with real coefficients has at least one real root, by the Intermediate Value Theorem. Let \( f(X) = aX^3 + bX^2 + cX + d \), and suppose \( a > 0 \). Then when \( |X| \gg 0 \) is large the \( X^3 \) term dominates, so \( f(N) > 0 \) for \( N > 0 \) and \( f(M) < 0 \) for some \( M < 0 \). Since \( f \) is continuous, the IVT says that \( f \) restricted to \([M, N]\) outputs every value in \([f(M), f(N)]\), so in particular there exists \( C \in [M, N] \) such that \( f(C) = 0 \).

Date: December 10, 2019.
Since \( a \neq 0 \), you can divide through by \( a \) to get a monic cubic, of the form \( X^3 + bX^2 + cX + d = 0 \). So without loss of generality we can assume the polynomial is monic.

We can attempt to “complete the cube” by setting \( X = Y - \frac{b}{3} \), obtaining

\[
X^3 + bX^2 + cX + d = (Y - \frac{b}{3})^3 + b(Y - \frac{b}{3})^2 + c(Y - \frac{b}{3}) + d
= \cdots
= Y^3 + pY + q.
\]

Exercise. Show that \( p = -\frac{b^2 + 3c}{3} \) and \( q = \frac{2b^3 - 9bc + 27d}{27} \).

This operation is called a Tschirnhaus transformation. A cubic of the form \( Y^3 + pY + q = 0 \) is called a depressed cubic. To solve a general cubic, it suffices to solve the associated depressed cubic: if \( \alpha \) is a root of the depressed cubic, then \( \alpha - \frac{b}{3} \) is a root of the original cubic.

So without loss of generality we need to solve a cubic of the form

\[
X^3 + pX + q = 0.
\]

Cardano’s method involves two arbitrary looking “guesses”.

Guess #1: Assume that roots have the form

\[
X = u^{1/3} + v^{1/3},
\]

i.e., they are always a sum of two cube roots.

We plug this guess back into the equation. First, note that

\[
X^3 = (u^{1/3} + v^{1/3})^3
= (u^{1/3})^3 + 3(u^{1/3})^2v^{1/3} + 3u^{1/3}(v^{1/3})^2 + (v^{1/3})^3
= u + v + 3u^{1/3}v^{1/3}(u^{1/3} + v^{1/3})
= u + v + 3u^{1/3}v^{1/3}X.
\]

Therefore

\[
X^3 + pX + q = u + v + 3u^{1/3}v^{1/3}X + pX + q
= (u + v + q) + (3u^{1/3}v^{1/3} + p)X,
\]

i.e., the root of the original depressed cubic must also satisfy the equation

\[
0 = (u + v + q) + (3u^{1/3}v^{1/3} + p)X.
\]

Guess #2: The coefficients of the above equation are zero, so \( u + v + q = 0 \) and \( 3u^{1/3}v^{1/3} + p = 0 \).

Remark. Guess #1 is innocuous: any number can be written as a sum of two cube roots. (In fact, given \( X \in \mathbb{C} \) we could set \( u = X^3 \) and \( v = 0 \). However, the solutions that Cardano’s method gives do not typically have this form.)

Guess #2 is surprising. When you make a random guess like this, it is usually likely that it will fail: in fact, there might not exist any actual solution which is compatible with the guess. It will work out in this case, but it’s not immediately obvious why.

Assuming our guesses are good, we need to solve the system of equations

\[
u + v = -q,
\]

\[
u^{1/3}v^{1/3} = -\frac{p}{3}.
\]

\(^1\)Sigh.
for $u^{1/3}$ and $v^{1/3}$. We first try to solve for $u$ and $v$, which solve the system

$$u + v = -q,$$
$$uv = -\frac{p^3}{27}.$$

In fact, $u$ and $v$ are solutions of the associated quadratic

$$0 = (Z - u)(Z - v) = Z^2 - (u + v)Z + uv = Z^2 + qZ - \frac{p^3}{27}.$$  

We get (up to possibly switching $u$ with $v$):

$$u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \quad v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$  

Therefore we should have a root

$$X = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$  

**Example.** Consider

$$X^3 - 3X + 4 = 0,$$

so $p = -3$ and $q = 4$. Then $\sqrt{\frac{q^2}{4} + \frac{p^3}{27}} = \sqrt{\frac{16}{4} - \frac{27}{27}} = \sqrt{3}$, so we get

$$X = \sqrt[3]{-2 + \sqrt{3}} + \sqrt[3]{-2 - \sqrt{3}} \approx -2.1958.$$  

Check that this is really a root.

**Example.** Consider

$$X^3 - 3X - 18 = 0,$$

so $p = -3$ and $q = -18$. Then $\sqrt{\frac{q^2}{4} + \frac{p^3}{27}} = \sqrt{\frac{16}{4} - \frac{27}{27}} = \sqrt{80}$, so we get

$$X = \sqrt[3]{9 + \sqrt{80}} + \sqrt[3]{9 - \sqrt{80}} \approx 3.0000.$$  

Check that this is really a root. What is a little surprising is that it is actually equal to 3.

The reason for this is that $9 \pm \sqrt{80}$ have cube roots which themselves can be written in terms of square roots of integers:

$$\left(\frac{3}{2} + \frac{\sqrt{5}}{2}\right)^3 = 9 + \sqrt{80}, \quad \left(\frac{3}{2} - \frac{\sqrt{5}}{2}\right)^3 = 9 - \sqrt{80},$$

so $X = (\frac{3}{2} + \frac{\sqrt{5}}{2}) + (\frac{3}{2} - \frac{\sqrt{5}}{2}) = 3$.

In the previous examples, $p, q \in \mathbb{R}$ and $\frac{q^2}{4} + \frac{p^3}{27} > 0$, so everything is real. What if $\frac{q^2}{p} + \frac{p^3}{27} < 0$?

**Example.** Consider

$$X^3 - 15X - 4 = 0,$$

so $p = -15$ and $q = -4$. Then $\sqrt{\frac{q^2}{4} + \frac{p^3}{27}} = \sqrt{\frac{16}{4} - \frac{3375}{27}} = \sqrt{-121}$, so we get

$$X = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}.$$  

In fact, $X = 4$ is a root, as you can check directly. To get this from Cardano’s formula, use

$$(2 + \sqrt{-1})^3 = 2 + \sqrt{-121}, \quad (2 - \sqrt{-1})^3 = 2 - \sqrt{-121},$$

so $X = (2 + \sqrt{-1}) + (2 - \sqrt{-1}) = 4.$
It was examples like the previous one which lead to the “invention” of complex numbers: to solve for a real root of the cubic using Cardano’s method, intermediate results may be complex.

With complex numbers in hand, let’s think about what is going on a little more carefully. Remember that a (non-zero) number has three distinct complex roots. If $U$ is any one cube root of $u$, then the three cube roots are

$$ U, \omega U, \omega^2 U, $$

where $\omega = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$, since $\omega^3 = 1$. So if we pick cube roots $U = u^{1/3}$ and $V = v^{1/3}$, then we get nine possible answers:

$$ U + V \omega U + V \omega^2 U + V $$

$$ U + \omega V \omega U + \omega V \omega^2 U + \omega V $$

$$ U + \omega^2 V \omega U + \omega^2 V \omega^2 U + \omega^2 V $$

which is too many. However, recall the equations that $u$ and $v$ must satisfy:

$$ u + v = -q, $$

$$ u^{1/3} v^{1/3} = -p/3. $$

The second equation tells how to compute $v^{1/3}$ from $u^{1/3}$. Thus if we set $V = -\frac{p}{3U}$, we only have three solutions:

$$ U + V = U - \frac{p}{3U}, \quad \omega U + \omega^2 V = \omega U - \frac{p}{3\omega U}, \quad \omega^2 U + \omega V = \omega^2 U - \frac{p}{3\omega^2 U}. $$

**Example.** Consider $X^3 - 3X - 18 = 0$ again. Take $U = \sqrt[3]{9 + \sqrt{80}}$, the real cube root of $9 + \sqrt{80}$, so $V = \sqrt[3]{9 - \sqrt{80}}$ is also a real cube root since then $UV = 1 = -p/3$. The three solutions of the polynomial are thus

$$ U + V = 3, \quad \omega U + \omega^2 V, \quad \omega^2 U + \omega V. $$

The other two are non-real, and are complex conjugate to each other. Using that $U = \frac{3}{2} + \frac{\sqrt{15}}{2}$ and $V = \frac{3}{2} - \frac{\sqrt{15}}{2}$, we can solve for all three roots:

$$ 3, \quad -\frac{3}{2} + \frac{\sqrt{15}}{2} i, \quad -\frac{3}{2} - \frac{\sqrt{15}}{2} i. $$

**Example.** Consider $X^3 - 15X - 4 = 0$ again. Using the cube root $U = \sqrt[3]{2 + 11i} = 2 + i$, we must have $V = 2 - i$, so we can solve for all three roots:

$$ 4, \quad -2 - \sqrt{3}, \quad -2 + \sqrt{3}. $$

**Example.** Consider $X^3 - 3X + 4 = 0$ again. Using the real cube root $U = \sqrt[3]{-2 + \sqrt{3}}$, we must have $V = \sqrt[3]{-2 - \sqrt{3}}$ so that $UV = 1 = -3/p$. We get three roots:

$$ \sqrt[3]{-2 + \sqrt{3}} + \sqrt[3]{-2 - \sqrt{3}} \quad \omega\sqrt[3]{-2 + \sqrt{3}} + \omega^2 \sqrt[3]{-2 - \sqrt{3}} \quad \omega^2 \sqrt[3]{-2 + \sqrt{3}} + \omega \sqrt[3]{-2 - \sqrt{3}}. $$

Only the first one is real.

**Exercise.** The polynomial $X^3 - X = 0$ has roots $-1, 0, 1$. Solve it using Cardano’s method.

### 3. Solving the cubic: Lagrange resolvents

Let’s go back and see if we can explain why Cardano’s method worked. In summary, Cardano’s method says the the roots of $X^3 + pX + q = 0$ are

$$ \alpha_1 = U + V, $$

$$ \alpha_2 = \omega^2 U + \omega V, $$

$$ \alpha_3 = \omega U + \omega^2 V, $$

**W 28 Aug**
where \( \omega = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i \), and \( U \) and \( V \) are solutions to the system of equations

\[
U^3 + V^3 = -q,
UV = -p/3.
\]

The method is to solve for \( U^3 \) as a root of the auxiliary quadratic equation \((Y - U^3)(Y - V^3) = Y^2 + qY - p^3/27 = 0\), take a cube root to get \( U \), then set \( V = -p/3U \).

In this set up, if you know \( U \) and \( V \), then you know the roots \( \alpha_1, \alpha_2, \alpha_3 \), by the formulas above. But it goes the other way. Notice that, in addition to \( \omega^3 = 1 \), the number \( \omega \) satisfies

\[
\omega^2 + \omega + 1 = 0.
\]

Using this, we can turn it around:

\[
0 = \frac{1}{3}(\alpha_1 + \alpha_2 + \alpha_3),
U = \frac{1}{3}(\alpha_1 + \omega \alpha_2 + \omega^2 \alpha_3),
V = \frac{1}{3}(\alpha_1 + \omega^2 \alpha_2 + \omega \alpha_3).
\]

Thus, the roots determine \( U \) and \( V \) as well. The \( U \) and \( V \) are called **Lagrange resolvents**. Lagrange realized that finding the roots is exactly the same as finding \( U \) and \( V \).

Recall that if we plug in \( \alpha_1 = U + V \) for \( Y \) in the original depressed cubic \( Y^3 + pY + q = 0 \), we could rewrite it as

\[
0 = (U^3 + V^3 + q) + (3UV + p)\alpha_1.
\]

In fact, the same is true for \( \alpha_2 \) and \( \alpha_3 \): all three roots are solutions of the linear equation

\[
0 = (U^3 + V^3 + q) + (3UV + p)X.
\]

One way this can happen is if \( \alpha_1 = \alpha_2 = \alpha_3 \), which implies all three roots are 0 (and so \( p = q = 0 \)). The only other way it can happen is if the equation is itself trivial, i.e., if \( 3UV + p = 0 \) and \( U^3 + V^3 + q = 0 \). This validates “Guess #2” in the description of Cardano’s method I gave last time: the Lagrange resolvents, which we can define in terms of the three roots of the cubic, must satisfy Cardano’s equations \( U^3 + V^3 = -q \) and \( UV = -p/3 \). Thus we have proved that the method works.

Recall that the labelling of the roots as \( \alpha_1, \alpha_2, \alpha_3 \) is arbitrary: it should make no difference if we permute the roots by some element \( \sigma \in S_3 \) of the symmetric group on \( \{1, 2, 3\} \), i.e.,

\[
\alpha_k \mapsto \alpha_{\sigma(k)}.
\]

Such relabellings would change the definitions of \( U \) and \( V \) as well. We can compute how this would work, as shown in the following chart.

<table>
<thead>
<tr>
<th>e</th>
<th>( \alpha_1 )</th>
<th>( \alpha_2 )</th>
<th>( \alpha_3 )</th>
<th>( U )</th>
<th>( V )</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2 3)</td>
<td>( \alpha_1 )</td>
<td>( \alpha_2 )</td>
<td>( \alpha_3 )</td>
<td>( V )</td>
<td>( \bar{U} )</td>
</tr>
<tr>
<td>(1 2)</td>
<td>( \alpha_2 )</td>
<td>( \alpha_1 )</td>
<td>( \alpha_3 )</td>
<td>( \omega V )</td>
<td>( \omega^2 U )</td>
</tr>
<tr>
<td>(1 3)</td>
<td>( \alpha_3 )</td>
<td>( \alpha_2 )</td>
<td>( \alpha_1 )</td>
<td>( \omega^2 V )</td>
<td>( \omega U )</td>
</tr>
<tr>
<td>(1 2 3)</td>
<td>( \alpha_2 )</td>
<td>( \alpha_3 )</td>
<td>( \alpha_1 )</td>
<td>( \omega U )</td>
<td>( \omega^2 V )</td>
</tr>
<tr>
<td>(1 3 2)</td>
<td>( \alpha_3 )</td>
<td>( \alpha_1 )</td>
<td>( \alpha_2 )</td>
<td>( \omega U )</td>
<td>( \omega^2 V )</td>
</tr>
</tbody>
</table>

In particular, the quantities \( U^3 + V^3 \) and \( UV \) would not be changed by any of the relabellings. Thus, they only depend on the unordered set of the three roots, and so we would expect that we could compute \( U^3 + V^3 \) and \( UV \) just from knowing the original cubic. This is in fact the case.
4. Solving equations by radicals

A similar approach works for equations of degree 4, and reduces the problem of solving the quartic to solving an associated cubic.

I’ll briefly sketch the idea as a series of exercises. Given a depressed quartic
\[ X^4 + pX^2 + qX + r = 0 \]
with roots \( \alpha_1, \alpha_2, \alpha_3, \alpha_4 \), we define the following “Lagrange resolvents”:
\[
0 = \frac{1}{4}(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4), \\
L_1 = \frac{1}{4}(\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4), \\
L_2 = \frac{1}{4}(\alpha_1 - \alpha_2 + \alpha_3 - \alpha_4), \\
L_3 = \frac{1}{4}(\alpha_1 - \alpha_2 - \alpha_3 + \alpha_4).
\]
The matrix is invertible: you can write formulas for the \( \alpha \)s in terms of the \( L \)s:
\[
\alpha_1 = L_1 + L_2 + L_3, \\
\alpha_2 = L_1 - L_2 - L_3, \\
\alpha_3 = -L_1 + L_2 - L_3, \\
\alpha_4 = -L_1 - L_2 + L_3.
\]

Now consider how the \( L \)s transform under permutations \( \alpha_k \mapsto \alpha_{\sigma(k)} \) where \( \sigma \in S_4 \).

**Exercise.** Show that the quantities \( L_1L_2L_3, L_1^2 + L_2^2 + L_3^2, \) and \( L_1^2L_2^2 + L_2^2L_3^2 + L_3^2L_1^2 \) are invariant under all relabellings of the roots.

Thus, we expect that these quantities can be computed directly from the coefficients of the quartic.

**Exercise.** Show that:
\[
L_1^2 + L_2^2 + L_3^2 = -8p, \\
L_1^2L_2^2 + L_2^2L_3^2 + L_3^2L_1^2 = 16(p^2 - 4r), \\
L_1L_2L_3 = -8q.
\]

Hint: by expanding the quartic as \( (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)(X - \alpha_4) \), write \( p, q, r \) as symmetric polynomials in the \( \alpha \)s.

Now you can form the associated cubic
\[
(Y - L_1^2)(Y - L_2^2)(Y - L_3^2) = Y^3 - (L_1^2 + L_2^2 + L_3^2)Y^2 + (L_1^2L_2^2 + L_2^2L_3^2 + L_3^2L_1^2)Y - L_1^2L_2^2L_3^2 \\
= Y^3 + 8pY^2 + 16(p^2 - 4r)Y - 64q^2.
\]

Solve this to find two roots \( L_1^2 \) and \( L_2^2 \), take square roots of each to get \( L_1 \) and \( L_2 \), use \( L_1L_2L_3 = -8q \) to get \( L_3 \), and from these produce roots of the quartic.

In general one may ask:
Can every polynomial of degree \( n \) (with real or complex coefficients) be solved by radicals: that is, can the roots be written in terms of the coefficients using only the operations of \( +, -, \times, \div, \sqrt[\cdot] \) (which may be iterated).

This comes in two forms:
**Strong form:** Is there a “formula” which calculates the roots of the polynomial in terms of the above operations applied to the coefficients, which works for every polynomial of degree \( n \)?

**Weak form:** For a particular polynomial of degree \( n \), when is it possible to express the roots in terms of the coefficients using only the above operations?
The answers are:

**Strong form:** NO iff \( n \geq 5 \) (Abel-Ruffini, Galois).

**Weak form:** YES exactly when the Galois group of the polynomial is “solvable”. There are explicit methods for determining the Galois group of any particular polynomial (though they may be hard to use) (Galois).

We will prove all of this in the course.

5. Rings and fields

Some basic terminology.

A **ring** is data \((R, +, \cdot, 0, 1)\) where \(+, \cdot : R \times R \to R\) and \(0, 1 \in R\), such that

- \((R, +, 0)\) is an abelian group with operation + and unit 0,
- \((R, \cdot, 1)\) is a monoid with operation \(\cdot\) and unit 1, and
- the distributive law holds: \(a(b + c) = ab + ac\) and \((a + b)c = ac + bc\) for all \(a, b, c \in R\).

As usual, we write \(R\) instead of \((R, +, \cdot, 0, 1)\).

Example: \(R = \mathbb{M}_{n \times n}(F)\) with \(F = \mathbb{R}\) or \(F = \mathbb{C}\), with the usual matrix operations, \(0 = \) zero matrix, \(1 = \) identity matrix.

Some remarks.

- Because \((R, +, 0)\) is an abelian group, there are additive inverses of \(a \in R\), which we write as \(-a\).
- Note that \((R, \cdot, 1)\) is only a monoid: multiplication is associative and has a unit, but is not assumed to be commutative or to have multiplicative inverses.

A **commutative ring** is one where multiplication is commutative: \(ab = ba\) for all \(a, b \in R\).

Almost all rings in the course will be commutative.

A **domain** is a commutative ring with the property that (i) \(1 \neq 0\), and (ii) \(ab = 0\) implies \(a = 0\) or \(b = 0\).

Example: the integers \(\mathbb{Z}\) is a domain, but \(\mathbb{Z} \times \mathbb{Z}\) is not. The polynomial ring \(\mathbb{R}[X]\) is a domain as we will see.

A **field** is a commutative ring with the property that (i) \(1 \neq 0\), and (ii) every non-zero element has a multiplicative inverse.

Example: \(\mathbb{Q}\), \(\mathbb{R}\), \(\mathbb{C}\).

Example: for \(n > 0\), the set \(\mathbb{Z}/n\) of integers modulo \(n\) is a commutative ring. It is a domain iff \(n\) is prime, in which case it is actually a field.

6. Polynomials

For any commutative ring \(R\), the **polynomial ring**

\[
R[X] := \{ a_0 + a_1 X + \cdots + a_r X^r \mid a_0, \ldots, a_r \in R, \ r \geq 0 \}
\]

is also a commutative ring. We think of this as “formal expressions in powers of \(X\) with coefficients in \(R\)”. Very explicitly, we can define elements \(f \in R[X]\) to be sequences \(\{f_k \in R\}_{k \geq 0}\) such that \(f_k = 0\) for all sufficiently large \(k\), with operations defined by

- \((f + g)_k = f_k + g_k\),
- \((fg)_k = \sum_{i=0}^{k} f_i g_{k-i}\),
- \(0_k = 0\),
- \(1_k = 0\) if \(k \neq 1\), \(1_0 = 1\), i.e., \(1 = (1, 0, 0, 0, 0, \ldots)\).

In practice we identify elements \(a \in R\) with sequences \((a, 0, 0, \ldots)\), and set \(X = (0, 1, 0, 0, \ldots)\), in which case we can write any polynomial as an expression as above.

Any polynomial \(f \in R[X]\) gives a function \(c \mapsto f(c)\) on \(R\), defined in the obvious way.
Warning: It is possible that two different polynomials can give the same function \( R \rightarrow R \). However, it turns that this does not happen if \( R \) is any infinite field, as we will see.

Example: Let \( F = \mathbb{Z}/2 \) and \( f = X^2 - X \) in \( F[X] \). Then \( f(0) = 0 \) and \( f(1) = 1 \), so the function defined by \( f \) is a constant function.

Example: we can form polynomial rings in several variables, by setting \( R[X,Y] := (R[X])[Y] \).

We have a **degree** function

\[
\deg: R[X] \to \{\infty\} \cup \mathbb{Z}_{\geq 0}
\]

(Stewart writes \( \partial \) instead of \( \deg \)) so that for \( f = \sum a_k X^k \),

\[
\deg(f) = \sup \{ k \in \mathbb{Z}_{\geq 0} \mid a_k \neq 0 \}.
\]

Thus \( \deg(f) = -\infty \) iff all \( a_k = 0 \), i.e., iff \( f = 0 \).

**Exercise.** Check that

1. \( \deg(f + g) \leq \max(\deg f, \deg g) \),
2. \( \deg(fg) \leq \deg(f) + \deg(g) \), and we can replace “\( \leq \)” with “\( = \)” if \( R \) is a domain.

**Proposition.** If \( R \) is a domain, so is \( R[X] \).

**Proof.** Immediate from properties of the degree function: \( -\infty = \deg(fg) = \deg(f)\deg(g) \) implies either \( \deg(f) = -\infty \) or \( \deg(g) = -\infty \). \( \square \)

In particular, \( F[X] \) is a domain when \( F \) is a field.

7. **Division algorithm**

The division algorithm for polynomials over a field is crucial.

**Proposition (Division algorithm).** Let \( F \) be a field. Let \( f, g \in F[X] \) with \( g \neq 0 \). Then there exist unique \( q, r \in F[X] \) such that

1. \( f = qg + r \),
2. \( \deg r < \deg g \).

**Proof.** Uniqueness is easy: if \( f = qg + r = q'g + r' \), then \( (q - q')g = r - r' \) and so \( \deg(q - q') + \deg g = \deg(r - r') < \deg g \), which since \( g \neq 0 \) can only happen if \( \deg(q - q') = -\infty \), i.e., if \( q - q' = 0 \).

Existence is proved by the usual “polynomial long division” argument: you can always carry out this algorithm when \( g \neq 0 \), which produces \( f/g = q + r/g \). \( \square \)

For polynomials \( f \) over a field \( F \), a **root** of \( f \) in \( F \) is a \( c \in F \) such that \( f(c) = 0 \).

**Corollary.** Let \( F \) be a field. For \( f \in F[X] \) and \( c \in F \), we have that \( f(c) = 0 \) iff \( f = (X - c)g \) for some \( g \in F[X] \).

**Proof.** Division algorithm applied to \( f \div (X - c) \) gives \( f = (X - c)q + r \) with \( r \in F \), and plugging in \( X = c \) gives \( 0 = f(c) = r(c) = r \). \( \square \)

**Corollary.** If \( f \in F[X] \) with \( f \neq 0 \) and \( \deg f = n \), then \( f \) has at most \( n \) distinct roots in \( F \).

**Proof.** By induction on \( n \). Given \( f \in F[X] \) with \( \deg f = n \), if \( f \) has no roots, we are done. If \( c \) is a root of \( f \), then \( f = (X - c)g \) for some \( g \in F[X] \) which must have \( \deg g = n - 1 \). By induction \( g \) has \( k \) roots with \( k \leq n - 1 \), so \( f \) has at most \( k + 1 \) roots. \( \square \)
8. Divisibility of polynomials

A unit in a ring \( R \) is an element which has a multiplicative inverse in \( R \). I write \( R^\times \subseteq R \) for the set of units. By definition, \( R^\times \) is a group under multiplication, and is commutative if \( R \) is a commutative ring.

If \( F \) is a field, then \( F^\times = F \setminus \{0\} \).

Example: \( \mathbb{Z}^\times = \{\pm 1\} \).

Example: \((\mathbb{Z}/n)^\times\) is also called \( \Phi(n) \). It is the set of congruence classes \([a]\) modulo \( n \) such that \( \gcd(a,n) = 1 \).

Given elements \( f, g \in R \) in a commutative ring, we say that \( g \) divides \( f \) if there exists \( h \in R \) such that \( f = gh \). (I prefer to say that \( f \) is a multiple of \( g \)). The standard notation is \( g \mid f \).

Remark: The relation “\( | \)” on \( R \) satisfies (i) \( f \mid f \) and (ii) \( f \mid g \) and \( g \mid h \) imply \( f \mid h \). Such a relation is called a preorder on \( R \).

The notion of divisibility is most useful in a domain, such as \( F[X] \).

**Lemma.** If \( R \) is a domain and \( f, g \in R \), and \( f \mid g \) and \( g \mid f \), then \( g = uf \) for some \( u \in R^\times \).

**Proof.** If \( f = 0 \), then \( f \mid g \) implies \( g = 0 \), so clearly \( g = uf \) for any unit \( u \). Likewise if \( g = 0 \).

Suppose \( f, g \in R \setminus \{0\} \). If \( f = ug \) and \( g = vf \), then \( f = uvf \), so \( 1 = uv \) by cancellation, and \( u, v \in R^\times \).

We say that two elements \( f, g \in R \) in a domain \( R \) are the same up to units if \( g = uf \) for some \( u \in R^\times \). This is an equivalence relation on \( R \). The lemma says that the divisibility defines a partial order on “elements of \( R \) up-to-units”.

Example: The elements up to units in \( \mathbb{Z} \) are \( \{0\}, \{\pm 1\}, \{\pm 2\}, \) etc.

Given \( f, g \in R \), a common divisor or common factor, is a \( d \in R \) such that \( d \mid f \) and \( d \mid g \). A greatest common divisor or highest common factor is a common divisor \( d \) such that for any other common divisor \( d′ \), we have that \( d′ \mid d \).

**Lemma.** In a domain \( R \), if elements \( f, g \) have a gcd, it is unique up-to-units.

Existence of gcds is non-trivial, and they can fail to exist in general. However, they do always exist in \( R = F[X] \), polynomials over a field \( F \).

**Proposition.** Let \( f, g \in F[X] \) with \( F \) a field. There exist \( a, b \in F[X] \) such that \( d := af + bg \) is a common divisor of \( f, g \), and this element is in fact a gcd of \( f \) and \( g \).

**Proof.** If \( f = g = 0 \) then \( d = 0 \) is a gcd. So suppose at least one of \( f, g \) is non-zero.

Let \( I = \{af + bg \mid a, b \in F[X]\} \), and note that this set contains non-zero elements. Choose \( d \in I \setminus \{0\} \) with minimal degree \( m \). I claim that \( d = af + bg \) divides every element of \( I \). Let \( e = a′f + b′g \in I \). By the division algorithm for \( e \div d \) we have \( q, r \in F[X] \) with \( \deg r < m \) and

\[
e = qd + r,
\]

that is\( a′f + b′g = qa f + qb g + r \), so \( r = (a′ - qa)f + (b′ - qb)g \in I \).

Since \( \deg r < m \) we must have \( r = 0 \), so \( d \mid e \).

Therefore \( d \) is a common divisor of \( f \) and \( g \). If \( e \) is another common divisor of \( f \) and \( g \), then \( e \mid af + bg \), i.e., \( e \mid d \).

In practice, you can compute the gcds of polynomials by the Euclidean algorithm.

Example: \( F = \mathbb{Q} \), \( f = X^3 + 2X^2 - 6X + 3 \), \( g = X^2 + 2X - 3 \). The algorithm proceeds by iteratively computing division with remainder. First compute \( f \div g \):

\[
X^3 + 2X^2 - 6X + 3 = (X)(X^2 + 2X - 3) + (-3X + 3).
\]

Let \( f′ = g \) and \( g′ = \text{remainder} \) and compute \( f′ \div g′ \):

\[
(X^2 + 2X - 3) = (-\frac{1}{3}X - 1)(-3X + 3) + (0).
\]

Once we get the remainder \( = 0 \), the gcd is \( g′ = -3X + 3 \), which up-to-units is \( X - 1 \).
Note: it can be very hard to compute the roots or factor a polynomial. But it is always easy to determine whether two polynomials have a common factor: just use the Euclidean algorithm.

## 9. Irreducibility and Unique Factorization

An element of a domain $R$ is **irreducible** if:

- it is not 0 and not a unit,
- it is not a product of two non-zero non-units.

Example: In $\mathbb{Z}$ the irreducible elements are the $\pm p$ where $p$ is a prime number.

In $R = F[X]$ with $F$ a field, a polynomial $f$ is a non-zero non-unit iff $\deg f \geq 1$. Since $\deg(fg) = \deg f + \deg g$, this means that: a polynomial is irreducible iff it is non-constant and is not a product of two polynomials of smaller degree. (This is the definition used in the book.)

In this case, we also say that $f$ is irreducible over $F$, for the following reason.

Suppose that $F$ is a subfield of a larger field $K$ (i.e., a subset closed under $+$ and $\times$, containing 0 and 1, and with this structure is a field). Then $F[X]$ is a subring of $K[X]$. A polynomial $f \in F[X]$ is also an element of $K[X]$, and can be irreducible over $F$ while reducible over $K$.

Example: $f = X^2 + 1 \in \mathbb{R}[X]$ is irreducible as an element of $\mathbb{R}[X]$, but reducible in $\mathbb{C}[X]$ since $f = (X - i)(X + i)$.

Thus, “irreducible” is always relative to the ground field.

**Proposition.** Let $F$ be a field. Any non-zero non-unit polynomial in $F[X]$ is a product of one or more irreducible polynomials over $F$.

**Proof.** A proof by induction on degree of $f \in F[X]$. If $f$ is irreducible, we are done. If not, $f = gh$ where $\deg g, \deg h < \deg f$, and by induction $g$ and $h$ are products of irreducibles.

The following is often summarized as: “irreducible polynomials are prime”.

**Lemma.** If $f, g, h \in F[X]$ are polynomials, $f$ irreducible, and $f \mid gh$, then either $f \mid g$ or $f \mid h$.

**Proof.** Suppose $f$ is irreducible and $f \mid g$. Let $d$ be a gcd of $f, g$. Necessarily $d \mid f$, so $f = de$ for some $e$. Since $f$ is irreducible, either $d$ or $e$ is a unit. If $e$ is a unit, then $f$ is the same as $d$ up-to-units so $f \mid g$, contradicting the hypothesis. If $d$ is a unit (i.e., $f$ and $g$ are “relatively prime”), then we can say $d = 1$, and then $1 = af + bg$ for some polynomials $a, b$. Then $f$ divides

$$h = (af + bg)h = afh + bgh$$

as desired.

**Proposition.** Any factorization of $f$ in $F[X]$ into a product of irreducibles is unique up to constant factors and the order of the factors.

**Proof.** Suppose $f = p_1 \cdots p_k = q_1 \cdots q_l$, where $p_i, q_j$ are irreducible. By the previous lemma, since $p_k \mid f$, we must have $p_k \mid q_j$ for some $j$, which after reordering the factors we can take to be $j = \ell$. Since $q_\ell$ is also irreducible, $q_\ell = up_\ell$ for some unit $u$. Then since $F[X]$ is a domain, cancelling $p_\ell$ gives $p_1 \cdots p_{k-1} = (up_1)q_2 \cdots q_{\ell-1}$. The proof proceeds by induction on the number of factors.

Example: Consider $f = X^4 + 1 \in \mathbb{Q}[X]$. Over $\mathbb{C}$, this has roots $(\pm 1 \pm i)/\sqrt{2}$, and so factors over $\mathbb{C}$ into irreducibles as:

$$X^4 + 1 = (X - (1 + i)/\sqrt{2})(X - (1 - i)/\sqrt{2})(X - (-1 + i)/\sqrt{2})(X - (-1 - i)/\sqrt{2}).$$

Over $\mathbb{R}$, $f$ is a product of two irreducible quadratics:

$$X^4 + 1 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1).$$

Over $\mathbb{Q}$, $f$ is irreducible. How can you prove this?
(Here’s one way: In general, if \( g \in \mathbb{Q}[X] \) is a factor of \( f \), then unique factorization in \( \mathbb{C}[X] \) implies that \( g \) is up-to-units a product of a subset of the linear factors of \( f \). If \( f \) is not irreducible then it must have an irreducible factor of degree 1 or 2. Thus, we just need to note that none of the four linear factors \((X - (\pm 1 \pm i)/\sqrt{2})\) are in \( \mathbb{Q}[X] \), and also that no product of two of the linear factors are in \( \mathbb{Q}[X] \) (there are 6 products to check).)

10. Algebraic closure and the fundamental theorem of algebra

We say that a field \( F \) is a \textit{algebraically closed} if every \( f : F[X] \) with \( \deg f \geq 1 \) has a root in \( F \).

**Proposition.** If \( F \) is algebraically closed, then every \( f \in F[X] \) with \( \deg f \geq 1 \) can be factored into linear (\( = \text{degree 1} \)) factors.

**Proof.** Proceed by induction on \( \deg f \). If \( c \in F \) is a root, then using the division algorithm we have \( f = (X - c)g \) for some \( g \in F[X] \), and \( \deg g < \deg f \).

**Theorem** (Fundamental theorem of algebra). \( \mathbb{C} \) is algebraically closed.

There are many proofs of this. I’ll sketch the one that Stewart gives. Some other interesting ones can be found at [https://kconrad.math.uconn.edu/blurbs](https://kconrad.math.uconn.edu/blurbs).

Note: this proof uses a special case: \( n \)th roots of complex numbers always exist, i.e., \( X^n - c = 0 \) has a complex root for all \( n \in \mathbb{Z}_{>0} \) and \( c \in \mathbb{C} \). This relies on the fact that we can always write:

\[
c = re^{i\theta} = r(\cos \theta + i \sin \theta), \quad r, \theta \in \mathbb{R}, \ r \geq 0,
\]

and that \((e^{i\theta})^n = e^{i\theta n}\), so \( r^{1/n} e^{i\theta/n} \) is a root.

**Proof.** We write \( f(z) = a_0 + a_1 z + \cdots + a_n z^n \). Assume \( n \geq 1 \) and \( a_n \neq 0 \).

We need to use the fact that as a function, \( f \) is continuous, and therefore so is \( g : \mathbb{C} \to \mathbb{R} \) defined by \( g(x) = |f(x)| \).

The “minimum principle” says: Any continuous function \( g : D \to \mathbb{R} \) on a compact subset \( D \subseteq \mathbb{R}^m \) attains a minimum value at some point \( x_0 \in D \). (Compact=closed and bounded; see any real analysis course.)

We use this to show that \( g(z) = |f(z)| \) attains a minimum value as a function \( \mathbb{C} \to \mathbb{R} \).

First, note that for all \( m > 0 \), there exists \( R > 1 \) such that \( |f(z)| > M \) for all \( |z| > R \). This is because the \( a_n z^n \) term dominates the other terms as \( |z| \) becomes large. More explicitly, we have (using the triangle inequality \( |A + B| \leq |A| + |B| \), which implies \( |A + B| \geq |A| - |B| \)):

\[
|f(z)| = |(a_0 + a_1 z + \cdots + a_{n-1} z^{n-1}) + a_n z^n| \\
\geq |a_n z^n| - |a_0 + a_1 z + \cdots + a_{n-1} z^{n-1}| \\
\geq |a_n z^n| - (|a_0| + |a_1| + \cdots + |a_{n-1}| z^{n-1}) \\
= |z|^n (|a_n| - (|a_0| |z|^{-n} + \cdots + |a_{n-1}| |z|^{-1})).
\]

If \( |z| > 1 \) then \( |z|^{-k} < |z|^{-1} \) for \( k \geq 1 \), so

\[
|f(z)| \geq |z|^n (|a_n| - (|a_0| + \cdots + |a_{n-1}|) |z|^{-1})
\]

So choose \( R \) such that \( R > 1 \) and \( R > |a_n| / (|a_0| + \cdots + |a_{n-1}| + 1) \) and \( R > M^{1/n} \).

Now let \( M = |f(0)| \) and \( R \) such that \( |f(z)| > M \) if \( |z| > R \). Then \( |f(z)| \) must attain its minimum in the closed disk \( \{|z| \leq R\} \), and so by the minimum principle attains its global minimum at some \( z_0 \).

If the minimum value is 0, then \( z_0 \) is a root, so we suppose \( f(z_0) \neq 0 \) and derive a contradiction. Without loss of generality we can assume \( z_0 = 0 \) and \( f(0) = -1 \) (by replacing \( f \) with \(-f(z_0)^{-1}f(z - z_0)\), which is also a polynomial of degree \( n \)).

Then

\[
f(z) = -1 + a_k z^k + \cdots + a_n z^n, \quad 1 \leq k \leq n, \ a_k \neq 0.
\]
In fact, we can assume WLOG that \( a_k = 1 \) (by replacing \( f(z) \) with \( f(b^{-1}z) \), where \( b \) is a kth root of \( a_k \)). Thus we can write
\[
f(z) = -1 + z^k + z^{k+1}g(z), \quad g \in \mathbb{C}[X].
\]
It’s enough to find a \( z \) such that \(|f(z)| < 1\). Note that if \( g = 0 \) (so \( k = n \)), then this is easy: just let \( z \in (0,1) \), so \(|f(z)| = 1 - z^n < 1\).

More generally, assuming \( z \in (0,1) \), we have
\[
|f(z)| \leq \left|-1 + z^k\right| + \left|z^{k+1}g(z)\right| = 1 - z^k + z^{k+1}|g(z)|.
\]
Choose \( M \geq 1 \) and so that it is greater than the max value of \(|g(z)|\) on \([0,1]\). If \( z \in (0,1/M) \) then \( z|g(z)| < 1 \), so \( z^{k+1}|g(z)| < z^k \) and so \( 1 - z^k + z^{k+1}|g(z)| < 1 - z^k + z^k = 1 \) as desired.

\[\square\]

11. Factoring Polynomials over \( \mathbb{R} \)

Over \( \mathbb{C} \) every polynomial is a product of linear factors. We have a similar result over \( \mathbb{R} \) if we also allow quadratic factors.

Let \( f \in \mathbb{R}[X] \) be a real polynomial. If \( c \in \mathbb{R} \) is a real root of \( f \), then we can factor \( f = (X - c)g \), where \( g \in \mathbb{R}[X] \). What about non-real roots?

**Proposition.** If \( \lambda \in \mathbb{C} \setminus \mathbb{R} \) is a non-real root of \( f \in \mathbb{R}[X] \), then there exists a factorization \( f = gh \) over \( \mathbb{R} \) such that \( g \) is irreducible of degree 2 and \( g(\lambda) = 0 \).

**Proof.** Given a non-real root \( \lambda \) of \( f \), note that \( \bar{\lambda} \) is also a non-real root since \( f \) has real coefficients: if \( f \in \mathbb{R}[X] \), then \( f(\lambda) = f(\bar{\lambda}) \).

Set
\[
g = (X - \lambda)(X - \bar{\lambda}) = X^2 + bX + c, \quad b = -\lambda + \bar{\lambda}, c = \lambda\bar{\lambda} \in \mathbb{R}.
\]
Then \( g \) is irreducible over \( \mathbb{R} \), since otherwise it would factor into linear factors over \( \mathbb{R} \) and thus have a real root, but the only roots in \( \mathbb{C} \) are non-real.

By the division algorithm, we have \( f = qg + r \) for some \( q, r \in \mathbb{R}[X] \) with \( \deg r \leq 1 \). Plugging in \( \lambda \) gives
\[
0 = f(\lambda) = q(\lambda)g(\lambda) + r(\lambda) = 0 + r(\lambda).
\]
Since \( r \) is real is we cannot have \( r(\lambda) = 0 \) unless \( r = 0 \), so we have \( f = qg \) a factorization over \( \mathbb{R} \). \[\square\]

**Corollary.** The only irreducible polynomials over \( \mathbb{R} \) are (up-to-units), of the form
\[
X - c, \quad c \in \mathbb{R} \quad \text{or} \quad X^2 + bX + c, \quad b^2 - 4c < 0.
\]
Every \( f \in \mathbb{R}[X] \) factors as a product of polynomials of the above type, uniquely up-to-units and reordering.

**Proof.** It is straightforward to see that these polynomials are irreducible over \( \mathbb{R} \): the first because it is degree 1, the second because it has no real roots. Furthermore, these are the only irreducibles (up-to-units) of degree \( \leq 2 \).

If \( \deg f > 2 \), choose a root \( \lambda \in \mathbb{C} \) which exists since \( \mathbb{C} \) is algebraically closed. Then we can factor \( f = gh \) over \( \mathbb{R} \) where \( g \) is one of the two types above, depending on whether \( \lambda \in \mathbb{R} \) or not. Thus the claim about factorization follows by induction on degree. \[\square\]
We are going to need techniques to determine whether particular polynomials are irreducible. The main example is for polynomials over \( \mathbb{Q} \), and luckily there are several methods you can use here. The book defines \( f \in \mathbb{Z}[X] \) to be **irreducible over** \( \mathbb{Z} \) if (i) \( \deg f \geq 1 \) and (ii) \( f \) is not a product of elements of \( \mathbb{Z}[X] \) of smaller degree.

**Warning:** this is not the same as irreducibility in the domain \( \mathbb{Z}[X] \). I.e., \( 6X - 12 = 6(X - 2) \) is not irreducible as an element of \( \mathbb{Z}[X] \), but is an irreducible polynomial according to the book’s definition. This distinction will be important in what follows.

Since \( \mathbb{Z}[X] \subseteq \mathbb{Q}[X] \) is a subring, *a priori* irreducibility (either the standard or the book definition) in \( \mathbb{Z}[X] \) is not the same thing as irreducibility in \( \mathbb{Q}[X] \). It is easy to see that if \( f \in \mathbb{Z}[X] \) is irreducible over \( \mathbb{Q} \), then it is irreducible over \( \mathbb{Z} \) (in the sense of factoring into lower degree).

In fact, the converse is also true, by the following, which says that any factorization of \( f \in \mathbb{Z}[X] \) over \( \mathbb{Q} \) can be adjusted to one over \( \mathbb{Z} \).

**Theorem** (Gauss’s lemma). Suppose \( f \in \mathbb{Z}[X] \) and that \( f = g_1 \cdots g_r \) for some \( g_1, \ldots, g_r \in \mathbb{Q}[X] \). Then there exist \( c_1, \ldots, c_r \in \mathbb{Q} \) such that \( c_i g_i \in \mathbb{Z}[X] \) for all \( i = 1, \ldots, r \), and

\[
 f = (c_1g_1) \cdots (c_rg_r).
\]

In particular, we get the following criterion for irreducibility over \( \mathbb{Q} \).

**Corollary.** An integer polynomial \( f \in \mathbb{Z}[X] \) is irreducible over \( \mathbb{Q} \) if and only if it is irreducible over \( \mathbb{Z} \), i.e., cannot be factored into polynomials of strictly smaller degree over \( \mathbb{Z} \).

Here is a consequence of Gauss’s lemma that you may already know.

**Corollary** (Rational roots test). If \( f = c_0 + \cdots + c_nX^n \in \mathbb{Z}[X] \), then every rational root \( q \in \mathbb{Q} \) of \( f \) must have the form \( q = d/b \), where \( d \) and \( b \) are integers such that \( d \mid c_0 \) and \( b \mid c_n \).

**Proof.** If \( f(q) = 0 \) then we can factor \( f = g(X - q) \) with \( g, X - q \in \mathbb{Q}[X] \). By Gauss’s lemma there are \( a, b \in \mathbb{Q} \) such that

\[
 f = (ag)(bX - bq), \quad ag, bX - bq \in \mathbb{Z}[X].
\]

Write \( d = bq \in \mathbb{Z} \), whence \( q = d/b \). If we write \( ag = a_0 + \cdots + a_{n-1}X^{n-1} \) with \( a_0, \ldots, a_{n-1} \in \mathbb{Z} \), then the factorization \( f = (ag)(bX - d) \) has the form

\[
 c_0 + \cdots + c_nX^n = (a_0 + \cdots + a_{n-1}X^{n-1})(-d + bX),
\]

whence \( c_0 = -a_0d \) and \( c_n = a_{n-1}b \), so \( d \mid c_0 \) and \( b \mid c_n \) as desired. \( \square \)

Example: Let \( f = X^7 - 5 \). The rational root test says that any rational root must have the form \( q = d/b \) with \( d \in \{ \pm 1, \pm 5 \} \) and \( b \in \{ \pm 1 \} \). That is, \( q \in \{ \pm 1, \pm 5 \} \). It is easy to check directly that the four possibilities for \( q \) cannot be roots of \( f \), so we have proved that \( \sqrt{5} \) is irrational.

Observe that if \( p \) is a prime number and \( f = \sum c_k X^k \in \mathbb{Z}[X] \) is a polynomial, then \( p \mid f \) in \( \mathbb{Z}[X] \) if and only if \( p \) divides all the coefficients: i.e., if \( p \mid c_k \) in \( \mathbb{Z} \) for all \( k \). The proof of “Gauss’s lemma” uses the following observation.

**Lemma.** Suppose \( f = g_1 \cdots g_k \), where \( f, g_1, \ldots, g_k \in \mathbb{Z}[X] \). If \( p \in \mathbb{Z} \) is a prime number which divides all the coefficients of \( f \), then there exists an \( i \) such that \( p \) divides all the coefficients of \( g_i \), and thus \( g_i = pf_i \) for some \( g_i \in \mathbb{Z}[X] \).

**Proof.** If \( r = 1 \) there is nothing to prove.

Suppose \( r = 2 \). I’ll prove the converse: if \( p \) doesn’t divide all coefficients of \( g \) and doesn’t divide all coefficients of \( h \), then \( p \) doesn’t divide all coefficients of \( gh \). (Equivalently: \( p \mid gh \) implies \( p \mid g \) or \( p \mid h \).)
Write \( g = a_0 + a_1 X + \cdots + a_m X^m \) and \( h = b_0 + b_1 X + \cdots + b_n X^n \). Since \( p \) does not divide all coefficients of either of these, there is a smallest integer \( r \) such that \( p \mid a_r \) and a smallest integer \( s \) such that \( p \mid b_s \). Let \( t = r + s \), and consider the coefficient of \( X^t \) in \( f = gh \), which is equal to

\[
c_t = a_0b_t + a_1b_{t-1} + \cdots + a_{r-1}a_{s+1} + a_r b_s + a_{r+1}a_{s-1} + \cdots + a_{t-1}b_1 + a_t b_0.
\]

All the terms in the first group are divisible by \( p \) since \( p \mid a_i \) if \( i < r \), and all the terms in the second group are divisible by \( p \) since \( p \mid b_j \) if \( j < s \). Therefore

\[
c_t \equiv a_r b_s \mod p.
\]

Since \( p \) is prime and does not divide either \( a_r \) or \( b_s \), it does not divide \( c_t \).

Now suppose \( r \geq 3 \), and proceed by induction on \( r \). Writing the identity as \( f = (g_1 \cdots g_{r-1})g_r \) and applying case \( r = 2 \) with \( g = g_1 \cdots g_{r-1} \) and \( h = g_r \), we see that either (i) \( p \mid (g_1 \cdots g_{r-1}) \), and so \( p \mid g_i \) for some \( i = 1, \ldots, r - 1 \) by induction, or (ii) \( p \mid g_r \).

\[\square\]

**Proof of “Gauss’s lemma”**. If \( f = 0 \) then the theorem is trivial, so assume \( f \neq 0 \). The case of \( r = 1 \) is also trivial, since \( g_1 = f \in \mathbb{Z}[X] \).

For the \( r \geq 2 \) case, given \( f = g_1 \cdots g_k \) with \( f \in \mathbb{Z}[X] \) and \( g_i \in \mathbb{Q}[X] \), first choose positive integers \( a_1, \ldots, a_k \in \mathbb{Z}_{>0} \) such that \( a_i g_i \in \mathbb{Z}[X] \). For instance, you can let \( a_i \) be the product of the denominators of each of the rational coefficients of \( g_i \).

This shows that there exists \( n \in \mathbb{Z}_{>0} \) and \( a_1, \ldots, a_r \in \mathbb{Q} \) such that

\[
nf = (a_1g_1) \cdots (a_r g_r), \quad a_i g_i \in \mathbb{Z}[X].
\]

We want an identity of this form with \( n = 1 \). I’ll show that such an identity exists by induction on \( n \). If \( n > 1 \), choose a prime number \( p \) such that \( p \mid n \) in \( \mathbb{Z} \). Then by the above lemma, \( p \mid a_k g_k \) for some \( k \in \{1, \ldots, r\} \). Therefore

\[
(n/p)f = (a_1g_1) \cdots ((a_k/p)g_k) \cdots (a_r g_r)
\]

holds, and is an identity of the same type with smaller “\( n \)”, since \( a_k/p \in \mathbb{Q} \) and \( (a_k/p)g_k \in \mathbb{Z}[X] \).

Proceding inductively, we get the desired identity. \(\square\)

### 13. Characteristic and prime fields

Given any field \( F \) and any \( n \in \mathbb{Z}_{\geq0} \), we can form the sum

\[
1 + 1 + \cdots + 1 \in F,
\]

which we conventionally call “\( n \in F \)”. The notation is ambiguous (“\( n \)” represents an element of \( \mathbb{Z} \) and an element of \( F \), which need not be the same), but we can deal with it.

The **characteristic** of \( F \) is either (i) the smallest \( n > 0 \) such that \( n = 0 \) if \( F \), or (ii) 0 if \( n \neq 0 \) in \( F \) for all \( n \in \mathbb{Z}_{>0} \). We say that \( F \) has **finite characteristic** if the characteristic is \( > 0 \).

**Proposition.** If \( F \) has finite characteristic \( n \), then \( n \) is a prime.

**Proof.** Suppose not, i.e., suppose \( F \) has characteristic \( n = de \) for some \( d, e \in \mathbb{Z}_{\geq0} \). Then this same identity holds in \( F \):

\[
1 + \cdots + 1 = (1 + \cdots + 1)(1 + \cdots + 1)
\]

Since \( F \) is a field, one of the factors must be 0 in \( F \), contradicting the minimality of \( n \). \(\square\)
The standard example of a field of finite characteristic is $\mathbb{F}_p = \mathbb{Z}/p$, the integers modulo $p$.

Given a field $F$, its **prime subfield** is its smallest subfield, i.e., the smallest subset containing 0 and 1 and closed under addition, multiplication, and additive and multiplicative inverses. A field is a **prime field** if it is its own prime subfield.

**Proposition.** $\mathbb{Q}$ and $\mathbb{F}_p$ for $p$ prime are prime fields. Every prime subfield of a field $F$ is isomorphic to one of these, depending on the characteristic of $F$.

**Proposition.** It is easy to see that $\mathbb{Q}$ and the $\mathbb{F}_p$ are prime fields, since all elements in them can be obtained from 0, 1 using the operations. If $F$ has characteristic $p > 0$, it is easy to see that the subset $\{0, \ldots, p-1\} \subseteq F$ is a subfield, and is isomorphic to $\mathbb{F}_p$. If $F$ has characteristic 0, then the subset $\{n \in F \mid n \in \mathbb{Z}\}$ is a subring of $F$, and since $F$ is a field we have elements $a/b \in F$ for $a, b \in \mathbb{Z}, b \neq 0$. It is straightforward to show that $\mathbb{Q} \to F$ gives an isomorphism to a subfield of $F$.

14. **Polynomials over Z: reducing modulo a prime**

Let $f \mapsto \overline{f}: \mathbb{Z}[X] \to \mathbb{F}_p[X]$ be the function given by reducing coefficients modulo $p$. That is, if $f = \sum a_k X^k$ with $a_k \in \mathbb{Z}$, then
\[
\overline{f} = \sum \overline{a_k} X^k,
\]
where $\overline{a_k} \in \mathbb{Z}/p$ is the mod $p$ reduction of $a_k$.

**Lemma.** The function $f \mapsto \overline{f}$ is a ring homomorphism.

**Proof.** Straightforward: need to show $\overline{0} = 0$, $1 \overline{f} = \overline{f}$, $\overline{f+g} = \overline{f} + \overline{g}$, $\overline{fg} = \overline{f} \overline{g}$. \(\square\)

**Remark.** Note that since $\mathbb{F}_p$ is a field, $\mathbb{F}_p[X]$ is a domain. Also note that for $f \in \mathbb{Z}[X]$, we have $\overline{f} = 0$ if and only if $p$ divides all coefficients of $f$. If $g, h \in \mathbb{Z}[X]$ and $f = gh$, we must have $\overline{f} = 0$ if and only if either $\overline{g} = 0$ or $\overline{h} = 0$. This is exactly the lemma we needed in the proof of Gauss’s lemma.

**Corollary.** If $f \in \mathbb{Z}[X]$ is such that $\overline{f} \in \mathbb{F}_p[X]$ is irreducible, then $f$ is irreducible.

This test is hard to use in general, since there isn’t an easy way to recognize that a polynomial over $\mathbb{F}_p$ is going to be irreducible. It is useful for cubics however, since to show that a cubic is irreducible you just have to show it has no root.

Example. Let $f = X^3 + 5X^2 - 4X + 11$. Modulo 5 this becomes $\overline{f} = X^3 + X + 1$. To show this is irreducible over $\mathbb{F}_5$, just check that it has no roots in $\mathbb{F}_5$:
\[
\overline{f}(0) = 1, \quad \overline{f}(1) = 3, \quad \overline{f}(2) = 1, \quad \overline{f}(3) = 1, \quad \overline{f}(4) = 4.
\]
Therefore $f$ is irreducible over $\mathbb{Z}$, and hence over $\mathbb{Q}$.

Warning: This kind of test can fail. There are irreducible $f \in \mathbb{Z}[X]$ which are reducible modulo every prime.

15. **Polynomials over Z: Eisenstein criterion**

The Eisenstein criterion is one for irreducibility over $\mathbb{Z}$. It only works in special situations, but it is useful for some cases we will need.

**Theorem** (Eisenstein criterion). Consider a polynomial $f = c_0 + c_1 X + \cdots + c_n X^n \in \mathbb{Z}[X]$ with integer coefficients, and a prime $p \in \mathbb{Z}$. If
\[
\begin{align*}
(1) & \ p \mid c_n, \\
(2) & \ p \mid c_i \text{ for } i = 0, \ldots, n-1, \text{ and} \\
(3) & \ p^2 \nmid c_0,
\end{align*}
\]
then $f$ is irreducible in $\mathbb{Q}[X]$.
**Proof.** By Gauss’s Lemma, it suffices to show that \( f \) cannot be factored over \( \mathbb{Z} \) into polynomials of strictly smaller degree.

Suppose \( f = gh \) over \( \mathbb{Z} \), where \( g = \sum_{i=0}^{d} a_i X^i \), \( h = \sum_{j=0}^{e} b_j X^j \) have degrees \( \deg(g) = d \) and \( \deg(h) = e \), with \( d + e = n \) and \( 0 < d, e < n \). Note that therefore \( c_n = a_d b_e \), so \( p \nmid a_d \) and \( p \nmid b_e \).

Modulo \( p \), \( f = gh \) has the form

\[
\overline{c}_n X^n = \overline{g} = \overline{h}
\]

in \( \mathbb{F}_p[X] \).

Therefore \( \overline{g} = \overline{a}_d X^d \) and \( \overline{h} = \overline{b}_e X^e \), whence

\[
g = a_d X^d + pu, \quad h = b_e X^e + pv, \quad u, v \in \mathbb{Z}[X], \quad \deg(u) < d, \deg(v) < e.
\]

Therefore

\[
f = gh = (a_d X^d + pu)(b_e X^e + pv) = c_n X^n + p(a_d X^d v + b_e X^e u) + p^2 uv.
\]

Evaluation at \( X = 0 \) gives \( c_0 = f(0) = p^2 u(0)v(0) \), which contradicts the hypothesis that \( p^2 \nmid c_0 \). \( \square \)

Example. Any polynomial of the form \( f = X^n - a \) with \( n \geq 1 \), and \( a \) an integer whose prime factorization has exactly one power of some prime \( p \), is irreducible over \( \mathbb{Q} \). E.g., \( f = X^{42} - 12 \).

Here is a useful observation, which is based on the fact that if \( f \) is a polynomial of degree \( n \), then so is \( f(X + a) \). I.e., a Tschirnhaus transformation does not change irreducibility.

**Proposition.** Let \( f \in F[X] \) be a polynomial and \( a \in F \), and consider \( g(X) = f(X - a) \). Then \( f \) is irreducible if and only if \( g \) is irreducible.

**Proof.** If \( f = f_1 f_2 \), then \( g(X) = f(X) = f_1(X - a)f_2(X - a) \), so \( f \) reducible implies \( g \) reducible. Conversely, if \( g = g_1 g_2 \), then \( f(X) = g(X + a) = g_1(X + a) g_2(X + a) \), so \( g \) reducible implies \( f \) reducible. \( \square \)

For instance, if \( f(X) = X^4 + X^3 + X^2 + X + 1 \), then

\[
g(X) = f(X + 1) = (X + 1)^4 + (X + 1)^3 + (X + 1)^2 + (X + 1) + 1 = X^4 + 5X^3 + 10X^2 + 10X + 5,
\]

and Eisenstein’s criterion with \( p = 5 \) shows that this is irreducible.

**Proposition.** Let \( p \) be a prime number and let \( \Phi_p(X) = \sum_{i=0}^{p-1} X^i = X^{p-1} + \cdots + X + 1 \). Then \( \Phi_p \) is irreducible over \( \mathbb{Q} \).

**Proof.** The case of \( p = 2 \) is obvious, so assume \( p \) is an odd prime. Let \( g(X) = \Phi_p(X + 1) \). We have

\[
g = \sum_{k=0}^{p-1} (X + 1)^k = \sum_{j=0}^{p-1} \sum_{j=0}^{k-j} \binom{k}{j} X^j = \sum_{j=0}^{p-1} \sum_{j=0}^{k-j} \binom{k}{j} X^j = \sum_{j=0}^{p-1} \binom{p}{j+1} X^j.
\]

This uses the identity

\[
\sum_{k=j}^{p-1} \binom{k}{j} = \binom{j}{j} + \binom{j+1}{j} + \binom{j+2}{j} + \cdots + \binom{p-1}{j} = \binom{p}{j+1},
\]

which is valid for all \( 0 \leq j < p \) (and \( p \) can be any natural number), and can be proved using the “Pascal identity” \( \binom{k}{j+1} + \binom{k}{j} = \binom{k+1}{j+1} \) and the fact that \( \binom{j}{j} = \binom{j+1}{j+1} \).

We have

\[
\binom{p}{j+1} = \frac{(p)(p-1) \cdots (p-j+1)(p-j)}{(j+1)(j+2) \cdots (2)(1)},
\]

which for \( 0 \leq j < p - 1 \) is divisible by \( p \), and also \( \binom{p}{p} = p \) is not divisible by \( p^2 \). Therefore Eisenstein applies to show that \( g \) is irreducible, hence \( f \) is irreducible. \( \square \)
16. Roots of unity

A \textit{nth root of unity} in a field $F$ is any element $a \in F$ such that $a^n = 1$. We say that $a$ is a \textit{primitive nth root of unity} if order($a$) = $n$ as an element of $F^\times$; that is, if $a^n = 1$ and $a^k \neq 1$ when $1 \leq k < n$.

Note that with this terminology, any \textit{nth root of unity} is also an \textit{mth root of unity} when $n \mid m$. However, a \textit{root of unity} is \textit{primitive} for only one value of $n$ (= its order in the group of units).

Note that since the \textit{nth roots of unity} satisfy the polynomial $X^n - 1$, there are at most $n$ of them in any field.

In \mathbb{C}, every \textit{nth root of unity} has the form

$$\zeta^k = e^{2\pi i k/n} = \cos(2\pi k/n) + i \sin(2\pi k/n), \quad 0 \leq k < n,$$

where $\zeta^n = e^{2\pi i/n}$. Since there are exactly $n$ of these, this gives all roots of unity in \mathbb{C}.

Note that $G := \{1, \zeta, \ldots, \zeta^{n-1}\} \subset \mathbb{C}^\times$ are a cyclic group of order $n$. The primitive \textit{nth roots of unity} are those single elements which generate $G$. Thus $\zeta^k$ is a \textit{primitive nth root of unity} if $\gcd(k, n) = 1$. The other elements of $G$ are \textit{dth roots of unity} for various smaller $d$ which divide $n$.

Here is a list of some roots of unity in \mathbb{C}.

- 1 is the only primitive first root of unity.
- There are two 2nd roots of unity, but only one is primitive: $-1$. $-1$ is the only primitive second root of unity.
- There are three 3rd roots of unity, but only two primitive ones: $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ and $\omega^2 = \omega^{-1} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$.

Note that $\omega, \omega^2$ are roots of of $\Phi_3(X) = X^2 + X + 1 = 0$, which is irreducible over \mathbb{Q} (or \mathbb{R}).

- $i$ and $-i$ are the only primitive 4th roots of unity. They are roots of $\Phi_4(X) = X^2 + 1 = 0$, which is irreducible over \mathbb{Q} (or \mathbb{R})

- $\zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4$ are the primitive 5th roots of unity. They are roots of $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1 = 0$, since $X^5 - 1 = (X - 1)\Phi_5(X)$.

Claim:

$$\zeta_5 = \cos(2\pi/5) + i \sin(2\pi/5) = \frac{-1 + \sqrt{5}}{4} + \frac{\sqrt{10 + 2\sqrt{5}}}{4}i.$$

How did I solve for this? Let $\alpha = \zeta_5 + \zeta_5^{-1}$, and notice that

$$\alpha^2 + \alpha - 1 = \zeta_5^2 + \zeta_5 + 1 + \zeta_5^{-1} + \zeta_5^{-2}.$$

If we multiply by $\zeta_5 - 1$, the right-hand side works out to $\zeta_5^{3} - \zeta_5^{-2} = 0$. Since $\zeta_5 - 1 \neq 0$, we must have $\alpha^2 + \alpha - 1 = 0$. Solving this quadratic gives $\alpha = \frac{-1 + \sqrt{5}}{2}$. Then $\alpha/2$ is the real part of $\zeta_5$.

- $\zeta_6 = -\omega^2$ and $\zeta_6^5 = -\omega$ are the only primitive 6th roots of unity. They are the roots of $\Phi_6(X) = X^2 - X + 1 = 0$, which is irreducible.

- $\zeta_7, \zeta_7^2, \zeta_7^3, \zeta_7^4, \zeta_7^5$ are the primitive 7th roots of unity, where $\zeta_7 = \cos(2\pi/7) + i \sin(2\pi/7)$. They are roots of $\Phi_7(X) = X^6 + \cdots + X + 1 = 0$, which is irreducible over \mathbb{Q}. (But reducible over \mathbb{R}.)

You can get an “explicit” expression for $\zeta_7$ by setting $\alpha = \zeta_7 + \zeta_7^{-1}$ and observing that it satisfies a cubic equation which you can solve; then $\alpha/2$ is the real part of $\zeta_7$.

- $(1 + i)/\sqrt{2}, (1 - i)/\sqrt{2}, (1 + i)/\sqrt{2}, (1 - i)/\sqrt{2}$ are the only primitive 8th roots of unity. They are roots of $\Phi_8(X) = X^4 + 1$, which is irreducible over \mathbb{Q}.

Exercise. There are six primitive 9th roots of unity. They are roots of a degree 6 monic polynomial $\Phi_9 \in \mathbb{Z}[X]$. What is $\Phi_9$?
The $n$th roots of unity in $\mathbb{C}$ are roots of a monic polynomial over $\mathbb{Z}$, namely $X^n - 1$. This polynomial is not irreducible (if $n > 1$) since 1 is a root.

Later on, we will show that for every $n$, there exists a monic polynomial $\Phi_n(X) \in \mathbb{Z}[X]$ such that the roots of $\Phi_n$ are precisely the primitive $n^{th}$ roots of unity, with multiplicity 1 (this is not so hard to prove). The $\Phi_n$ are called the cyclotomic polynomials. It also will turn out that $\Phi_n(X)$ is always irreducible (this is harder to prove).

We can’t do this yet, but we do have this now when $n = p$ is prime: $\Phi_p(X) = X^{p-1} + \cdots + X + 1$. This is just the fact that $X^p - 1 = (X - 1)(X^{p-1} + \cdots + X + 1)$.

Exercise: What is $\Phi_{p^r}(X)$ for $p$ prime and $r \geq 1$?

17. Field extensions

A homomorphism of rings is a function $\phi: R \to S$ between rings which preserves all the structure. That is:

- $\phi(0) = 0$ and $\phi(1) = 1$,
- $\phi(x + y) = \phi(x) + \phi(y)$ and $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in R$.

(That $\phi(0) = 0$ is actually a consequence of the other axioms so I don’t need to include it. However, $\phi(1) = 1$ is not a consequence of the other axioms.)

**Proposition.** If $\phi: K \to L$ is a homomorphism between fields, then $\phi$ is an injective function.

**Proof.** If $\phi(a) = 0$, then since $1 = aa^{-1}$ we have $1 = \phi(1) = \phi(a)\phi(a^{-1}) = 0$. But in the field $L$ we have $0 \neq 1$, so this is impossible. $\square$

The book calls a homomorphism between fields a monomorphism. This is ok: “monomorphism” is a technical term for a homomorphism which behaves like an injective function. I will probably just call them homomorphisms.

A field extension is a homomorphism $\iota: K \to L$ of fields.

A typical example of field extensions comes from subfields. If $F \subseteq K$ is a subfield, then the inclusion function $\iota: F \to K$ is a homomorphism.

**Proposition.** Given a field extension $\iota: K \to L$, let $K' = \iota(K) \subseteq L$, the image of $K$ under $\iota$. Then $K' \subseteq L$ is a subfield and $\iota$ restricts to an isomorphism $K \overset{\sim}{\to} K'$.

Every field $K$ contains a prime subfield $F$, so this always gives an example of a field extension. E.g., $\mathbb{Q} \subseteq \mathbb{C}$. Most extension we meet are of subfields.

18. Subfields generated by a set

Let $K$ be a field, and $X \subseteq K$ a subset. The subfield generated by $X$ is the intersection of all subfields which contain $X$.

**Proposition.** The subfield $F$ generated by $X$ is the set of elements which can be obtained from $X$ by a finite sequence of the operations $+, -, \times, \div$ applied to $X \cup \{0, 1\}$. This subfield always contains the prime subfield of $F$.

**Proof.** By definition, this subset of elements is a subfield containing $X$, and is contained in any subfield containing $X$. Since $F$ is a subfield, it necessarily contains the prime subfield. $\square$

In practice, our subset $X \subseteq K$ will have the form $X = F \cup \{\alpha_1, \ldots, \alpha_k\}$, where $F \subseteq K$ is a subfield. In this case we write the field generated by $X$ as $F(\alpha_1, \ldots, \alpha_k)$.

Thus we get two field extensions: $F \subseteq F(\alpha_1, \ldots, \alpha_k) \subseteq K$.

When $X \subseteq \mathbb{C}$, any subfield of $\mathbb{C}$ contains $\mathbb{Q}$, and we just always write $\mathbb{Q}(X)$. 

\[ \text{W 11 Sep} \]
Example. \( \mathbb{Q}(i) \subseteq \mathbb{C} \). This is just the set
\[
F = \{ a + bi \mid a, b \in \mathbb{Q} \}.
\]
To see that the set is a subfield, verify that \( 0, 1 \in F \), and that \( F \) is closed under operations \((a, b, a', b' \in \mathbb{Q})\):
\[
(a + bi) + (a' + b'i) = (a + a') + (b + b')i, \\
-(a + bi) = (-a) + (-b)i, \\
(a + bi)(a' + b'i) = (aa' - bb') + (ab' + ba')i,
\]
\[
(a + bi)^{-1} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}i, \quad \text{if } (a, b) \neq (0, 0).
\]
Example. \( \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{C} \). This is just the set
\[
\{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \},
\]
as can be proved by an argument as above.
Remark: note that \( a + b\sqrt{2} = 0 \) with \( a, b \in \mathbb{Q} \) only if \( a = b = 0 \), which implies that every element of \( \mathbb{Q}(\sqrt{2}) \) can be written uniquely in the above form. This is because \( \sqrt{2} \) is irrational!
Example. \( \mathbb{Q}(\sqrt{3}) \) is actually equal to \( \mathbb{Q} \), since \( \sqrt{3} = 3 \).
This means you have to be careful if you say something like \( \mathbb{Q}(\sqrt{N}) \) for some \( N \in \mathbb{Z} \). Whether \( \mathbb{Q}(\sqrt{N}) \neq \mathbb{Q} \) depends on the whether the integer \( N \) is a square.
Example. \( \mathbb{Q}(\sqrt{18}) = \mathbb{Q}(\sqrt{2}) \), since \( 18 = 3\sqrt{2} \).
Example. \( \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{C} \). This is the set
\[
\{ a + \sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q} \}.
\]
Again it is easy to show that this is a subring of \( \mathbb{C} \), but work is needed to show it has multiplicative inverses.
Here is an argument for \( \mathbb{Q}(\sqrt{2}, \sqrt{3}) \). First we need
**Lemma.** \( \sqrt{3} \notin \mathbb{Q}(\sqrt{2}) \).
**Proof.** Suppose \( \sqrt{3} \in \mathbb{Q}(\sqrt{2}) \). I.e., suppose there exist \( a, b \in \mathbb{Q} \) such that \( (a + b\sqrt{2})^2 = 3 \). Then
\[
a^2 + 2b^2 + 2ab\sqrt{2} = 3.
\]
But (because \( \sqrt{2} \) is irrational), this implies
\[
a^2 + 2b^2 = 3, \quad 2ab = 0, \quad \text{where } a, b \in \mathbb{Q}.
\]
The second equation gives two cases: \( a = 0 \) or \( b = 0 \), and it is easy to see that in either case there is no solution in \( \mathbb{Q} \) of the first equation, since \( \pm \sqrt{3}, \pm \sqrt{3/2} \notin \mathbb{Q} \).
Now suppose \( \alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \) with \( a, b, c, d \in \mathbb{Q} \). I will use the fact that \( \mathbb{Q}(\sqrt{2}) \) is a field. Write
\[
u = a + b\sqrt{2}, \quad v = c + d\sqrt{2}, \quad \text{so} \quad \alpha = u + v\sqrt{3}.
\]
I claim that
\[
\alpha^{-1} = \frac{1}{u + v\sqrt{3}} \cdot \frac{u - v\sqrt{3}}{u - v\sqrt{3}} = \frac{u - v\sqrt{3}}{u^2 - 3v^2} = \frac{u}{u^2 - 3v^2} + \frac{-v}{u^2 - 3v^2}\sqrt{3}.
\]
This works fine as long as \( u^2 - 3v^2 \neq 0 \). But if \( u^2 - 3v^2 \neq 0 \), then \( 3 = (u/v)^2 \) with \( u/v \in \mathbb{Q}(\sqrt{2}) \), which we proved is impossible.
Example. $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{C}$. This is the set
\[ \{ a + b\sqrt{2} + c\sqrt{4} \mid a, b, c \in \mathbb{Q} \}. \]
It turns out that we need the third term here: $\sqrt{4} = (\sqrt{2})^2$ cannot be written as $a + b\sqrt{2}$ for any $a, b \in \mathbb{Q}$. (Why?)

As above, it is easy to prove directly that $\mathbb{Q}(\sqrt{2})$ is a subring of $\mathbb{C}$. Existence of multiplicative inverses is trickier. We will have a good proof of this soon.

Exercise. Find an explicit formula for multiplicative inverse in $\mathbb{Q}(\sqrt{2})$.

A simple extension is a field extension $\iota: K \to L$ such that $L = \iota(K)(\alpha)$ for some $\alpha \in L$. Pretty much always we assume $K \subseteq L$, so we can just say $L = K(\alpha)$.

Example. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then $K/\mathbb{Q}$ is a simple extension. In fact, $K = \mathbb{Q}(\alpha)$ where $\sqrt{2} + \sqrt{3}$.

To see this, first note that $\alpha \in K$, so $\mathbb{Q}(\alpha) \subseteq K$.

To show $K \subseteq \mathbb{Q}(\alpha)$, it suffices to show $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\alpha)$. Since $\sqrt{3} = \alpha - \sqrt{2}$, it is enough to show $\sqrt{2} \in \mathbb{Q}(\alpha)$.

Here are some elements of $\mathbb{Q}(\alpha)$:
\[ \alpha = \sqrt{2} + \sqrt{3}, \quad \alpha^2 = (\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}, \quad \sqrt{6} = (\alpha^2 - 5)/2, \quad \alpha\sqrt{6} = 2\sqrt{3} + 3\sqrt{2}. \]
Then
\[ \sqrt{2} = \alpha\sqrt{6} - 2\alpha = (\alpha^3 - 9\alpha)/2 \in \mathbb{Q}(\alpha). \]

Also $\sqrt{3} = \alpha - \sqrt{2} \in \mathbb{Q}(\alpha)$, so we are done.

If $F \subseteq K$ is a subfield, then we can write “$K : F$” as notation for the extension $F \to K$. Note: this is the book’s notation. Many people (like me) prefer to write $K/F$ for the extension, but I’ll try to follow the book here.

19. Algebraic and transcendental

Let $K \subseteq L$ be a subfield and $\alpha \in L$. We say that
\begin{itemize}
  \item $\alpha$ is algebraic over $K$ if $\alpha$ is a root of some $f \in K[X]$, $f \neq 0$, and
  \item $\alpha$ is transcendental over $K$ if there is so such $f \in K[X]$.
\end{itemize}

When $K = \mathbb{Q}$ we just say “algebraic” and “transcendental”.

Example. Every number $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{R}$, since it is a root of $f = (X - \alpha)(X - \overline{\alpha}) \in \mathbb{R}[X]$.

Over $\mathbb{Q}$, elements of $\mathbb{C}$ like $\sqrt{a}$ for $a \in \mathbb{Q}$ are always algebraic. On the other hand, $\pi$ and $e$ are transcendental: the book gives a proof in Chapter 24. Some numbers related to these are also transcendental, but others are not known.

For instance, it is apparently not known whether $e + \pi$ or $e\pi$ are transcendental, or even that they are rational. (However, at least one of the two is irrational (Why?).)

20. Fields of rational functions

A standard example of transcendental elements comes from fields of rational functions.

Given a domain $D$, one can always construct a field $K$, called the fraction field of $D$, together with a ring homomorphism $\iota: D \to K$ so that
\begin{itemize}
  \item $\iota$ is injective, so that $D$ is isomorphic to the image subring $\iota(D) \subseteq K$ (and so by abuse of notation we identity $D$ with this subring of $K$), and
  \item every element of $K$ has the form $ab^{-1}$ for some $a, b \in D$.
\end{itemize}

The recipe for construction the fraction field is basically: fractions!
Elements of $K$ are defined to be equivalence classes of pairs $(a, b)$ with $a, b \in D$ and $b \neq 0$, using the equivalence relation

$$(a, b) \sim (a', b') \iff ab' = ba'.$$

(To check that this is an equivalence relation, you need to use the fact that $D$ is a domain, not merely a commutative ring.)

Write $\left[ \begin{array}{c} a \\ b \end{array} \right]$ for the equivalence class of $(a, b)$. Define

$$\left[ \begin{array}{c} a \\ b \end{array} \right] + \left[ \begin{array}{c} a' \\ b' \end{array} \right] = \left[ \begin{array}{c} ab' + ba' \\ bb' \end{array} \right]$$

and

$$\left[ \begin{array}{c} a \\ b \end{array} \right] \cdot \left[ \begin{array}{c} a' \\ b' \end{array} \right] = \left[ \begin{array}{c} aa' \\ bb' \end{array} \right].$$

You need to verify that these are well-defined, since a priori the formulas depend on the choice pairs $(a, b)$ and $(a', b')$, and not obviously only on the equivalence classes of these.

Also define $0 := \left[ \begin{array}{c} 0 \\ 1 \end{array} \right]$ and $1 := \left[ \begin{array}{c} 1 \\ 1 \end{array} \right]$.

Define $\iota: D \to K$, $\iota(a) := \left[ \begin{array}{c} a \\ 1 \end{array} \right]$.

Verify the axioms for a field, and that $\iota$ is an injective ring homomorphism. In particular, you discover that

$$-\left[ \begin{array}{c} a \\ b \end{array} \right] = \left[ \begin{array}{c} -a \\ b \end{array} \right], \quad \left[ \begin{array}{c} a \\ b \end{array} \right]^{-1} = \left[ \begin{array}{c} b \\ a \end{array} \right].$$

Exercise. Show that $\left[ \begin{array}{c} fh \\ gh \end{array} \right] = \left[ \begin{array}{c} f \\ g \end{array} \right]$ for any $f, g, h \in D$, $g$ and $h$ non-zero.

Example. The fraction field of $\mathbb{Z}$ is $\mathbb{Q}$.

Exercise. Suppose $D$ is already a field. Show that in the above construction $D \to K$ is an isomorphism.

Given a field $K$, let $D = K[t]$ be the polynomial ring over $K$ in one variable $t$, which is a domain. Hence we can construct its fraction field, denoted $K(t)$. Elements of this are “fractions of polynomials”, i.e., are represented by

$$\frac{f(t)}{g(t)}, \quad f, g \in K[t], \quad g \neq 0.$$

This is called the field of rational functions over $K$, or the field of rational expressions.

Note that $K \subseteq K(t)$ is a simple extension.

Note that $K[t_1, \ldots, t_n]$ is a domain for any $n$, so it also has a fraction field, denoted $K(t_1, \ldots, t_n)$. (It turns out not to be a simple extension when $n \geq 2$.)

Example. For any field $K$, the element $t \in K(t)$ is transcendental over $K$.

To see this: if $f \in K[X]$, then plugging in $t$ into $f$ gives $f(t) \in K(t)$. This can only be 0 when $f = 0$, because $\iota: K[t] \to K(t)$ is injective.

21. Minimal polynomial

If $L/K$ is an extension and $\alpha \in L$ is algebraic over $K$, consider all non-zero polynomials $f \in K[X]$ which have $\alpha$ as a root. Among these are ones with minimal degree, and there is a unique such which is monic.

The minimal polynomial over $K$ of $\alpha \in L$ (algebraic over $K$) is the unique monic polynomial $f \in K[X]$ of minimal degree such that $f(\alpha) = 0$.

Notation: I’m going to write

$$f_{\alpha/K} \in K[X]$$

to mean the minimal polynomial over $K$. (The book provides no notation for this.)
Example. Let \( \alpha = (1+i)/\sqrt{2} \in \mathbb{C} \). Then
\[
\begin{align*}
f_{\alpha/\mathbb{Q}} &= X^4 + 1, \\
f_{\alpha/\mathbb{R}} &= X^2 - \sqrt{2}X + 1, \\
f_{\alpha/\mathbb{C}} &= X - \alpha.
\end{align*}
\]

The following is crucial.

**Proposition.** If \( \alpha \) is algebraic over \( K \) (in some extension \( L/K \)), then the minimal polynomial \( f = f_{\alpha/K} \) divides every polynomial \( g \in K[X] \) which has \( \alpha \) as a root.

**Proof.** By the division algorithm applied to \( g \div f \), there exist \( q, r \in K[X] \) with \( \deg r < \deg f \) such that
\[
g = qf + r.
\]
Plugging in \( X = \alpha \) gives \( g(\alpha) = q(\alpha)f(\alpha) + r(\alpha) \), so \( r(\alpha) = 0 \). But \( f \) is the minimal polynomial, so \( r = 0 \), so \( g = qf_{\alpha/K} \).

**Remark.** The set \( I = \{ g \in K[X] \mid g(\alpha) = 0 \} \) is an ideal in \( K[X] \), and so is a principal ideal. By definition, \( f_{\alpha/K} \) is the monic polynomial of minimal degree in \( I \), and the previous proof is the standard proof that such an element generates the ideal \( I \).

**Corollary.** A minimal polynomial \( f_{\alpha/K} \in K[X] \) is irreducible over \( K \).

**Proof.** If it factors, \( \alpha \) must be a root of one of the factors.

**Remark.** Let \( K \subseteq \mathbb{C} \) be a subfield and \( f \in K[X] \) irreducible over \( K \). Then \( f = f_{\alpha/K} \) for some element in \( \mathbb{C} \). In fact, \( \alpha \) can be chosen to be any root of \( f \) in \( \mathbb{C} \).

For instance, \( f = X^3 - 2 \in \mathbb{Q}[X] \) is irreducible over \( \mathbb{Q} \), and is therefore the minimal polynomial of three elements in \( \mathbb{C} \):
\[
\sqrt[3]{2}, \quad \omega \sqrt[3]{2}, \quad \omega^2 \sqrt[3]{2}, \quad \text{where} \quad \omega = e^{2\pi i/3}.
\]

### 22. Constructing Simple Algebraic Extensions

Let \( K \) be a field and \( K[X] \) the polynomial ring. Given \( f \in K[X] \), say that \( g, h \in K[X] \) are **congruent modulo** \( f \) (\( g \equiv h \pmod{f} \)) if there exists \( m \in K[X] \) such that
\[
h = g + mf.
\]
This is an equivalence relation on \( K[X] \). The quotient of \( K[X] \) by this equivalence relation is called
\[
R := K[X]/(f).
\]
This is a commutative ring, with operations “inherited” from \( K[X] \), so that the projection map
\[
\pi: K[X] \to K[X]/(f)
\]
is a ring homomorphism. I might write \([g] = \pi(g)\) for the equivalence class containing \( g \).

**Example.** If \( f = 0 \), then \( g \equiv h \pmod{f} \) iff \( g = h \), so \( R = K[X] \) in this (boring) case.

**Example.** If \( f \neq 0 \), so \( \deg f = n \geq 0 \), then there for each \( g \in K[X] \) is a **unique** element \( r \in K[X] \) such that (i) \( g \equiv r \pmod{f} \) and (ii) \( \deg r < n \). This is just a consequence of the division algorithm.

I’ll call such \( r \) the **canonical representative** of \( [g] \in K[X]/(f) \). Using the division algorithm, we can always carry out calculations of addition and multiplication in \( K[X]/(f) \) using canonical representatives.

**Example.** \( R = \mathbb{Q}[X]/(X^3 - 2) \) or \( R' = \mathbb{Q}[X]/(X^2 - 1) \).

**Proposition.** \( R = K[X]/(f) \) is a field if and only if \( f \in K[X] \) is irreducible over \( K \).
Remark. You don’t really need to compute 

This gives 

The degree of the LHS is too big, so we “correct” it to get rid of the 

c from both sides: 

Now multiply through by X again: 

Multiply everything through by X (keeping f and g the same): 

The degree of the LHS is too big, so we “correct” it to get rid of the $X^3$ term by subtracting an appropriate multiple of $f$ from both sides: 

Now multiply through by X again: 

Example. Let $K = \mathbb{Q}[X]/(X^3 - 2)$, where $f = X^3 - 2$ is irreducible over $\mathbb{Q}$, so $K$ is a field. To compute the multiplicative inverse of $\alpha = [g] = [c_2X^2 + c_1X + c_0]$ in $K$, use the Euclidean algorithm to find $m, n \in \mathbb{Q}[X]$ such that $1 = mf + ng$. Then $[g]^{-1} = [n]$ (unless $[g] = 0$, in which case no answer will be found).

I find carrying out the Euclidean algorithm by hand to be very annoying. Here’s how I like to do it, using $\alpha = [g] = [X^2 + 1]$ in $\mathbb{Q}[X]/(X^3 - 2)$ as an example.

Suppose $f \in F[X]$ is irreducible of degree $n$, and I want to compute $[g]^{-1} \in F[X]/(f)$. The idea is to construct a bunch of expressions of the form $r_k := s_kf + X^kg$ with deg $r_k < n$, for all $k = 0, \ldots, n - 1$, with $s_k \in F[X]$. Then do linear algebra to solve for $c_k \in F$ for such that $\sum_{k=0}^{n-1} c_k(s_kf + X^kg) = 1$. Then $[g]^{-1}$ is represented by $\sum_k c_kX^k$. (If you can’t solve the linear system, that’s because $[g] = [0]$.)

Get the $r_k$ by using polynomial long division $(X^kg) \div f$. In the example this gives 

Now we need to find $c_k \in \mathbb{Q}$ such that 

Collecting coefficients we get: 

This gives $c_0 = 1/5$, $c_1 = 2/5$, $c_2 = -1/5$.

Note: as we will see, this $K$ is really the same as $\mathbb{Q}(\sqrt[3]{2})$. Thus, the above actually provides a method for computing multiplicative inverses in $\mathbb{Q}(\sqrt[3]{2})$. So $(1 + \sqrt[3]{4})^{-1} = (1 + 2\sqrt[3]{2} - \sqrt[3]{4})/5$.

Proof. Suppose $R$ is a field, and suppose $f = gh$ in $K[X]$ with deg $g$, deg $h < \deg f$. Then in $R$ we have $[0] = [f] = [gh] = [g][h]$. Since $R$ is a field, then either $[g] = [0]$ or $[h] = [0]$, i.e., either $f \mid g$ or $f \nmid h$ in $K[X]$. But this is impossible by degree reasons, so $f$ is irreducible.

Now suppose $f$ is irreducible. If $[g] \neq [0]$ in $R$, then $f \nmid g$. Therefore $f$ and $g$ have no common factors other than units, so there exist $m, n \in K[X]$ such that $1 = mf + ng$, which implies $[n][g] = [1]$ in $K[X]$.

Let $f \in K[X]$ be irreducible, and $L := K[X]/(f)$. Then there is an injective homomorphism $\iota: K \to L$ by $\iota(a) = a$ (send an element to the constant polynomial). Thus $L = K[X]/(f)$ is a field extension of $K$, and is actually a simple extension, generated by $[X] \in L$.

M 16 Sep
In this case nothing needs to be fixed.

**Remark.** Formally, the general method for computing \([g]^{-1}\) in \(K = F[X]/(f)\) looks like this. For each \(j = 0, \ldots, n - 1\) with \(n = \deg f\) compute the remainders \(r_j\) of \((X^j g) \div f\), which have the form \(l_j = \sum_{i=0}^{n-1} a_{ij} X^i\). Then solve the linear system

\[
\begin{bmatrix}
a_{00} & a_{01} & \cdots & a_{0,n-1} \\
a_{10} & a_{11} & \cdots & a_{1,n-1} \\
\vdots & \vdots & \ddots & \vdots \\
a_{n-1,0} & a_{n-1,1} & \cdots & a_{n-1,n-1}
\end{bmatrix}
\begin{bmatrix}
c_0 \\
c_1 \\
\vdots \\
c_{n-1}
\end{bmatrix}
= \begin{bmatrix} 1 \\
0 \\
\vdots \\
0 \end{bmatrix}
\]

Then \([g]^{-1} = [h]\) with \(h = \sum c_k X^k\).

The idea is: \(K\) is an \(n\)-dimensional \(F\) vector space with basis \([1], [X], \ldots, [X^{n-1}]\). The matrix \((a_{i,j})\) represents multiplication by \([g]\) in terms of this basis.

**23. Classification of simple extensions**

Suppose given two extensions \(\iota: F \to K\) and \(\iota': F' \to K'\). An isomorphism between the two extensions will be a pair of isomorphisms \(\lambda: F \to F'\) and \(\mu: K \to K'\) of fields such that \(\iota' \circ \lambda = \mu \circ \iota\).

\[
\begin{array}{ccc}
K & \xrightarrow{\mu} & K' \\
\iota & & \iota' \\
F & \xleftarrow{\sim} & F'
\end{array}
\]

I’ll say the extensions are isomorphic if such a thing exists.

This is the definition given in Chapter 4. It is the most general possible definition, and we sometimes need it.

We usually use a special case. Given two extensions \(\iota: F \to K\) and \(\iota': F \to K'\) of \(F\), an isomorphism over \(F\) is an isomorphism \(\mu: K \to K'\) such that \(\mu \circ \iota = \iota'\).

\[
\begin{array}{ccc}
K & \xrightarrow{\mu} & K' \\
\iota & & \iota' \\
F & \xleftarrow{\sim} & F'
\end{array}
\]

Here is the big theorem (Theorem 5.11 in the book).

**Proposition.** Let \(F \subseteq K = F(\alpha)\) be a simple extension. Then

- If \(\alpha\) is transcendental over \(F\), then this extension is isomorphic over \(F\) to \(F \subseteq F(X)\). In fact, there is a unique isomorphism \(F(X) \xrightarrow{\sim} K\) sending \(X \mapsto \alpha\).
- If \(\alpha\) is algebraic over \(F\), then this extension is isomorphic over \(F\) to \(F \subseteq F[X]/(f)\), where \(f = f_{\alpha/F}\) is the minimal polynomial of \(\alpha\). In fact, there is a unique isomorphism \(F[X]/(f) \xrightarrow{\sim} K\) sending \(X \mapsto \alpha\).

**Example.** We have an isomorphism over \(\mathbb{Q}\) of the form:

\[\mathbb{Q}[X]/(X^2 - 2) \xrightarrow{\sim} \mathbb{Q}(\sqrt{2}), \quad [X] \mapsto \sqrt{2}.\]

In fact, this sends \([g] \mapsto g(\sqrt{2})\).

Note that there is another, different, isomorphism over \(\mathbb{Q}\), which sends \([X] \mapsto -\sqrt{2}\). These are the only two isomorphisms, since \(\pm \sqrt{2}\) are the only two roots of \(X^2 - 2 = 0\).
Example. We have an isomorphism over \( \mathbb{Q} \) of the form:

\[
\mathbb{Q}[X]/(X^3 - 2) \cong \mathbb{Q}(\sqrt[3]{2}), \quad [X] \mapsto \sqrt[3]{2}.
\]

In fact, this sends \([g] \to g(\sqrt[3]{2})\).

This implies that \( \mathbb{Q}(\sqrt[3]{2}) = \{ a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q} \} \) as asserted earlier, since \( X^3m + k \mapsto \sqrt[3]{2}^{3m+k} = 2^{1/3}\sqrt[3]{2}^k \) so the RHS contains the image of the isomorphism.

Example. Since \( \pi \) is transcendental, we have \( \mathbb{Q}(X) \cong \mathbb{Q}(\pi) \). This sends \( f \in \mathbb{Q}(X) \) to \( f(\pi) \).

Proof. Let \( \phi : F[X] \to K \) be the function sending

\( f(X) \mapsto f(\alpha) \).

This is a ring homomorphism (because \((f + g)(\alpha) = f(\alpha) + g(\alpha)\) and \((fg)(\alpha) = f(\alpha)g(\alpha)\)). In fact, it is the unique ring homomorphism sending \( X \) to \( \alpha \).

Now there are two cases.

1. If \( \alpha \) is transcendental, then \( f(\alpha) = 0 \) only when \( f \in F[X] \) is the zero polynomial. Thus, \( \phi \) is injective.

   Now define \( \psi : F(X) \to K \) by

   \[
   \left[ \frac{g(X)}{h(X)} \right] \mapsto \frac{g(\alpha)}{h(\alpha)}, \quad g, h \in F[X].
   \]

   Note that \( h(\alpha) \neq 0 \) as long as \( h \neq 0 \) since \( \alpha \) is transcendental. Check that the above is well-defined: if \( \left[ \frac{g}{h} \right] = \left[ \frac{g'}{h'} \right] \) then \( gh' = g'h \), whence \( g(\alpha)h'(\alpha) = g'(\alpha)h(\alpha) \), so \( \frac{g(\alpha)}{h(\alpha)} = \frac{g'(\alpha)}{h'(\alpha)} \).

   Next check that \( \psi \) is a ring homomorphism: this is straightforward so I won’t write it out.

   Thus \( \psi : F(X) \to K \) is a homomorphism of fields, so injective. It’s image is a subfield of \( K \) containing \( F \) and \( \alpha \), and since \( K = F(\alpha) \) we see \( \psi \) is also surjective.

2. If \( \alpha \) is algebraic with minimal polynomial \( f = f_{\alpha/F} \), then the kernel of \( \phi \) is

   \[
   I = \ker \phi = \{ g \in F[X] \mid g(\alpha) = 0 \} = \{ hf \mid h \in F[X] \} = (f),
   \]

   the principal ideal generated by \( f \). Thus, by the “isomorphism theorem” for rings, there is a unique ring homomorphism

   \[
   \psi : F[X]/(f) \to K
   \]

   such that \( \psi([g]) = \phi(g) \), i.e., \( \psi[g(X)] = g(\alpha) \). It is clear that \( \psi \) is injective. It is also surjective since the image \( \psi(F[X]/(f)) \) is a subfield of \( K \) containing \( F \) and \( \alpha \).

\[\square\]

24. Degree of an Extension

Given a field homomorphism \( \iota : F \to K \), then \( K \) has the structure of a vector space over \( F \): addition is addition, scalar multiplication is \( c \cdot v := \iota(c)v \).

The degree of the extension \( \iota : F \to K \) is the dimension of \( K \) as an \( F \) vector space. Note that this dimension can be infinite. We write

\[
[K : F] = \dim_F K \in \mathbb{Z}_{\geq 1} \cup \{ \infty \}.
\]

A finite extension is one where \([K : F] < \infty \). If \([K : F] = n \), this means there exists a basis \( \alpha_1, \ldots, \alpha_n \in K \) over \( F \) of size \( n \). Therefore, every \( \beta \in K \) can be written as

\[
\beta = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n, \quad c_n \in F
\]

for a unique choice of \( c_1, \ldots, c_n \).

For instance, \([\mathbb{C} : \mathbb{R}] = 2\), \([\mathbb{R} : \mathbb{Q}] = \infty \) (in fact, uncountably infinite). Also \([\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4\) and \([\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 3\).
Remark. Suppose we have field extensions $K \subseteq L$.

Example. Let $\alpha \in K$. We have $K(\alpha)$. This is because $f(\alpha) = 0$. By writing this as $0 = \sum_j b_j x_i y_j$, we see that linear independence of $\{x_i\}$ over $K$ implies all $b_j = 0$, so $0 = \sum_i a_{ij} x_i$, and then linear independence of $\{x_i\}$ over $F$ implies all $a_{ij}$ are linearly independent.

Proposition (Tower law). If $F \subseteq K \subseteq L$ are subfields, then $[L : F] = [L : K][K : F]$.

Proof. Let $\{x_i\}$ be an $F$-basis of $K$, and $\{y_j\}$ a $K$-basis of $L$. We show that $S = \{x_i y_j\}$ is an $F$-basis of $L$. (Note: I am allowing these bases to be infinite if necessary.)

First we show $S$ spans $L$ over $F$. Given $c \in L$, we can write $c = \sum b_j y_j$ with the $b_j \in K$ and all but finitely many terms 0, because $\{y_j\}$ spans $L$ over $K$. Likewise for each $b_j \in K$ we can write $b_j = \sum a_{ij} x_i$ with $a_{ij} \in F$ and all but finitely many terms 0, because $\{x_i\}$ spans $K$ over $F$. Then

$$c = \sum_j b_j y_j = \sum_j \sum_i a_{ij} x_i y_j$$

which is a sum with finitely many terms, with $a_{ij} \in F$. Thus $\{x_i y_j\}$ spans $L$ over $F$.

Now we show linear independence. Suppose we have a sum $\sum_{i,j} a_{ij} x_i y_j = 0$, where $a_{ij} \in F$ with all but finitely many terms 0. By writing this as

$$0 = \sum_j \left( \sum_i a_{ij} x_i \right) y_j = \sum_j b_j y_j, \quad b_j := \sum_i a_{ij} x_i \in K,$$

we see that linear independence of $\{y_j\}$ over $K$ implies all $b_j = 0$, so $0 = \sum_i a_{ij} x_i$, and then linear independence of $\{x_i\}$ over $F$ implies all $a_{ij}$ is 0.

Corollary (General tower law). If $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = L$, then $[L : F] = [K_r : K_{r-1}] \cdots [K_1 : K_0]$.

Remark. Suppose we have field extensions $F \subseteq K \subseteq L$ and $\alpha \in L$. We get field extensions

$$\begin{align*}
K(\alpha) & \xrightarrow{\text{inclusion}} K \\
F(\alpha) & \xrightarrow{\text{inclusion}} F \\
\end{align*}$$

The tower law says that $[K(\alpha) : F] = [K(\alpha) : K][K : F] = [K(\alpha) : F(\alpha)][F(\alpha) : F]$. Note if $\alpha$ is algebraic we only know that

$$[K(\alpha) : K] \leq [F(\alpha) : F].$$

This is because $f_{\alpha/K}$ divides $f_{\alpha/F}$ in $K[X]$, but they might not be equal.

Example. Let $\alpha = \sqrt[3]{2} \in \mathbb{R}$ and $\omega = e^{2\pi i/3} \in \mathbb{C}$. We have

$$\begin{align*}
\mathbb{Q}(\alpha) & \xrightarrow{\text{inclusion}} \mathbb{Q}(\sqrt[3]{2}) \\
\mathbb{Q}(\alpha, \omega) & \xrightarrow{\text{inclusion}} \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}) \\
\mathbb{Q}(\alpha) & \xrightarrow{\text{inclusion}} \mathbb{Q}(\omega) \\
\end{align*}$$

We have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3 = [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}]$ because $\alpha$ and $\alpha \omega$ are roots of the same irreducible $X^3 - 2$ over $\mathbb{Q}$. Since $\alpha \omega \notin \mathbb{R}$ it is not in $\mathbb{Q}(\alpha)$, so $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)] \geq 2$. But $X^3 - 2 = (X - \alpha)(X^2 + \alpha X + \alpha)$ over $\mathbb{Q}(\alpha)$, so the degree is at most 2.
Example. Let $K = \mathbb{Q}(\sqrt{7}, i) \subseteq \mathbb{C}$. Using $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{7}) \subseteq K$, we have

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt{7}, i) : \mathbb{Q}(\sqrt{7})][\mathbb{Q}(\sqrt{7}) : \mathbb{Q}].$$

Since $\sqrt{7}$ is irrational, $f_{\sqrt{7}/\mathbb{Q}} = X^2 - 7$, so $[\mathbb{Q}(\sqrt{7}) : \mathbb{Q}] = 2$. We know that $f_i/\mathbb{Q} = X^2 + 1$, however to compute $[\mathbb{Q}(\sqrt{7}, i) : \mathbb{Q}(\sqrt{7})]$ we need $f_i/\mathbb{Q}(\sqrt{7})$, which we only know divides $f_i/\mathbb{Q}$. In this case, we have an easy trick: $i$ is not a real number, but $\mathbb{Q}(\sqrt{7}) \subseteq \mathbb{R}$, so $i \notin \mathbb{Q}(\sqrt{7})$. Thus $[\mathbb{Q}(\sqrt{7}, i) : \mathbb{Q}(\sqrt{7})] = 2$. So $[K : \mathbb{Q}] = 4$.

25. COMPOSITE SUBFIELDS

Consider the following diagram of field extensions:

```
        M
       / \  \
      /   \ /
     /     F
    /  \  /  \
   K    L
```

The **composite subfield** of $K$ and $L$ is the smallest subfield of $M$ containing $K$ and $L$. It is sometimes denoted $KL$. It is exactly the subfield of $M$ generated by the elements of $K$ and $L$.

**Example.** If $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_r)$ and $L = \mathbb{Q}(\beta_1, \ldots, \beta_s)$, then $KL = \mathbb{Q}(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s)$.

**Proposition.** If $K, L \subseteq M$ are subfields with $F \subseteq K \cap L$, and if $K : F$ is a finite extension, then

$$[KL : L] \leq [K : F].$$

**Proof.** We have already observed the special case of $K = F(\alpha)$ with $\alpha$ algebraic, in which case $KL = L(\alpha)$, and $[L(\alpha) : L] \leq [F(\alpha) : F]$, which we see by comparing the degrees of $f_{\alpha/F}$ and $f_{\alpha/L}$.

For a general finite extension $K : F$ there is a tower

$$F \subseteq F(\alpha_1) \subseteq \cdots \subseteq F(\alpha_1, \ldots, \alpha_r) = K,$$

and therefore a tower

$$L \subseteq L(\alpha_1) \subseteq \cdots \subseteq L(\alpha_1, \ldots, \alpha_r) = KL.$$  

The case of simple extensions gives

$$[L(\alpha_1, \ldots, \alpha_j) : L(\alpha_1, \ldots, \alpha_{j-1}) \subseteq [F(\alpha_1, \ldots, \alpha_j) : F(\alpha_1, \ldots, \alpha_{j-1})],$$

and the tower law gives the desired result. 

26. ALGEBRAIC EXTENSIONS AND ALGEBRAIC CLOSURE

An extension $[K : F]$ is **algebraic** if every element of $K$ is algebraic over $F$.

**Proposition.** Every finite extension is algebraic.

**Proof.** Let $K : F$ be a finite extension and $\alpha \in K$. Then the tower law applied to $F \subseteq F(\alpha) \subseteq K$ implies that $[F(\alpha) : F] < \infty$. As a vector space of $F$, the field $F(\alpha)$ is spanned by all powers of $\alpha$: $\{ \alpha^k \mid k \geq 0 \}$. Since $\dim_F F(\alpha) < \infty$, this spanning set is not linearly independent, so there exists a linear dependence $\sum_{k=0}^{m} c_k \alpha^k$ with $c_0, \ldots, c_m \in F$ not all zero. This gives a polynomial over $F$ which has $\alpha$ as a root, so $\alpha$ is algebraic.

The converse is not true: there are algebraic extensions which are not finite. I will give an example.

Let $\mathbb{Q}^{\text{alg}} := \{ \alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q} \}$, the set of algebraic numbers.

**Proposition.** The set $\mathbb{Q}^{\text{alg}}$ of algebraic numbers is a subfield of $\mathbb{C}$, and $[\mathbb{Q}^{\text{alg}} : \mathbb{Q}] = \infty$.

**Proof.** To show $\mathbb{Q}^{\text{alg}}$ is a subfield, I need to show that if $\alpha, \beta \in \mathbb{Q}^{\text{alg}}$, then $\alpha + \beta, \alpha \beta, -\alpha, \alpha^{-1} \in \mathbb{Q}^{\text{alg}}$. 

• Clearly \(-\alpha, \alpha^{-1} \in \mathbb{Q}(\alpha)\), and so are algebraic since \(\mathbb{Q}(\alpha) : \mathbb{Q}\) is algebraic.
• We have \(\alpha + \beta, \alpha\beta \in \mathbb{Q}(\alpha, \beta)\), and so are algebraic since
\[
[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq [\mathbb{Q}(\beta) : \mathbb{Q}] [\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty.
\]

It is obvious that \(\mathbb{Q}^{\text{alg}} \subseteq \mathbb{Q}\) is algebraic. To show that it has infinite degree, it suffices to find subfields \(K \subseteq \mathbb{Q}^{\text{alg}}\) with \([K : \mathbb{Q}]\) finite but arbitrarily large. For instance, you can show that if \(p_1, \ldots, p_r\) are distinct prime numbers, then \([\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_r}) : \mathbb{Q}] = 2^r\) (see Exc. 6.14 in the book).

You can also describe \(\mathbb{Q}^{\text{alg}}\) as an intersection of subfields.

**Proposition.** \(\mathbb{Q}^{\text{alg}} = \bigcap_{K \subseteq \mathbb{C}} K\), where \(\mathbb{C}\) is the collection of all subfields of \(\mathbb{C}\) which are algebraically closed fields (i.e., Irred(\(\mathbb{K}\)) consists only of polynomials of degree 1).

**Proof.** Let \(L\) be the intersection of all algebraically closed subfields of \(\mathbb{C}\). It is easy to see that \(\mathbb{Q}^{\text{alg}}\) is contained in every algebraically closed subfield, so \(\mathbb{Q}^{\text{alg}} \subseteq L\).

To show that \(L \subseteq \mathbb{Q}^{\text{alg}}\), its enough to show that \(\mathbb{Q}^{\text{alg}}\) is itself algebraically closed. Let \(f \in \mathbb{Q}^{\text{alg}}[X]\) of degree \(\geq 1\), and let \(\alpha \in \mathbb{C}\) be a root of \(f\). I will show that \(\alpha \in \mathbb{Q}^{\text{alg}}\).

Write \(f = \sum_{j=0}^n c_j X^j\) with \(c_j \in \mathbb{Q}^{\text{alg}}\). Each \(c_j\) is thus algebraic over \(\mathbb{Q}\), and so \(c_0, \ldots, c_{n-1} \in K := \mathbb{Q}(c_0, \ldots, c_{n-1})\), which is a finite extension over \(\mathbb{Q}\).

For any root \(\alpha \in \mathbb{C}\) of \(f\), we have \([K(\alpha) : K] \leq \deg f\), and thus by the tower law \(K(\alpha) : \mathbb{Q}\) is a finite extension. But we proved that \(\mathbb{Q}^{\text{alg}}\) is the union of such extensions, so \(\alpha \in K(\alpha) \subseteq \mathbb{Q}^{\text{alg}}\).

\[\square\]

27. 2-RADICAL EXTENSIONS AND SQUARE ROOT CLOSURE

Algebraic numbers are what you get when you solve arbitrary polynomial equations over \(\mathbb{Q}\). Let’s think about what happens if you just allow solutions of quadratic equations.

Solving quadratic equations is basically the same as solving square roots, at least in the complex numbers.

**Lemma.** If \(K \subseteq L\) are subfields of \(\mathbb{C}\) with \([L : K] = 2\), then \(L = K(\sqrt{d})\) for some \(d \in K\).

**Proof.** Because \([L : K] = 2\), we have \(L \cong_K K[X]/(f)\) for some \(f = X^2 + bX + c \in \text{Irred}(K)\). From the quadratic formula we see that we can take \(d = b^2 - 4c\).

Say that an extension of fields \(K \subseteq L\) is 2-

**radical** if there exists a finite tower of subfields

\[K = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_r = L\]

such that \([L_j : L_{j-1}] = 2\). Note that \([L : \mathbb{Q}] = 2^r\).

**Example.** Consider

\[\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{\sqrt{2}}) \subseteq \mathbb{Q}(\sqrt{\sqrt{\sqrt{2}}}) \subseteq \cdots\]

You can show that each intermediate extension has degree 2.

**Example.** Consider

\[\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{1 + \sqrt{2}}) \subseteq \mathbb{Q}(\sqrt{1 + \sqrt{1 + \sqrt{2}}}) \subseteq \mathbb{Q}(\sqrt{1 + \sqrt{1 + \sqrt{1 + \sqrt{2}}}}) \subseteq \cdots\]

Can you prove that these extensions are all degree 2? I.e., that \(\sqrt{1 + \sqrt{2}} \notin \mathbb{Q}(\sqrt{2})\), etc.

Note that if \(L : K\) and \(K : F\) are both 2-

**radical**, then so is \(L : F\).

**Proposition.** If \(K, L \subseteq \mathbb{C}\) are 2-

**radical** over \(\mathbb{Q}\), then so is the composite extension \(KL : \mathbb{Q}\).
Proof. Consider towers \( \mathbb{Q} = K_0 \subseteq \cdots \subseteq K_r = K \) and with \( [K_i : K_{i-1}] = 2 \). Then there is a tower \( L = K_0 L \subseteq K_1 L \subseteq \cdots \subseteq K_r L = KL \), with \( [K_i L : K_{i-1} L] \leq [K_i : K_{i-1}] = 2 \). After discarding the \( K_i L \) which are equal to \( K_{i-1} L \), we get a chain of extensions between \( L \) and \( KL \) where every step has degree 2. Thus \( KL : L \) is 2-radical, and hence \( KL : \mathbb{Q} \) is 2-radical. \( \square \)

Say that a field \( K \) is squareroot closed if every element of \( K \) has a squareroot in \( K \); that is, if every polynomial of the form \( X^2 - a = 0 \) with \( a \in K \) has a root in \( K \). We usually just say this as: \( \pm \sqrt{a} \in K \) for all \( a \in K \). Note: if \( K \subseteq \mathbb{C} \), then \( K \) is squareroot closed iff every quadratic polynomial over \( K \) has a root in \( K \), by the quadratic formula.

Define \( \mathbb{Q}^{\sqrt{\cdot}} \) to be\footnote{Stewart calls this the “pythagorean closure”, see remark below.} the intersection of all squareroot closed subfields of \( \mathbb{C} \). It is clearly a squareroot closed subfield.

**Proposition.** A complex number is in \( \mathbb{Q}^{\sqrt{\cdot}} \) iff there exists a finite 2-radical extension \( K : \mathbb{Q} \) with \( \alpha \in K \).

Proof. Let \( L := \) the union of all subfields \( K \subseteq \mathbb{C} \) which are finite 2-radical extensions of \( \mathbb{Q} \). We want to show that \( L = \mathbb{Q}^{\sqrt{\cdot}} \). We do this by showing that \( L \) is a subfield of \( \mathbb{Q}^{\sqrt{\cdot}} \) which is squareroot closed.

It is clear that any 2-radical \( K : \mathbb{Q} \) is contained in \( \mathbb{Q}^{\sqrt{\cdot}} \), so \( L \subseteq \mathbb{Q}^{\sqrt{\cdot}} \).

Next we show that \( L \) is a subfield. If \( \alpha, \beta \in L \), then there exist 2-radical \( K, K' \) over \( \mathbb{Q} \) such that \( \alpha \in K \) and \( \beta \in K' \), whence \( \alpha + \beta, \alpha \beta, -\alpha, \alpha^{-1} \in KK' \). We have proved that the composite \( KK' \) is also 2-radical, so \( KK' \subseteq L \). Thus \( L \) is a subfield.

Finally, we show that \( L \) is squareroot closed. Suppose \( a \in L \); I want to show \( \sqrt{a} \in L \). Since \( L \) is a union of finite 2-radical extensions of \( \mathbb{Q} \), there exists a 2-radical \( K : \mathbb{Q} \) with \( a \in K \). Thus \( \sqrt{a} \in K(\sqrt{a}) \), which is itself 2-radical over \( \mathbb{Q} \), so \( K(\sqrt{a}) \subseteq L \) as desired. \( \square \)

**Remark.** Stewart calls the squareroot closure the “pythagorean closure” of \( \mathbb{Q} \), and writes it as \( \mathbb{Q}^{Py} \). However, that term has a different standard meaning (as you will see if you check it on wikipedia), so I won’t use it.

Also, the proof of Theorem 7.11 as given the book is simply incorrect. This theorem asserts: a complex number \( \alpha \) is in \( \mathbb{Q}^{\sqrt{\cdot}} \) iff \( \mathbb{Q}(\alpha) : \mathbb{Q} \) is a 2-radical extension. This is a true fact, but is surprisingly hard to prove given what we have so far. (We will be able to prove it later.)

One problem with his proof is that he assumes that every \( \alpha \in \mathbb{Q}^{\sqrt{\cdot}} \) is contained in some finite 2-radical extension over \( \mathbb{Q} \), but does not prove it. The proof I gave above fills that gap.

The more serious gap in Stewart’s proof of 7.11 is the claim that “either \( M_{j+1} = M_j \) or \( \dim M_{j+1} = 2 \dim M_j \)”. Basically, he has a situation of the form

\[
\begin{align*}
L_{j-1} & \quad 2 \quad L_j \quad \quad M_j \\
& \quad \quad M_{j-1} = L_{j-1} \cap M_j
\end{align*}
\]

and wants to show that \( [L_j : L_{j-1}] = 2 \) implies \( [M_j : M_{j-1}] \leq 2 \). But this is not justified, and is not true in general.

We do have the following.

**Proposition.** If \( \alpha \in \mathbb{Q}^{\sqrt{\cdot}} \) then \( [\mathbb{Q}(\alpha) : \mathbb{Q}] \) is a power of 2.

Proof. If \( \alpha \in \mathbb{Q}^{\sqrt{\cdot}} \) then \( \alpha \in K \) for some 2-radical extension \( K : \mathbb{Q} \). Since \( \mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq K \), the tower lemma gives \( 2^n = [K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \), so \( [\mathbb{Q}(\alpha) : \mathbb{Q}] \) is a power of 2. \( \square \)

The converse is not true: there exist \( \alpha \in \mathbb{Q}^{\text{alg}} \) such that \( [\mathbb{Q}(\alpha) : \mathbb{Q}] \) is a power of 2 but \( \alpha \notin \mathbb{Q}^{\sqrt{\cdot}} \).
28. RULER AND COMPASS CONSTRUCTIONS

A famous application of what we have learned is to the insolvability of certain geometric constructions by “ruler and compass”.

In the setting of ruler and compass constructions, you have some set of points \( \mathcal{P} \) in the plane. You are allowed to:

- draw a line between any two distinct points (“ruler”), and
- draw a circle with center at an element of \( \mathcal{P} \) with radius \( r = \) the distance between any two given points in \( \mathcal{P} \) (“compass”).

Given these, you are allowed to have a bigger set of points \( \mathcal{P}' \), which contains all elements of \( \mathcal{P} \) as well as: any point which is the intersection of two lines, line and circle, or two circles that you drew.

Given this, you can carry out some basic constructions, such as bisecting a line segment or angle. The ancient Greeks knew you could also trisect a line segment, but did not know how to trisect an angle. It turns out that this is because it is impossible to do so.

We can formalize this as follows. Identify the plane with \( \mathbb{C} \), and suppose we are given two points in the plane to start with, which we identify with 0 and 1. Say that \( z \in \mathbb{C} \) is constructible if there exists a sequence of elements \( \alpha \) in the plane to start with, which we identify with 0 and 1. Say that \( z \in \mathbb{C} \) is constructible iff \( z \in \mathbb{Q}^{\text{sqrt}} \).

The proof is kind of involved: see Chapter 7 in the book (where \( \mathbb{Q}^{\text{sqrt}} \) is called \( \mathbb{Q}^{\text{by}} \)). There are two parts of the proof.

1. Show how to carry out all the field operations in \( \mathbb{C} \) using ruler and compass constructions, and also how to compute square roots. This shows all elements of \( \mathbb{Q}^{\text{sqrt}} \) are constructible.

2. Show that all constructible points are in \( \mathbb{Q}^{\text{sqrt}} \). To see this you use the fact that computing intersection points of lines and/or circles involves solving polynomial equations of degree at most 2.

Here are several impossibility results that follow from this, using the facts that constructible \( \alpha \) are algebraic with \( [\mathbb{Q}(\alpha) : \mathbb{Q}] \) a power of 2.

- **Cannot duplicate the cube.** Basically, given a line segment of length \( r \), produce one of length \( r \sqrt[3]{2} \). (I.e., if you have a cube, produce one with twice the volume.) Equivalently, construct \( \alpha = \sqrt[3]{2} \). But \( [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \).

- **Cannot trisect every angle.** In particular, \( \theta = 2\pi/3 \) cannot be trisected. This amounts to showing that \( \zeta = e^{2\pi i/9} \) is not constructible. Note that \( \zeta \) is a root of \( \Phi_9 = X^6 + X^3 + 1 = 0 \), so \( \zeta^6 + \zeta^3 + 1 = 0 \), or equivalently \( \zeta^3 + \zeta^{-3} = -1 \).

  Let \( \alpha = \zeta + \zeta^{-1} \in \mathbb{Q}(\zeta) \). We can compute
  \[
  \alpha^3 = \zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3} = 3\alpha - 1.
  \]

  So \( \alpha \in \mathbb{Q}(\zeta) \) is a root of \( g = X^3 - 3X + 1 \). By the rational roots test \( g \) is irreducible over \( \mathbb{Q} \), so \( f_{\alpha/\mathbb{Q}} = g \), so \( [\mathbb{Q}(\alpha) : \mathbb{Q}] = 3 \), whence \( [\mathbb{Q}(\zeta) : \mathbb{Q}] \) is divisible by 3.

- **Cannot square the circle.** That is, given a circle you cannot construct a square with the same area. If the circle has radius \( r \), so area \( \pi r^2 \), we want a square with side \( \sqrt{\pi}r \), so we show \( \sqrt{\pi} \) is not constructible. If it is constructible, then \( \pi \in \mathbb{C}(\sqrt{\pi}) \) would be algebraic, which it is not by Lindemann’s theorem.
• Cannot construct the regular heptagon. Amounts to showing $\zeta = e^{2\pi i/7}$ is not-constructible. We have shown that $\Phi_7 = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ is irreducible over $\mathbb{Q}$, so $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 6$ which is not a power of 2.

**Remark.** If $p$ is a prime number, then $\zeta_p = e^{2\pi i/p}$ satisfies

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \deg \Phi_p = p - 1,$$

because $\Phi_p = \sum_{k=0}^{p-1} X^k$ is irreducible over $\mathbb{Q}$ using Eisenstein’s criterion. Thus it is impossible to construct a regular $p$-gon for a prime number $p$ unless it has the form $p = 2^m + 1$. These are the Fermat primes, of which examples are

$$3 = 2^1 + 1, \quad 5 = 2^2 + 1, \quad 17 = 2^4 + 1, \quad 257 = 2^8 + 1, \quad 65537 = 2^{16} + 1.$$  

Construction of regular triangles and pentagons was known classically. The next prime not excluded by what we have shown is 17. Gauss showed that $\zeta_{17}$ is in fact constructible, and actually produced a ruler-and-compass construction of a regular 17.

It turns out that $\zeta_p$ is constructible for any Fermat prime. Note that Fermat primes must actually have the form $2^d + 1$ for some $d$ (this is because $a + 1$ divides $a^k + 1$ whenever $k$ is odd). The only known Fermat primes are the ones I listed above; for instance $2^{32} + 1$ is composite.

### 29. Idea of Galois Theory

Fix a subfield $F \subseteq \mathbb{C}$ of the complex numbers and a polynomial $f \in F[X]$. Let $\alpha_1, \ldots, \alpha_r \in \mathbb{C}$ be the roots of $f$. This means that $f$ factors over $\mathbb{C}$ as

$$f = (X - \alpha_1)^{d_1} \cdots (X - \alpha_r)^{d_r}, \quad d_1, \ldots, d_r \geq 1.$$  

Notice that $r \leq \deg f$, but equality need not hold.

Associated to any such polynomial is a Galois group $G$. This will be a subgroup of $S_n$, the symmetric group of the set $\{1, \ldots, n\}$. The idea is that elements $\sigma \in G$ are permutations which “preserve all expressions over $F$ involving the roots”.

**Example.** $F = \mathbb{Q}$ and $f = (X^2 + 1)(X^2 - 5) = X^4 - 4X^2 - 5$. This quartic polynomial comes pre-factored into irreducible-over-$\mathbb{Q}$ factors. The roots are

$$\alpha_1 = i, \quad \alpha_2 = -i, \quad \alpha_3 = \sqrt{5}, \quad \alpha_4 = -\sqrt{5}.$$  

An element of $\sigma \in S_4$ acts on the set $R = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ by $\sigma(\alpha_k) := \alpha_{\sigma(k)}$. For instance:

$$\sigma = (1 2)(3 4) \implies \sigma(i) = -i, \quad \sigma(-i) = i, \quad \sigma(\sqrt{5}) = -\sqrt{5}, \quad \sigma(-\sqrt{5}) = \sqrt{5}.$$  

$$\gamma = (1 2 3) \implies \gamma(i) = -i, \quad \gamma(-i) = \sqrt{5}, \quad \gamma(\sqrt{5}) = i, \quad \gamma(-\sqrt{5}) = -\sqrt{5}.$$  

We can to extend this action to any “formula” involving the roots. For instance we would expect

$$\sigma(3 + 5i - 2\sqrt{5}) = 3 + 5(-i) - 2(-\sqrt{5}), \quad \gamma(3 + 5i - 2\sqrt{5}) = 3 + 5(\sqrt{5}) - 2\sqrt{5}.$$  

There is a problem with $\gamma$: applied to both sides of the equation $(\sqrt{5})^2 - 5 = 0$ you get different answers: $(i)^2 - 5 \neq 0$. However there is no such problem with $\sigma$: applied to $(\sqrt{5})^2 - 5 = 0$ you get $(-\sqrt{5})^2 - 5 = 0$.

It turns out that $G = \{e, (1 2), (3 4), (1 2)(3 4)\}$, which is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$. (This analysis is a bit hand-wavy. We'll be able to do it more carefully once we have set up a few things.)

**Example.** $F = \mathbb{Q}$ and $f = \Phi_5 = X^4 + X^3 + X^2 + X + 1$. Here the four roots are $\{\alpha_1 = \zeta, \alpha_2 = \zeta^2, \alpha_3 = \zeta^3, \alpha_4 = \zeta^4\}$, with $\zeta = e^{2\pi i/5}$. Note that we have identities among the roots such as $\alpha^2 = \alpha_j$. Thus for each integer $k$ not divisible by 5 we have $\sigma_k \in G$ defined by $\sigma_k(\zeta^i) = \zeta^j$, and $\sigma_k = \sigma_{kj}$ if $k \equiv k' \mod 5$. It turns out that $G = \{e, \sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ with group structure $\sigma_j \sigma_k = \sigma_{jk}$, which is a cyclic group: as a subgroup of $S_4$ it is generated by $\sigma_2 = (1 2 4 3)$. (It is isomorphic to $(\mathbb{Z}/5)^\times$, the multiplicative group of units in the field of integers modulo 5.)
The way to make the definition of $G$ be rigorously correct is to let $G$ be a group of automorphisms of the field $F = F(\alpha_1, \ldots, \alpha_n)$, obtained by adjoining all roots of $f$. The automorphisms will be identity on elements of the subfield $F$.

For every subgroup $H \leq G$ let

$$H^1 = L^H := \{ a \in L \mid \sigma(a) = a \forall a \in H \}$$

be the set of elements fixed by elements of $H$. This subset is a subfield containing $F$; i.e., $L^H$ is an intermediate field of $L : F$ (which just means $F \subseteq L^H \subseteq L$). The Galois correspondence is says that the rule $H \mapsto L^H : F$ defines a bijective correspondence

$$(\text{subgroups of } G) \leftrightarrow (\text{intermediate fields of } L : F).$$

**Example.** Consider $f = (X^2 + 1)(X^2 - 5)$ over $F = \mathbb{Q}$ as above with roots $(\alpha_1, \ldots, \alpha_4) = (i, -i, \sqrt{5}, -\sqrt{5})$. We have the following diagram illustrating the correspondence of subgroups and fixed fields.

![Diagram of subgroups and fixed fields](image)

**Example.** Consider $f = \Phi_5$ over $F = \mathbb{Q}$ as above with roots $(\alpha_1, \ldots, \alpha_4) = (\zeta, \zeta^2, \zeta^3, \zeta^4)$, $\zeta = e^{2\pi i/5}$. We have the following diagram of subgroups and fixed fields, where $\sigma = \sigma_2 = (1 \ 2 \ 4 \ 3)$ is a generator of $G$.

![Diagram of subgroups and fixed fields](image)

To calculate $K^H$, we can find an element by considering $\alpha := \zeta + \sigma^2(\zeta) = \zeta + \zeta^4 = \zeta + \zeta^{-1}$, which has $\sigma^2(\alpha) = \sigma^2(\zeta) + \zeta = \alpha$. We have $\alpha^2 = \zeta^2 + 2 + \zeta^{-2}$, so $\alpha^2 + \alpha - 1 = 0$, and thus we can compute that $\alpha = (-1 + \sqrt{5})/2$, so $\alpha \notin \mathbb{Q}$. It turns out that $K^H = \mathbb{Q}(\alpha)$.

### 30. Automorphism groups of extensions

An automorphism of a field $L$ is a field homomorphism $\alpha : L \to L$ which is a bijection. This implies that the inverse function is also an automorphism.

Given a field extension $L : F$, an $F$-**automorphism** (or “automorphism over $F$”) is an isomorphism of fields $\psi : L \to L$ such that $\psi(x) = x$ for all $x \in F$.

$$L \xrightarrow{\psi} L$$

$$L \xleftarrow{\psi} F$$

I write $\text{Aut}(L : K)$ for the set of $F$-automorphisms. It is a group under composition.

**Remark.** Stewart calls this $\Gamma(L : K)$, but I find this not memorable. He also calls it “the Galois group”, but this is actually not standard terminology: only *Galois extensions* have a Galois group.

**Example.** $\text{Aut}(\mathbb{C} : \mathbb{R})$ has exactly two elements: identity and complex conjugation. It is easy to see that $\psi \in \text{Aut}(\mathbb{C} : \mathbb{R})$ is completely determined by the value of $\psi(i)$. This is because $\mathbb{C} = \mathbb{R}(i)$.

Since $i^2 = -1$, we must have

$$-1 = \psi(-1) = \psi(i^2) = \psi(i)^2,$$

so $\psi(i)$ is a square-root of $-1$, i.e., $\psi(i) \in \{ \pm i \}$. 

---

W 25 Sep

| **automorphism of extension** | **lecture notes for 428 32** | **32** |
Example. \( \text{Aut}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}) = \{ e \} \) is the trivial group. This is because \( a = \psi(\sqrt{2}) \) satisfies
\[
a^3 = \psi(\sqrt{2})^3 = \psi((\sqrt{2})^3) = \psi(2) = 2.
\]
Thus \( a \) is a cube-root of 2, and since \( a \) must be real, it must be the unique real cube-root.

Example. \( \text{Aut}(\mathbb{R} : \mathbb{Q}) = \{ e \} \) is the trivial group. Here’s a sketch.

Suppose \( \psi \in \text{Aut}(\mathbb{R} : \mathbb{Q}) \). Then \( \psi \) fixes rational numbers. It suffices to show that \( a \leq b \) implies \( \psi(a) \leq \psi(b) \), since a real number is completely determined by which rationals it is greater or less than.

Since a real number is non-negative if and only if it is the square of a real number, we see that
\[
a \leq b \quad \text{if and only if} \quad b - a = c^2 \quad \text{for some} \quad c \in \mathbb{R}.
\]
Since \( \psi(b) - \psi(a) = \psi(b - a) = \psi(c^2) = \psi(c)^2 \), we see that \( a \leq b \) implies \( \psi(a) \leq \psi(b) \).

Example. \( \text{Aut}(\mathbb{C} : \mathbb{Q}) \) is an uncountable group. However, we only know how to construct two elements explicitly. The existence of other elements uses the axiom of choice!

Here is an important observation: if \( L : F \) is a finite extension, then any field homomorphism \( \phi : L \to L \) such that \( \phi|F = \text{id} \) is an isomorphism. This is because the image \( \phi(L) \subseteq L \) is a subfield of \( L \), and because \( L \to \phi(L) \) is an isomorphism it has the same degree over \( F \), i.e., \([\phi(L) : F] = [L : F] \).

We have the following crucial fact.

Proposition. If \( \phi \in \text{Aut}(L : F) \) and \( \alpha \in L \) is a root of \( f \in F[X] \) then \( \phi(\alpha) \) is also a root of \( f \).
That is: automorphisms of \( L : F \) permute roots of any polynomial in \( F[X] \).

Note: I am skipping sections 8.7 and 8.8 of the book for now. I will return to that topic later.

31. Splitting fields

Given a field extension \( K : F \) and polynomial \( f \in F[X] \), we say \( f \) splits over \( K \) if there exist \( c \in F^\times, \alpha_1, \ldots, \alpha_n \in K \) such that
\[
f = c(X - \alpha_1) \cdots (X - \alpha_n).
\]
Here I allow repetition in the list of \( \alpha_i \)s.

For instance, for any \( F \subseteq \mathbb{C} \), every \( f \in F[X] \) splits over \( \mathbb{C} \).

Given a field \( F \) and \( f \in F[X] \), a splitting field \( \Sigma \) is an extension \( \Sigma : F \) such that

1. \( f \) splits over \( \Sigma \), and
2. if \( F \subseteq K \subseteq \Sigma \) and \( f \) splits over \( K \), then \( K = \Sigma \).

In other words, the splitting field is a minimal example of a field over which \( f \) splits.

Example. \( F = \mathbb{Q} \) and \( f = (X^2 + 1)(X^2 - 5) \), then \( \Sigma = \mathbb{Q}(i, \sqrt{5}) \) is a splitting field.

A splitting field for \( f \) is one which “has all the roots of \( f \)” and is generated by those roots.

Lemma. An extension \( \Sigma : F \) is a splitting field of \( f \in F[X] \) if

1. \( f = c(X - \alpha_1) \cdots (X - \alpha_n) \) for some \( c \in F^\times, \alpha_1, \ldots, \alpha_n \in \Sigma \), and
2. \( \Sigma = F(\alpha_1, \ldots, \alpha_r) \).

Proof. Straightforward. \( \square \)

As a consequence: a splitting field is always a finite extension of the ground field, since each \( \alpha_k \) is algebraic over \( F \).

Exercise. If \( \Sigma : F \) is a splitting field of \( f \in F[X] \) with \( n = \deg f \), then \( [\Sigma : F] \) divides \( n! \).

Polynomials over subfields of the complex numbers have unique splitting fields in \( \mathbb{C} \).
Proposition. Let $F \subseteq \mathbb{C}$ be a subfield and $f \in F[X]$. Then there exists a unique subfield $\Sigma \subseteq \mathbb{C}$ containing $F$ which is a splitting field of $f$.

Proof. For existence, let $\alpha_1, \ldots, \alpha_k$ be the roots of $f$ in $\mathbb{C}$, and set $\Sigma := F(\alpha_1, \ldots, \alpha_k) \subseteq \mathbb{C}$. Since $\mathbb{C}$ is algebraically closed we see that $f$ splits over $\Sigma$. Property (2') implies $\Sigma$ is a splitting field.

Suppose $F \subseteq \Sigma' \subseteq \mathbb{C}$ with $\Sigma'$ some other splitting field of $f$. Then the above argument shows that $\Sigma \subseteq \Sigma'$, while property (2) applied to the splitting field $\Sigma'$ implies $\Sigma \supseteq \Sigma'$.

Example. $f = (X^2 + 1)(X^2 - 5) \in \mathbb{Q}[X]$. The splitting field is $\mathbb{Q}(i, \sqrt{5})$.

Example. $f = X^4 - 8X^2 + 36 \in \mathbb{Q}[X]$. The splitting field is also $\mathbb{Q}(i, \sqrt{5})$. An extension $L : F$ can be a splitting field for many different polynomials over $F$.

Example. $f = X^3 - 2 \in \mathbb{Q}[X]$. Write $\alpha = \sqrt{2}$. Note that $\mathbb{Q}(\alpha)$ is not a splitting field. Instead the splitting field is

$$\mathbb{Q}(\alpha, \omega \alpha, \omega^2 \alpha) = \mathbb{Q}(\alpha, \omega),$$

where $\omega = e^{2\pi i/3}$.

Example. $f = X^2 + X + 1 \in \mathbb{Q}[X]$. The splitting field is $\mathbb{Q}(\omega)$.

We have constructed splitting fields for subfields of $\mathbb{C}$, but in fact splitting fields exist for any polynomial over any field.

Proposition. For any field $F$ and any non-zero $f \in F[X]$ there is a homomorphism $\iota : F \to \Sigma$ making $\Sigma : F$ a splitting field of $f$.

Proof. Proof by induction of $n = \deg f$. If $n = 1$ then $\Sigma = F$.

Suppose $n \geq 2$. Choose an irreducible factor $g$ of $f$ over $F$, and construct a simple extension $K := F[X]/(g)$ of $F$. If we write $\alpha = \overline{X}$ in $K$ then $K = F(\alpha)$. Clearly $f$ factors as $f = (X - \alpha)f'$ over $K$ with $\deg f' < n$. By induction there is a splitting extension $K \to \Sigma$ of $f'$, and this gives a splitting extension $F \to \Sigma$ of $f$. □

32. Homomorphisms from splitting fields

A key feature of splitting fields is that it is easy to construct homomorphisms out of them. To do this we need the following notation.

If $\iota : F \to K$ is a homomorphism of fields, then we get a homomorphism of polynomial rings $\iota : F[X] \to K[X]$, defined by

$$f = \sum a_k X^k \mapsto \iota(f) := \sum \iota(a_k) X^k.$$

Note that if $\alpha \in F$ is a root of $f$, then $\iota(\alpha) \in K$ is a root of $\iota(f)$.

The following is a major tool in what follows; we’ve actually already used a special case.

Lemma (Lifting lemma). Let $K : F$ and $K' : F'$ be field extensions, and let $\iota : F \to F'$ be an isomorphism of fields. Suppose that $K = F(\alpha)$ is a simple extension of $F$ with minimal polynomial $f = f_\alpha / f \in F[X]$, and let $f' := \iota(f) \in F'[X]$.

Then for every root $\beta \in K'$ of $f'$, there exists a unique homomorphism $\phi : K \to K'$ such that

$$\phi|_F = \iota \quad \text{and} \quad \phi(\alpha) = \beta.$$

The image of such a $\phi$ is $F'(\beta) \subseteq K'$. In particular, if $K' = F'(\beta)$ then $\phi$ is an isomorphism.

$$\begin{CD}
F @>{\phi}>> K' \\
@VVV \sim @VVV \\
F @>{\iota}>> F'
\end{CD}$$
Then there exists a homomorphism $\varphi$. We can factor $g$ irreducible in $F'[X]$, and so $f' = f_{\beta/F'}$.

Recall that the extension $F(\alpha) : F$ is isomorphic over $F$ to the quotient ring $F[X]/(f)$, so we might as well assume $K = F[X]/(f)$. Then there exists a ring homomorphism

$$\bar{\varphi} : F[X] \to K' \quad \bar{\varphi}(\sum a_kX^k) = \varphi(a_k)\beta^k.$$ 

The image of $\bar{\varphi}$ is the subfield $F'(\beta) \subseteq K'$. The kernel of $\bar{\psi}$ is precisely those $g \in F[X]$ such that $\beta$ is a root of $g' = \varphi(g)$, i.e., such that $f'$ divides $g'$, or equivalently (since $F[X] \to F'[X]$ is an isomorphism), that $f$ divides $g$.

Thus, by the isomorphism theorem, there exists a unique factorization through an isomorphism $\phi$:

$$\begin{array}{ccc}
F[X] & \xrightarrow{\bar{\varphi}} & F(\beta) \\
\downarrow & & \downarrow \\
F[X]/(f) & \xrightarrow{\phi} & K'
\end{array}$$ 

The homomorphism $\phi$ is unique such that $\phi|F = \iota$ and $\phi(\alpha) = \beta$, since $F(\alpha)$ is generated as a field by $F \cup \{\alpha\}$.

$\square$

**Proposition.** Consider

- a field $F$,
- a nonzero polynomial $g \in F[X]$,
- a splitting field $\Sigma : F$ of $g$, and
- an extension $L : F$ over which $f$ splits.

Then there exists a homomorphism $\phi : \Sigma \to L$ such that $\phi|F = \iota$.

This is a special case of the following (Lemma 9.5). The more general version is needed to be able to give a proof by induction.

**Proposition.** Consider

- an isomorphism of fields $\iota : F \to F'$,
- a non-zero polynomial $g \in F[X]$,
- a splitting field $\Sigma : F$ of $g$, and
- an extension $L : F'$ over which $\iota(g)$ splits.

Then there exists a homomorphism $\phi : \Sigma \to L$ such that $\phi|F = \iota$.

**Proof.** Assume $g$ is monic and splits as $g = (X - \alpha_1) \cdots (X - \alpha_n)$ over $\Sigma$, so that $\Sigma(\alpha_1, \ldots, \alpha_n)$ (note: $\alpha_i$s can repeat). We will use induction on $\deg g$, noting that $\phi = \iota$ if $\deg g \leq 1$.

Let $f_1 = f_{\alpha_1/F} \in F[X]$, so $f_1 \mid g$ in $F[X]$. Therefore $\iota(f_1) \in F'[X]$ is an irreducible factor of $\iota(g)$ in $F'[X]$, and $\iota(f_1)$ splits in $L$ since $\iota(g)$ does.

Pick a root $\beta_1 \in L$ of $\iota(f_1)$. By the above lemma, there exists an isomorphism $\phi_1$ fitting in

$$\begin{array}{ccc}
\Sigma & \xrightarrow{\phi_1} & L \\
\downarrow & & \downarrow \\
F(\alpha_1) & \xrightarrow{\sim} & F'(\beta_1) \\
F \xrightarrow{\iota} & & F'
\end{array}$$

We can factor $g = (X - \alpha_1)h$ over $F(\alpha_1)$. Now note that we are in the same sitation: we have

- an isomorphism of fields $\phi_1 : F(\alpha_1) \to F'(\beta_1)$,
- a nonzero polynomial $h \in F(\alpha_1)[X]$,
- a splitting field $\Sigma : F(\alpha_1)$ of $h$, and
• an extension $L : F'(\alpha_1)$ over which $\phi_1(h)$ splits.

Since $\deg h < \deg g$, induction applies to produce the desired homomorphism $\phi$. \hfill \square

Note: Taking $F = F''$ and $\iota = \text{id}$, we see that any two splitting fields of $f$ are abstractly isomorphic as fields. (This works even if they are not subfields of $C$.)

It is important that the above actually gives a procedure for constructing homomorphism $\Sigma \rightarrow L$, and that there can be many such homomorphisms, depending on the choices you make. Careful analysis using this idea will often allow us to compute $\text{Aut}(\Sigma : F)$, the automorphism group of the splitting field extension.

Example (Important). Consider $g = X^3 - 2 \in \mathbb{Q}[X]$. This factors

$$g = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3) = (X - \alpha)(X - \omega\alpha)(X - \omega^2\alpha),$$

where $\alpha = \sqrt[3]{2} \in \mathbb{R}$ and $\omega = e^{2\pi i/3}$. Thus $\Sigma = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) \subseteq \mathbb{C}$ is the splitting field. I want to construct homomorphisms $\Sigma \rightarrow \mathbb{C}$. Of course, there is an obvious choice, namely the inclusion $\Sigma \subseteq \mathbb{C}$. But there are others. For instance:

• Define $\phi_1 : \mathbb{Q}(\alpha) \rightarrow \mathbb{C}$ to be the unique homomorphism sending $\alpha \mapsto \omega\alpha$, which we can do since $\omega\alpha$ is a root of the irreducible $g \in \mathbb{Q}[X]$. This gives an isomorphism

$$\mathbb{Q}(\alpha) \xrightarrow{\phi_1} \mathbb{Q}(\omega\alpha) \subseteq \mathbb{C}.$$  

• Note that over $K_1 = \mathbb{Q}(\alpha)$, $g$ factors as $(X - \alpha)g_1 = (X - \alpha)(X^2 + \alpha X + \alpha^2)$, and note that $g_1$ has roots $\omega\alpha$ and $\omega^2\alpha$ in $\mathbb{C}$. The homomorphism $\phi_1$ sends

$$g_1 = X^2 + \alpha X + \alpha^2 \mapsto g'_1 = X^2 + \omega\alpha X + \omega^2\alpha^2 \in L_1 = \mathbb{Q}(\omega\alpha).$$

The polynomial $g'_1$ has roots $\alpha$ and $\omega^2\alpha$ in $\mathbb{C}$. (The other two roots of $g$. This is expected because $g = (X - \alpha)g_1$ so $g = \phi_1(g) = (X - \omega\alpha)g'_1$.)

• Define $\phi_2 : \mathbb{Q}(\alpha, \omega\alpha) \rightarrow \mathbb{C}$ to be the unique homomorphism such that $\phi_2|K_1 = \phi_1$ and sending $\omega\alpha \mapsto \omega^2\alpha$, which we can do since $\omega^2\alpha$ is a root of the irreducible $g'_1 \in L_1[X]$. This gives an isomorphism

$$K_2 = \mathbb{Q}(\alpha, \omega\alpha) \xrightarrow{\phi_2} L_2 = \mathbb{Q}(\omega\alpha, \omega^2\alpha) \subseteq \mathbb{C}.$$  

• Note that over $K_2 = \mathbb{Q}(\alpha, \omega\alpha)$, $g_1$ factors as $(X - \omega\alpha)(X - \omega^2\alpha)$. In other words, it already splits: $\Sigma = \mathbb{Q}(\alpha, \omega\alpha)$ is the splitting field of $g$. Likewise, $L_2 = \mathbb{Q}(\omega\alpha, \omega^2\alpha) = \Sigma$ as well, so we have defined an isomorphism $\phi : \Sigma \rightarrow \Sigma$.

Since $\omega^2\alpha = (\omega\alpha)^2\alpha^{-1}$, we see that

$$\phi(\omega^2\alpha) = (\omega^2\alpha)^2(\omega\alpha)^{-1} = \omega^3\alpha = \alpha.$$  

We can represent this strategy by a diagram:

$$\begin{array}{ccc}
\mathbb{Q}(\alpha, \omega\alpha) & \xrightarrow{\omega\alpha \mapsto \cdot} & \Sigma \\
\downarrow & & \downarrow \\
\mathbb{Q}(\alpha) & \xrightarrow{\alpha \mapsto \cdot} & \mathbb{Q}(\phi(\alpha)) \\
\downarrow & & \downarrow \\
\mathbb{Q} & \xrightarrow{\cdot} & \mathbb{Q}
\end{array}$$

with two places to make choices. The possible choices are:

<table>
<thead>
<tr>
<th>$\phi(\alpha)$</th>
<th>$\alpha$</th>
<th>$\alpha$</th>
<th>$\omega\alpha$</th>
<th>$\omega\alpha$</th>
<th>$\omega^2\alpha$</th>
<th>$\omega^2\alpha$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\phi(\omega\alpha)$</td>
<td>$\omega\alpha$</td>
<td>$\omega^2\alpha$</td>
<td>$\alpha$</td>
<td>$\alpha$</td>
<td>$\omega\alpha$</td>
<td>$\omega\alpha$</td>
</tr>
<tr>
<td>$\phi(\omega^2\alpha)$</td>
<td>$\omega^2\alpha$</td>
<td>$\omega\alpha$</td>
<td>$\omega\alpha$</td>
<td>$\alpha$</td>
<td>$\omega\alpha$</td>
<td>$\omega\alpha$</td>
</tr>
</tbody>
</table>
Example. Consider \( g = (X^2 - 2)(X^2 - 3) \in \mathbb{Q} \), with roots \( \pm \sqrt{2}, \pm \sqrt{3} \). The splitting field is \( \Sigma = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \). We can construct isomorphisms \( \phi : \Sigma \to \Sigma \) according to the diagram:

\[
\begin{array}{c}
\mathbb{Q}(\sqrt{2}, \sqrt{3}) \xrightarrow{\phi} \Sigma \\
\downarrow \quad \downarrow \\
\mathbb{Q}(\sqrt{2}) \xrightarrow{\phi} \mathbb{Q}(\phi(\sqrt{2})) \\
\downarrow \quad \downarrow \\
\mathbb{Q} \xrightarrow{=} \mathbb{Q}
\end{array}
\]

Since \( f_{\sqrt{2}/\mathbb{Q}} = X^2 - 2 \), at the first step there are two choices: \( \phi(\sqrt{2}) \in \{ \pm \sqrt{2} \} \). Over \( \mathbb{Q}(\sqrt{2}) \) the element \( \sqrt{3} \) still has minimal polynomial \( f_{\sqrt{3}/\mathbb{Q}(\sqrt{2})} = X^2 - 3 \). This is because \( \sqrt{3} \notin \mathbb{Q}(\sqrt{2}) \). So there are two choices here as well.

\[
\begin{array}{c|cccc}
\phi(\sqrt{2}) & \sqrt{2} & \sqrt{2} & -\sqrt{2} & -\sqrt{2} \\
\phi(\sqrt{3}) & \sqrt{3} & -\sqrt{3} & \sqrt{3} & -\sqrt{3}
\end{array}
\]

Example. Consider \( g = X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X] \). It turns out that the roots of this polynomial in \( \mathbb{C} \) are

\[
\alpha_1 = \zeta + \zeta^{-1}, \quad \alpha_2 = \zeta^2 + \zeta^{-2}, \quad \alpha_3 = \zeta^3 + \zeta^{-3}, \quad \zeta = e^{2\pi i/7}.
\]

Since none of these are in \( \mathbb{Q} \) and \( \deg g = 3 \) we see \( g \) is irreducible.

Using this you can check that: \( \alpha_2 = \alpha_1^2 - 2, \alpha_3 = \alpha_2^2 - 2 \). Thus \( \Sigma = \mathbb{Q}(\alpha_1) \) is already a splitting field of \( g \), and a homomorphism \( \phi : \Sigma \to \Sigma \) is determined by where it sends \( \alpha_1 \). The possible choices are:

\[
\begin{array}{c|ccc}
\phi(\alpha_1) & \alpha_1 & \alpha_2 & \alpha_3 \\
\phi(\alpha_2) & \alpha_2 & \alpha_3 & \alpha_1 \\
\phi(\alpha_3) & \alpha_3 & \alpha_1 & \alpha_2
\end{array}
\]

Question: what if we didn’t already know the roots of \( g \)? How could we have analyzed this in that case?

33. Normal extensions

We noted that a given finite extension can be the splitting field of many different polynomials. There is an abstract characterization of when such an extension is a splitting field, which doesn’t require mentioning a particular polynomial.

An algebraic extension \( L : F \) is normal if every \( f \in \text{Irred}(F) \) which has a root in \( L \) splits in \( L \).

Example. \( \mathbb{Q}^{\text{alg}} : F \) for any subfield \( F \) is a normal extension, since it is an algebraic extension and all polynomials over \( \mathbb{Q}^{\text{alg}} \) (and hence over \( F \)) split in \( \mathbb{Q}^{\text{alg}} \).

Example. \( \mathbb{Q}(\sqrt{2}) : \mathbb{Q} \) is normal. To see this, consider \( f \in \text{Irred}(\mathbb{Q}) \) which has a root \( \alpha \in \mathbb{Q}(\sqrt{2}) \). Write \( \alpha = u + v\sqrt{2} \) with \( u, v \in \mathbb{Q} \). There are two cases.

- If \( v = 0 \) then \( \alpha = a \in \mathbb{Q} \), so \( X - a \) is a factor of \( f \) over \( \mathbb{Q} \). Since \( f \) is monic and irreducible we must have \( f = X - a \), i.e., it splits into one linear factor.
- If \( v \neq 0 \), consider \( g = (X - (u + v\sqrt{2}))(X - (u - v\sqrt{2})) = X^2 - 2uX + (u^2 - 2v^2) \in \mathbb{Q}[X] \). Since \( \alpha \notin \mathbb{Q} \) this quadratic must be irreducible over \( \mathbb{Q} \), i.e., \( g = f_{\alpha/\mathbb{Q}} \) is the minimal polynomial. Since \( f(\alpha) = 0 \) we must have \( g | f \), and since \( f \) is monic irreducible we must have \( g = f \), and clearly \( g \) splits over \( \mathbb{Q}(\sqrt{2}) \).

Exercise. Show that every degree 2 extension is normal.

Example. \( \mathbb{Q}(\sqrt{2}) : \mathbb{Q} \) is not normal, since \( f = X^3 - 2 \) does not split over \( \mathbb{Q}(\sqrt{2}) \).
**Theorem.** An finite extension $L : F$ is normal if and only if it is a splitting field for some polynomial $f \in F[X]$.

**Proof part 1:** Finite normal extensions are splitting fields: If $L : F$ is a finite extension we can find a finite list of elements of $L$ so that

$$L = F(\alpha_1, \ldots, \alpha_m).$$

Since it is a finite extension each $\alpha_j$ is algebraic over $F$, so let $f_j = f_{\alpha_j/F}$ be the minimal polynomial of $\alpha_j$ over $F$. Because $L : F$ is normal $f_j$ splits over $L$. Then $f = f_1 \cdots f_m \in F[X]$ is a polynomial which splits over $L$ and whose roots generate $L$ over $F$, i.e., $L$ is a splitting field of $f$. □

We get the second part as a special case of a more general claim.

**Lemma.** Suppose $F \subseteq \Sigma \subseteq L$, where $\Sigma = \Sigma_{f/F}$ is a splitting field of some $f \in F[X]$. If $\alpha, \beta \in L$ are roots of the same irreducible polynomial $g \in \text{Irred}(F)$, then $[\Sigma(\alpha) : \Sigma] = [\Sigma(\beta) : \Sigma]$.

**Proof.** Consider the following diagram of subfields of $L$.

\[
\begin{array}{c}
\Sigma(\alpha) \\
\downarrow \\
\Sigma \\
\downarrow \\
F(\alpha) \\
\downarrow \\
F
\end{array}
\quad
\begin{array}{c}
\Sigma(\beta) \\
\downarrow \\
\Sigma \\
\downarrow \\
F(\beta) \\
\downarrow \\
F
\end{array}
\]

To prove the result it suffices to show that $[F(\alpha) : F] = [F(\beta) : F]$ and $[\Sigma(\alpha) : F(\alpha)] = [\Sigma(\beta) : F(\beta)]$, using the tower law. In fact, I claim there exist isomorphisms $\phi$ and $\psi$ which are compatible with the inclusions in

\[
\begin{array}{c}
\Sigma(\alpha) \xrightarrow{\phi} \Sigma(\beta) \\
\downarrow \\
F(\alpha) \xrightarrow{\psi} F(\beta)
\end{array}
\]

That is, $\phi|_K$ is the inclusion of the subfield $K \subseteq K(\beta)$, and $\psi|_{K(\alpha)}$ is $\phi$.

To see that $\phi$ exists, just note that both $K(\alpha)$ and $K(\beta)$ are simple extensions generated over $K$ by roots of the irreducible polynomial $g \in \text{Irred}(K)$, so there are isomorphisms $K(\alpha) \approx K[X]/(g(X)) \approx K(\beta)$ compatible with the inclusions of $K$.

To see that $\psi$ exists, note that $\phi(f) = f$ since $f \in K[X]$ and observe that $\Sigma(\alpha) = \Sigma_{f/K(\alpha)}$ and $\Sigma(\beta) = \Sigma_{f/K(\beta)}$ are both splitting fields for $f$ over the respective subfields, so there exists an isomorphism $\psi$ extending the isomorphism $\phi$. □

**Proof of part 2:** splitting fields are normal extensions. Suppose $\Sigma : F$ is a splitting field of $f \in F[X]$, and $g \in \text{Irred}(F)$ is some irreducible polynomial with root $\alpha \in \Sigma$.

Form a splitting field $L : \Sigma$ of the polynomial $g$. (If $L \subseteq \mathbb{C}$ just let $\Sigma = L(\beta_1, \ldots, \beta_r)$ where the $\beta_j$ are the roots of $g$ in $\mathbb{C}$.) If $\beta$ is any root of $g$ in $\Sigma$, the previous lemma says

$$[\Sigma(\alpha) : \Sigma] = [\Sigma(\beta) : \Sigma].$$

But $\alpha \in \Sigma$ so these are 1, so $\beta \in \Sigma$. Thus all roots of $g$ are in $\Sigma$, so $g$ splits over $\Sigma$ as desired. □
This is cool: a splitting field $\Sigma : F$ is a splitting field for any polynomial in $F$ which has a root in $\Sigma$.

We also have the following, which will be important for us.

**Proposition.** Consider fields $F \subseteq K \subseteq L$. If $L : F$ is normal then $L : K$ is normal.

**Proof.** First note that since $L : F$ is algebraic then so is $L : K$ and $K : F$.

Suppose $f \in \text{Irred}(K)$ has a root $\alpha \in L$. Since $K : F$ is algebraic it has a minimal polynomial $g = f_{\alpha/F} \in F[X]$ over $F$. Since $g$ has $\alpha$ as a root, over $K$ we must have $f \mid g$. Since $L : F$ is normal we have that $g$ splits over $\Sigma$, and therefore its factor $f$ splits over $\Sigma$. \[\square\]

Note: in the above the special case of $[L : F] < \infty$ is easier to prove. In this case $L : F$ normal implies $L$ is a splitting field of some $f \in F[X]$, whence $L : K$ is also a splitting field of the same polynomial $f \in F[X] \subseteq K[X]$, and hence normal.

### 34. Separable polynomials and extensions

We often have an inclusion of fields $F \subseteq K$, and a polynomial $F[X]$ which can thus also be considered as in $K[X]$. We note the following.

1. $f$ can factor differently in $F[X]$ vs $K[X]$. For instance, $X^4 + 1$ is irreducible over $\mathbb{Q}$, has two irreducible quadratic factors over $\mathbb{R}$, and splits over $\mathbb{C}$.

2. In particular, it is possible that $f$ is irreducible over $F$ but not over $K$.

Thus, factorization is highly dependent on the context.

However, some facts about pairs of polynomials are independent of context.

3. If $f, g \in F[X]$ and $f \mid g$ in $F[X]$, then also $f \mid g$ in $K[X]$.

4. Furthermore, if $f, g \in F[X]$ and $f \mid g$ in $K[X]$, then $f \mid g$ in $F[X]!$

   **Proof:** suppose $g = fh$ with $h \in K[X]$. We can also carry out the division algorithm in $F[X]$, so $g = qf + r$ with $q, r \in F[X]$ and $\deg r < \deg f$. But then we have the identity $hf = qf + r$ in $K[X]$, so $r = (h - q)f$, which is impossible by degree reasons unless $r = 0$. So $hf = qf$, whence $h = q$ by cancellation.

5. If $f, g \in F[X]$ have a GCD $d \in F[X]$, then $d$ is also their GCD in $K[X]$. Any GCD in $K[X]$ will be a $K$-scalar multiple of a GCD in $F[X]$.

   **Proof:** We know that $d$ is a GCD in $F[X]$ if $d \mid f$ and $d \mid g$ and if there exist $u, v \in F[X]$ such that $d = uf + vg$. All of this will still hold for $K[X]$, so $d$ is a GCD of $f, g$ over $K$.

6. Thus $f, g$ are relatively prime in $F[X]$ if and only if they are relatively prime in $K[X]$.

Note: The same kinds of remarks if instead of an inclusion $F \subseteq K$ we have a homomorphism $\iota: F \to K$, except that we then to rephrase these in terms of $\iota(f), \iota(g) \in K[X]$.

Given a polynomial

$$f = a_0 + a_1 X + \cdots + a_n X^n \in F[X],$$

define its **formal derivative** is defined to be

$$Df := a_1 + 2a_2 X + \cdots + na_n X^{n-1} \in F[X].$$

**Exercise.** Check that the formal derivative satisfies:

$$D(f + g) = Df + Dg, \quad D(fg) = (Df)g + f(Dg),$$

$$Dc = 0 \quad \text{and} \quad D(cf) = cD(f) \quad \text{if} \ c \in F.$$

We say that $f \in F[X]$ is **separable** if $f$ and $Df$ are relatively prime in $F[X]$. **separable polynomial**

**Exercise.** Show that if $f = gh \in F[X]$ and $f$ is a separable polynomial, so are $g$ and $h$.

The above remarks, together with the fact that the formula for $D$ doesn’t change when we pass to a larger field, imply that this is independent of context: if $F \subseteq K$, then $f$ is separable in $F[X]$ iff it is separable in $K[X]$. Thus, we don’t need to say things like “separable over $K$”, we just say $f$ is separable.
Exercise. Show that if \( \phi : F \to K \) is a homomorphism of fields, then \( f \in F[X] \) is a separable polynomial if and only if \( \phi(f) \in K[X] \) is a separable polynomial.

You probably know that \( \alpha \in \mathbb{R} \) is a repeated root of some \( f \in \mathbb{R}[X] \) if and only if \( \alpha \) is a critical point of \( \mathbb{R} \). This is actually a purely algebraic fact.

**Proposition.** Suppose \( f \in F[X] \) splits over \( L : F \). Then \( f \) is separable if and only if \( f \) has simple roots in \( L \).

**Proof.** Suppose \( f \) has a repeated root in \( L \). This means

\[
f = (X - \alpha)^2 g, \quad \alpha \in L, \quad g \in L[X].
\]

Then

\[
Df = 2(X - \alpha)g + (X - \alpha)^2 Dg = (X - \alpha)(2g + (X - \alpha)g),
\]

so \( f \) and \( Df \) have a linear common factor \( X - \alpha \) over \( L \).

Now suppose \( f \) and \( Df \) have a common factor in \( F \), which we can suppose to be an irreducible \( g \in \text{Irred}(F) \), which will have a root \( \alpha \in L \). Thus \( f \) and \( Df \) will have a common factor \( X - \alpha \) in \( L[X] \). Write \( f = (X - \alpha)h \) for \( h \in L[X] \), whence

\[
Df = h + (X - \alpha)(Dh).
\]

But since \( X - \alpha \) divides \( Df \) it must divide \( h \). So \( (X - \alpha)^2 \) divides \( f \).

Thus, we can say \( f \) is separable if and only if it has simple roots over its splitting field.

**Example.** The polynomial \( f = X^4 + 2X^2 + 1 \in \mathbb{Q}[X] \) has \( Df = 4X^3 + 4X \). It is not hard to see they have a common factor \( X^2 + 1 \). Thus \( f \) is not separable. In fact, \( f = (X^2 + 1)^2 \) over \( \mathbb{Q} \), and 

\[
f = (X - i)^2(X + i)^2 \quad \text{over} \quad \mathbb{C}.
\]

**Example.** The polynomial \( f = X^n - 1 \) is separable over \( \mathbb{Q} \) since \( Df = X^{n-1} \) and \( X \nmid f \). Thus \( f \) has \( n \) distinct roots over \( \mathbb{C} \), as we know.

We would like to be able to say that irreducible polynomials are almost separable. This is true for fields of characteristic 0, e.g., subfields of \( \mathbb{C} \).

**Proposition.** Suppose \( F \) is a field of characteristic 0 and that \( f \in F[X] \) is irreducible. Then \( f \) is separable.

**Proof.** Write \( f = a_0 + a_1X + \cdots + a_nX^n \), with \( a_n \neq 0 \) and \( n \geq 1 \). Then \( Df = a_1 + 2a_2X + \cdots + na_nX^{n-1} \). Because \( F \) has characteristic 0, \( n \neq 0 \), so \( na_n \neq 0 \), so \( \deg Df = n - 1 \). Therefore \( f \nmid Df \), and since \( f \) is irreducible, \( f \) and \( Df \) must be relatively prime.

**Example.** In finite characteristic there is an issue. Consider a field \( F \) of prime characteristic \( p \) and \( f = X^p - a \in F[X] \), \( a \in F \).

Then \( Df = pX^{p-1} = 0 \), so \( \deg Df = -\infty \) rather than \( p - 1 \). So \( f \) actually does divide \( Df \) in this case. So \( f \) is not separable.

For example, any polynomial of the form \( f = X^p - a \in F[X] \) is separable if \( F \) has characteristic \( p \). If this polynomial has a root \( b \), then \( b^p = a \), and you can check that

\[
(X - b)^p = \sum_{j=0}^{p} \binom{p}{j} X^j (-b)^j = X^p + (-1)^p b^p = X^p - b^p = X^p - a \in F[X],
\]

so it only has one root of multiplicity \( p \). (Note: \((-1)^p \equiv -1 \mod p \) for every prime \( p \), though the proof is different depending on whether \( p \) is odd or \( p = 2 \).)

It turns out that there are actually irreducible polynomials of this form. For instance, consider the field \( F = \mathbb{F}_p(t) \) of rational functions over \( \mathbb{F}_p \) and let \( f = X^p - t \). Then \( f \) is irreducible over \( F \) but not separable.

We will return to this when we discuss finite characteristic more carefully.
Given \( L : F \) we say that \( \alpha \in L \) is **separable over** \( F \) if \( \alpha \) is algebraic over \( F \) and \( f_{\alpha/F} \in F[X] \) is a separable polynomial. We say that \( L : F \) is a **separable extension** if every element of \( L \) is separable over \( F \).

**Proposition.** In characteristic 0, every algebraic extension is separable.

We won’t worry about non-separable extensions right now. However, the separability condition will come up in our statement of the Galois correspondence (which also works in finite characteristic), so I needed to be able to talk about it. We do have the following in general.

**Proposition.** If \( F \subseteq K \subseteq L \) and \( L : F \) is a separable extension, then \( L : K \) and \( K : F \) are separable extensions.

**Proof.** Note that by definition if \( L : F \) is a separable extension then every \( \alpha \in L \) is separable over \( F \), and so in particular every \( \alpha \in K \) is separable over \( F \). Thus \( K : F \) is a separable extension.

Consider \( \alpha \in L \). Since \( L : F \) is a separable extension the minimal polynomial \( f = f_{\alpha/F} \in F[X] \) over \( F \) is separable. The minimal polynomial \( g = f_{\alpha/K} \in K[X] \) is an irreducible factor of \( g \), so \( g \) is also separable, whence \( \alpha \) is separable over \( K \). Therefore \( L : K \) is a separable extension. \( \square \)

35. **The Galois Correspondence**

I am going to state and prove the Galois correspondence, modulo two “technical lemmas”, which I will prove soon. These technical lemmas are results about counting things (orders of groups or degrees of extensions), and are the following.

**Lemma (Tech Lemma 1).** Let \( G \leq \text{Aut}(L) \) be a finite subgroup of the automorphism group of a field \( L \). Then

\[
\]

**Lemma (Tech Lemma 2).** Let \( K : F \) be a finite and separable extension. Then

\[
|\text{Aut}(K : F)| \leq [K : F],
\]

with equality if and only if \( K : F \) is also normal.

It is because of the hypotheses of the second lemma that the correspondence will apply only to finite extensions which are normal and separable. We will also need the following fact(s), which we proved earlier: if \( K \) is an intermediate field of a normal separable extension \( L : F \), then \( L : K \) is also normal separable. (Note: \( K : F \) will also be separable, but may not be normal, though it can be.)

If we stick to characteristic 0, then all extensions are separable, so we won’t have to worry about that part.

Also remember that all finite normal extensions arise as splitting fields of polynomials, so this is where all examples will come from.

**Theorem (Basic Galois correspondence).** Let \( L : F \) be a finite normal separable extension and let \( G = \text{Aut}(L : F) \). The operations

\[
\begin{align*}
H & \quad \mapsto \quad L^H \\
\text{Aut}(L : K) & \quad \mapsto \quad K
\end{align*}
\]

are inverse one-to-one correspondences

\[
\{\text{subgroups of } G\} \quad \leftrightarrow \quad \{\text{intermediate extensions of } L : F\}.
\]

Recall that

\[
L^H := \{ x \in L \mid h(x) = x \ \forall h \in H \}, \quad \text{Aut}(L : K) := \{ g \in G \mid g(x) = x \ \forall x \in K \}.
\]

In particular, \( L^H \) is an intermediate extension \( F \subseteq L^H \subseteq L \), and \( \text{Aut}(L : K) \) is a subgroup of \( G = \text{Aut}(L : F) \).
Remark. Stewart writes $H^\dagger = L^H$ and $K^* = \text{Aut}(L : K)$, but frankly I find his notation confusing and hard to remember. It’s also not in any way standard. I’m just not going to use it.

Notice that both operations are order reversing, where the ordering is inclusion:

$$H \subseteq H' \implies L^H \supseteq L^{H'},$$

$$K \subseteq K' \implies \text{Aut}(L : K) \supseteq \text{Aut}(L : K').$$

That is, if $a \in L$ is such that $h(a) = a$ for all $h \in H$, then certainly that is true for all $h \in H' \subseteq H$; and if $g \in G = \text{Aut}(L : F)$ is such that $g|K' = \text{id}$, then certainly $g|K = \text{id}$ since $K \subseteq K'$.

Proof of the main Galois correspondence, using the technical lemmas. I show that the two operations are inverse to each other: doing one and then the other (in either order) gets you back where you started.

Let $H \leq G$ be a subgroup, and consider

$$H \implies L^H \implies \text{Aut}(L : L^H).$$

Observe that $H \leq \text{Aut}(L : L^H)$ by definition of $L^H = \{ a \in L \mid h(a) = a \ \forall h \in H \}$. By the technical lemmas

$$|\text{Aut}(L : L^H)| = \text{Lemma 2} \quad [L : L^H] = \text{Lemma 1} |H|,$$

where Lemma 2 applies because $L : L^H$ is normal and separable since $L^H$ is intermediate to the normal separable $L : F$. Therefore the two groups must be equal: $H = \text{Aut}(L : L^H)$.

Let $K$ be an intermediate field of $L : F$, and consider

$$K \implies \text{Aut}(L : K) \implies L^{\text{Aut}(L : K)}.$$  

Observe that $K \subseteq L^{\text{Aut}(L : K)}$ by definition of $\text{Aut}(L : K) = \{ g \in G \mid g|K = \text{id} \}$. By the technical lemmas

$$[L : L^{\text{Aut}(L : K)}] = \text{Lemma 1} |\text{Aut}(L : K)| = \text{Lemma 2} [L : K],$$

where Lemma 2 applies because $L : K$ is normal separable since $K$ is intermediate to the normal separable $L : F$. Therefore the two intermediate fields must be equal using the tower law $[L : K] = [L : L^{\text{Aut}(L : K)}][L^{\text{Aut}(L : K)} : K]$, so: $K = L^{\text{Aut}(L : K)}$. $\square$

Assume a fixed finite normal separable extension $L : F$ with automorphism group $G = \text{Aut}(L : F)$. An automorphism group of a normal separable extension is also called its Galois group.

As an immediate consequence of the proof, we get a relation between degrees of extensions and order of subgroups.

**Proposition.** For any intermediate field $K$ of $L : F$ we have

$$[L : K] = |\text{Aut}(L : K)|, \quad [K : F] = |G| / |\text{Aut}(L : K)|.$$

**Example.** $f = x^3 - 2 \in \mathbb{Q}[X], F = \mathbb{Q}, L = \Sigma_f/\mathbb{Q} = \mathbb{Q}(\alpha, \alpha\omega, \alpha\omega^2)$, with $\alpha = \sqrt[3]{2}$ and $\omega = e^{2\pi i/3}$. I’ll list the roots as $\alpha_1 = \alpha, \alpha_2 = \alpha\omega, \alpha_3 = \alpha\omega^2$. Then $G = \text{Aut}(L : \mathbb{Q}) \approx S_3$. The following diagram shows subgroups and corresponding subfields.
There is an additional part of the correspondence as usually stated, which deals with whether the “lower” extension \( K : F \) is normal, and if so what its automorphism group is.

**Theorem** (Normality in the Galois correspondence). Let \( L : F \) and \( G \) be as before, and suppose \( K \) is an intermediate field.

1. \( K : F \) is a normal extension if and only if \( H = \text{Aut}(L : K) \) is a normal subgroup of \( G \).
2. If \( K : F \) is a normal extension then \( \text{Aut}(K : F) \cong G/H \).

We can actually prove something a little bit stronger. Since \( L : F \) is a finite normal separable extension, it is the splitting field of some polynomial \( f \in F[X] \). Therefore \( L : K \) is also a splitting field of \( f \), this time thought of as a polynomial in \( K[X] \). Any \( \phi \in \text{Aut}(K : F) \) sends \( \phi(f) = f \), so \( \phi(f) \) also splits over \( L \). By our theorem about constructing homomorphisms from splitting fields, there exists a \( \tilde{\phi} : L \rightarrow L \) such that \( \tilde{\phi}|K = \phi \).

\[
\begin{array}{ccc}
L & \sim & L \\
\downarrow \phi & & \downarrow \tilde{\phi} \\
K & \sim & K \\
& & \downarrow \sim \\
& & F
\end{array}
\]

The upshot of the above argument is that every element of \( \text{Aut}(K : F) \) “comes from” an element \( g \in G \). More precisely, define the subset

\[
N := \{ g \in G \mid g(K) = K \},
\]

which you can see is actually a subgroup of \( G \). Do not confuse this with \( H = \{ g \in G \mid g|K = \text{id} \} \), which is a subgroup of \( N \). In fact, it’s a normal subgroup of \( N \): if \( h \in H \) and \( n \in N \), then for any \( a \in K \) we have that \( n^{-1}(a) \in K \), so \( hn^{-1}(a) = n^{-1}(a) \), so \( nhn^{-1}(a) = a \), i.e., \( nhn^{-1} \in H \).

There is an obvious group homomorphism

\[
N \rightarrow \text{Aut}(K : F)
\]

which sends \( g \in N \) to \( g|K : K \rightarrow K \). The above argument says that this is surjective, with kernel is exactly \( H \). By the isomorphism theorem for groups this gives a group isomorphism

\[
N/H \cong \text{Aut}(K : F).
\]

Next, we want to identify \( N \) in terms of the subgroup \( H \) alone (i.e., not in terms of the field \( K \)).

**Lemma.** For any \( g \in G \), we have \( \text{Aut}(L : g(K)) = gHg^{-1} \).

**Proof.** Given \( \sigma \in G \), let’s figure out when \( \sigma \in \text{Aut}(L : g(K)) \). This means exactly that

\[
\sigma g(a) = g(a) \quad \text{for all } a \in K,
\]

i.e. that \( g^{-1}\sigma g(a) = a \) for all \( a \in K \), i.e., that \( h = g^{-1}\sigma g \in H \). Equivalently, \( \sigma = ghg^{-1} \) for some \( h \in H \). \( \square \)

Using the basic Galois correspondence, we have that \( g(K) = K \) if and only if \( gHg^{-1} = H \).

Therefore we have the following.

**Proposition.** There is an isomorphism of groups \( \text{Aut}(K : F) \cong N/H \), where

\[
N = \{ g \in G \mid gHg^{-1} = H \}
\]

is the **normalizer** of \( H \) in \( G \).
The normality part of the correspondence follows: we have

\[ |\text{Aut}(K : F)| = \frac{|N|}{|H|}. \]

By the tower law

\[ [K : F] = \frac{[L : F]}{[L : K]} = \frac{|G|}{|H|}, \]

so \([K : F] = |\text{Aut}(K : F)|\) iff \(N = G\). Technical lemma 2 says the equality is equivalent to \(K : F\) being normal. In the case that \(K : F\) is normal then \(N = G\) so \(\text{Aut}(K : F) \approx G/H\) as claimed.

Finally, note that if \(g(K) \neq K\), you have found another intermediate field of \(L : F\) which is \(F\)-isomorphic to \(K\). All intermediate fields of \(L : F\) which are \(F\)-isomorphic to \(K\) this way (because if \(\tilde{\phi}: K \rightarrow K'\) is an \(F\)-isomorphism between intermediate fields, you can extend it to an automorphism \(\phi: L \rightarrow L\) since \(L : F\) is a splitting field), and there are exactly \(|G| / |N|\) of them.

**Example.** \(f = X^3 - 2 \in \mathbb{Q}[X]\).

**Example** (from Chapter 13). \(f = X^4 - 2 \in \mathbb{Q}[X], F = \mathbb{Q}, L = \Sigma_{f/\mathbb{Q}}, G = \text{Aut}(L : \mathbb{Q}) \leq S_4\). The polynomial has roots

\[ \alpha_1 = \alpha = \sqrt[3]{2}, \quad \alpha_2 = i\alpha, \quad \alpha_3 = i^2\alpha = -\alpha, \quad \alpha_4 = i^3\alpha = -i\alpha. \]

Consider the following partial diagram of subfields.

\[
\begin{array}{c}
L = \mathbb{Q}(\alpha, i) \\
\downarrow \\
\mathbb{Q}(i) \\
\downarrow \\
\mathbb{Q} \\
\end{array}
\]

Claim: \(f\) is irreducible (e.g., by Eisenstein). Also, \(f_{i/\mathbb{Q}} = X^2 + 1\). Therefore \([\mathbb{Q}(\alpha) : \mathbb{Q}] = 4\) and \([\mathbb{Q}(i) : \mathbb{Q}] = 2\).

Also, \(i \notin \mathbb{Q}(\alpha) \subseteq \mathbb{R}\), so \([L : \mathbb{Q}(\alpha)] \geq 2\). Also \([L : \mathbb{Q}(\alpha)] \leq 2\) since \(i\) satisfies \(X^2 + 1\). We conclude that \([L : \mathbb{Q}(\alpha)] = 2\) and thus \([L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)] [\mathbb{Q}(\alpha) : \mathbb{Q}] = 8\), and so \(|G| = 8\).

I claim that \(G = D_4\). To see this, note that the relations \(\alpha_1 = -\alpha_3\) and \(\alpha_2 = -\alpha_4\) limit how elements of \(G\) can permute the roots, so that only 8 elements of \(S_4\) are possibilities. These include \(r = (1\ 2\ 3\ 4)\) and \(s = (2\ 4)\).

Here is the full diagram of subgroups and subfields.

Aside from \(\{e\}\), the normal subgroups of \(G\) are exactly those which contain \(r^2\). Thus, the intermediate fields \(K\) such that \(K : \mathbb{Q}\) is normal are precisely the subfields of \(\mathbb{Q}(\sqrt{2}, i)\). The four extensions \(\mathbb{Q}(\alpha_k) : \mathbb{Q}\) are not normal over \(\mathbb{Q}\); instead, they are all isomorphic to each other.
Example. $f = X^5 - 2 \in \mathbb{Q}[X]$, $F = \mathbb{Q}$, $L = \Sigma_f/\mathbb{Q}$, $G = \text{Aut}(L : \mathbb{Q}) \leq S_5$. This polynomial has roots

$$
\alpha_1 = \alpha = \sqrt[5]{2}, \quad \alpha_2 = \zeta \alpha, \quad \alpha_3 = \zeta^2 \alpha, \quad \alpha_4 = \zeta^3 \alpha, \quad \alpha_5 = \zeta^4 \alpha,
$$

where $\zeta = e^{2\pi i/5}$.

Since $f$ is irreducible and $\zeta = \alpha_2/\alpha_1 \in L$ has minimal polynomial $\Phi_5$, we have that $[L : \mathbb{Q}]$ is divisible by $\mathbb{Q}[\alpha] : \mathbb{Q} = 5$ and $\mathbb{Q}([\zeta]) : \mathbb{Q} = 4$. So $20 \mid [L : \mathbb{Q}] = |G|$. In fact, using the fact that $\alpha_{n+1}/\alpha_n = \zeta$ for all $n = 1, \ldots, 5$ (where I let $\alpha_6 = \alpha_1$), you can see that there are at most 20 elements in $G$.

Exercise: what is the structure of $G$? What is its lattice of subgroups? What are the corresponding fixed fields?

36. Linear independence of field homomorphisms

We now tackle the first technical lemma. This material is from Chapter 10 of the book.

Let $K : F$ and $L : F$ be two field extensions over $F$. Let

$$
\text{Hom}_F(K, L) := \{ \phi : K \to L \mid \phi \text{ is a field homomorphism, } \phi|_F = \text{id} \}.
$$

This is the set of all $F$-homomorphisms of fields. Note that if $L : F$ is a finite extension, then $\text{Hom}_F(L, L) = \text{Aut}(L : F)$ (because for $\phi \in \text{Hom}_F(L, L)$ the image $\phi(L) \subseteq L$ is a subfield containing $F$, and $[L : F] = [\phi(L) : F]$ which implies $[L : \phi(L)] = 1$).

This is a subset of a larger set:

$$
\text{Lin}_F(K, L) := \{ \alpha : K \to L \mid \alpha \text{ is an } F\text{-linear map of vector spaces} \}.
$$

We make an observation: the set $\text{Lin}_F(K, L)$ is itself a vector space over $L$. Clearly we can add elements in $\text{Lin}_F(K, L)$. If $\lambda \in L$ and $\alpha \in \text{Lin}_F(K, L)$ then the function $x \mapsto \lambda \alpha(x)$ is also in $\text{Lin}_F(K, L)$.

Thus, it makes sense to talk about a subset of $\text{Lin}_F(K, L)$ being linearly independent, by which we mean linearly independent over $L$.

Proposition (Linear independence of field homomorphisms). The subset $\text{Hom}_F(K, L)$ of $\text{Lin}_F(K, L)$ is linearly independent over $L$.

Proof. We have to show: for any list $\phi_1, \ldots, \phi_n$ of distinct homomorphisms, and list $a_1, \ldots, a_n$ of elements of $L$, that $\sum_j a_j \phi_j = 0$ implies all $a_j = 0$. This really means showing: if $\sum_j \phi_j(x) = 0$ for all $x \in K$, then all $a_j = 0$.

The key observation is that for any linear dependence $a_1 \phi_1 + \cdots + a_n \phi_n = 0$ with $\phi_j \in \text{Hom}_F(K, L)$ and $a_j \in L$, and any $c \in K$, we can produce a new linear dependence $a_1 \phi_1(c) \phi_1 + \cdots + a_n \phi_n(c) \phi_n = 0$. This is simply because for all $x \in K$,

$$
0 = a_1 \phi_1(cx) + \cdots + a_n \phi_n(cx) = a_1 \phi_1(c) \phi_1(x) + \cdots + a_n \phi_n(c) \phi_n(x).
$$

In particular, by subtracting $\phi_n(c) \sum_j a_j \phi_j = 0$ from this, we get

$$
a_1(\phi_1(c) - \phi_n(c)) \phi_1 + \cdots + a_{n-1}(\phi_{n-1}(c) - \phi_n(c)) \phi_{n-1} = 0.
$$

We argue by contradiction, i.e., suppose there exists a linear dependence $a_1 \phi_1 + \cdots + a_n \phi_n = 0$ with $\phi_1, \ldots, \phi_n$ distinct homomorphisms and not all $a_j = 0$. Choose from among these one with shortest length $n$. This implies $a_j \neq 0$ for $j = 1, \ldots, n$, since otherwise we can discard the 0 term to get a shorter linear dependence.

If $n = 1$ then $a_1 \phi_1 = 0$, whence $a_1 \phi_1(1) = a_1$ is 0, which contradicts $a_1 \neq 0$.

If $n \geq 2$ choose $c \in K$ such that $\phi_1(c) \neq \phi_n(c)$. Then the argument given above produces a linear dependence

$$
a_1(\phi_1(c) - \phi_n(c)) \phi_1 + \cdots + a_{n-1}(\phi_{n-1}(c) - \phi_n(c)) \phi_{n-1} = 0,
$$

which is non-trivial (since $a_1(\phi_1(c) - \phi_n(c)) \neq 0$) but has shorter length $n - 1$. This contradicts our hypothesis of minimal length.
We are going to need a bit of linear algebra.

**Lemma.** Let
\[ a_{i1}x_1 + \cdots + a_{in}x_n = 0, \quad i = 1, \ldots, m, \]
be a system of \( m \) homogenous linear equations in \( n \)-variables, with coefficients \( a_{ij} \) in a field \( K \). If \( m < n \) then there exists a non-trivial solution \( (x_1, \ldots, x_n) \in K^n \), i.e., one not equal to \((0, \ldots, 0)\). Equivalently, if the only solution to the system is the trivial solution \((0, \ldots, 0)\), then \( n \leq m \).

**Proof.** This is a theorem of linear algebra. The space of solutions is the nullspace of the \( m \times n \) matrix \( A = (a_{ij}) \), consisting of column vectors in \( x \in K^n \) such that \( Ax = 0 \). The dimension over \( K \) of the null space is
\[ \text{nullity } A = \text{(number of columns of } A) - \text{(rank of } A) = n - \text{rank } A. \]
If the only solutions are trivial, then nullity \( A = 0 \) whence \( n = \text{rank } A \). But in general rank \( A = \min(m, n) \), so we must have \( n \leq m \) as desired.

Together with linear independence of homomorphisms we get the following consequence.

**Proposition.** Let \( K : F \) and \( L : F \) be extensions. If \( [K : F] < \infty \) then \( |\text{Hom}_F(K, L)| \leq [K : F] \).

**Proof.** Let \( v_1, \ldots, v_m \) be an \( F \)-basis of \( K \), and consider a sequence of elements \( \phi_1, \ldots, \phi_n \in \text{Hom}_F(K, L) \). We want to show that \( n \leq m \).

Consider any solution \( x_1, \ldots, x_n \in L \) of the system of equations
\[ \phi_1(v_i)x_1 + \cdots + \phi_n(v_i)x_n = 0, \quad i = 1, \ldots, m. \]
That is, \((x_1, \ldots, x_n) \in L^n \) is in the nullspace of the \( m \times n \) matrix \((\phi_j(v_i)) \in L^{m \times n} \). I will show that \((x_1, \ldots, x_n) = (0, \ldots, 0)\), i.e., the only solution is trivial, so \( n \leq m \) as desired.

Any \( y \in K \) can be written as \( y = \sum_i y_i v_i \) for some \( y_1, \ldots, y_m \in F \), whence
\[
\sum_j x_j \phi_j(y) = \sum_j x_j \phi_j \left( \sum_i y_i v_i \right)
= \sum_j \sum_i x_j y_i \phi_j(v_i)
= \sum_i y_i \sum_j x_j \phi_j(v_i) = 0.
\]
Since this holds for arbitrary \( y \in K \), we have that \( \sum_j x_j \phi_j = 0 \). By linear independence of homomorphisms, this implies that \( x_1 = \cdots = x_n = 0 \), as desired.

37. **Proof of the first technical lemma**

Here is the proof of “Technical lemma 1”.

**Theorem.** Let \( G \leq \text{Aut}(L) \) be a finite subgroup of the automorphisms of a field \( L \), and let \( L^G \) be the fixed field. Then \([L : L^G] = |G|\).

(Note: in the book it is implicitly assumed that \([L : L^G] < \infty\), but not proven. I will prove this.)

**Proof.** Write \( F = L^G \) in the following. Proof that \([L : F] \geq |G|\). Either \([L : F] \) is infinite in which case the conclusion is immediate, or \([L : F] < \infty\), in which case it follows from the previous proposition which asserts that \( |\text{Hom}_F(L, L)| \leq [L : F] \), and since \( G \subseteq \text{Hom}_F(L, L) \).

**Proof that \([L : F] \leq |G|\).** Write \( \phi_1, \ldots, \phi_n \) for the distinct elements of \( G \). We need to show that given any \( v_1, \ldots, v_m \in L \) which are \( F \)-linearly independent, we must have \( m \leq n \). (If \([L : F] < \infty\),
then we can take \( v_1, \ldots, v_m \) to be a basis over \( F \) as the book does, but this presupposes that \([L : F] < \infty\. The way I have stated things, the proof will imply that \([L : F] \) is finite.\)

We suppose \( m > n \) and obtain a contradiction. By the linear algebra lemma there exist \( y_1, \ldots, y_m \in L \) not all zero such that

\[
\phi_j(v_1)y_1 + \cdots + \phi_j(v_m)y_m = 0, \quad j = 1, \ldots, n,
\]

i.e., \((y_1, \ldots, y_m)\) is a non-trivial element in the nullspace of \((\phi_j(v_i))^\top\). Choose the \( y \)s so that as few as possible are non-zero, and renumber so that \( y_1, \ldots, y_r \neq 0, y_{r+1} = \cdots = y_m = 0 \), so we have

\[
y_1\phi_j(v_1) + \cdots + y_r\phi_j(v_r) = 0, \quad j = 1, \ldots, n.
\]

If \( r = 1 \) this would mean \( y_1\phi_j(v_1) = 0 \) for all \( j \), and thus in particular \( \phi_1(v_1) = 0 \) (since \( n \geq 1 \)). But since \( \phi_1 \) is an isomorphism, this implies \( v_1 = 0 \), which contradicts linear independence over \( F \). So \( r \geq 2 \).

Now let \( \phi \in G \) be any element. Applying it to the above equation gives

\[
\phi(y_1)(\phi\phi_j)(v_1) + \cdots + \phi(y_r)(\phi\phi_j)(v_r) = 0, \quad j = 1, \ldots, n.
\]

Note that the list of elements \( \phi\phi_j \) as \( j = 1, \ldots, n \) goes through all elements of \( G \), just in a different order. Thus we actually have that \( y_1, \ldots, y_r \in F \) satisfy

\[
\phi(y_1)\phi_j(v_1) + \cdots + \phi(y_r)\phi_j(v_r) = 0, \quad j = 1, \ldots, n, \quad \phi \in G.
\]

Form \( \phi(y_r) \) times original equation minus \( y_r \) times this equation to get

\[
(\phi(y_r)y_1 - y_r\phi(y_1))\phi_j(v_1) + \cdots + (\phi(y_r)y_r - y_r\phi(y_r))\phi_j(v_r) = 0, \quad j = 1, \ldots, n.
\]

Since \( \phi(y_r)y_r - y_r\phi(y_r) = 0 \), these equations are really of the form

\[
z_1\phi_j(v_1) + \cdots + z_{r-1}\phi_j(v_{r-1}) = 0, \quad j = 1, \ldots, n, \quad z_i = \phi(y_r)y_i - y_r\phi(y_i).
\]

Minimality of \( r \) (and the fact that \( r \geq 2 \)) means that we must have \( z_1 = \cdots = z_{r-1} = 0 \). That is, we have (since \( y_r \neq 0 \)) that

\[
\phi(y_i/y_r) = y_j/y_r, \quad i = 1, \ldots, r - 1.
\]

Since this is true for any \( \phi \in G \), we have that \( c_i := y_i/y_r \in L^G = F \). That is, \( y_i = c_i y_r \) for some \( c_1, \ldots, c_r \in F \), with \( c_r = 1 \).

Now take the original equations involving the \( y_i \)s and divide through by \( y_r \) to get

\[
c_1\phi_j(v_1) + \cdots + c_r\phi_j(v_r) = 0, \quad j = 1, \ldots, n.
\]

Since \( c_i \in F \) this says

\[
\phi_j(c_1v_1 + \cdots + c_rv_r) = 0, \quad j = 1, \ldots, n.
\]

In particular, taking \( \phi_j = \text{id} \) we get \( c_1v_1 + \cdots + c_rv_r = 0 \) with \( c_j \in F \) and \( c_r = 1 \neq 0 \). But this contradicts the \( F \)-linear independence of the \( v_i \)s. We have thus obtained the desired contradiction. \( \square \)

**Remark.** Here is a summary of the structure of the proof that \([L : L^G] = |G|\). The idea is that we formed the \( m \times n \)-matrix \( A = (\phi_j(v_i)) \in M_{m \times n}(L) \), where \( m = [L : L^G] \) and \( n = |G| \), with \( v_1, \ldots, v_m \) an \( L^G \)-basis of \( L \) and \( \phi_1, \ldots, \phi_n \in G \).

We need to show \( A \) is a square matrix. We do this by showing it is a nonsingular matrix. We do this by showing that

\[
Ax = 0 \quad \text{implies} \quad x = 0 \quad \text{for all} \quad x \in M_{n \times 1}(L),
\]

and

\[
yA = 0 \quad \text{implies} \quad y = 0 \quad \text{for all} \quad y \in M_{1 \times m}(L).
\]
This proves rank $A = n$ and rank $A = m$, and thus $m = n$. We do this in each case using the observations that
\[
A \begin{bmatrix} x_1 \\ \vdots \\ x_m \end{bmatrix} = 0 \implies A \begin{bmatrix} \phi_1(c)x_1 \\ \vdots \\ \phi_m(c)x_m \end{bmatrix} = 0 \quad \text{for all } c \in L,
\]
and
\[
[ y_1 \cdots y_m ] A = 0 \implies [ \phi(y_1) \cdots \phi(y_m) ] A = 0 \quad \text{for all } \phi \in G.
\]
In each case, you use these to show that the existence of even one non-trivial element of the column-null-space or row-null-space implies the existence of one with only one non-zero component, which is then seen to be impossible.

### 38. Normal closure

Let $K : F$ be a a finite extension. A **normal closure** of it is an extension $N : K$ such that

(i) $N : F$ is normal, and (ii) if $K \subseteq M \subseteq N$ and $M : K$ is normal, then $M = N$. It’s a “smallest normal extension of $F$ which contains $K$”.

**Example.** If $K : F$ is already normal then the normal closure is $K$.

**Example.** If $K = F(\alpha)$ with $\alpha$ algebraic over $F$, then a normal closure is exactly a splitting field $\Sigma$ of $f = f_{\alpha/F} \in \text{Irred}(F)$. This is because given $F \subseteq K \subseteq \Sigma$ with $M : F$ normal, $f$ has a root in $M$ and so splits over $M$.

**Example.** If $K = F(\alpha_1, \ldots, \alpha_r)$ with all $\alpha_j$ algebraic over $F$, then a normal closure is exactly a splitting field of $f = f_1 \cdots f_r$ where $f_j = f_{\alpha_j/F} \in \text{Irred}(F)$. Proof is the same as in the previous example.

**Proposition.** Every finite extension $K : F$ has a normal closure.

**Proof.** Since $[K : F] < \infty$ we have $K = F(\alpha_1, \ldots, \alpha_r)$ for some finite list of algebraic elements. A normal closure is a splitting field, as in the previous example. \qed

In particular, if $F \subseteq K \subseteq \mathbb{C}$, then there is a unique normal closure which is a subfield of $\mathbb{C}$: the normal closure must be a splitting field of the polynomial $f$ constructed in the proof, so this is unique.

Similarly, abstract normal closures are unique up to isomorphism.

**Remark.** “Normal closure” is basically a way of talking about splitting fields of polynomials without mentioning any particular polynomial.

**Proposition.** Let $K : F$ be a finite separable extension with $[K : F] = n$. Let $N : F$ be a normal closure of $K : F$. Then
\[
|\text{Hom}_F(K, N)| = [K : F] = n.
\]

Note that we have already proved (by linear independence of homomorphisms) that for any finite extension $K : F$ we must have $|\text{Hom}_F(K, N)| \leq [K : F]$.

**Proof.** Since $[K : F] < \infty$, we can write $K = F(\alpha_1, \ldots, \alpha_r)$. Let $K_j = F(\alpha_1, \ldots, \alpha_j)$, so that $K_0 = F$ and $K_r = K$. I will show for all $j = 0, \ldots, r$ that
\[
|\text{Hom}_F(K_j, N)| = [K_j : F].
\]

The case of $j = 0$ is clear.

By the tower law $[K_j : F] = [K_j : K_{j-1}] [K_{j-1} : F]$. Thus, it will suffice to show that for each $\psi \in \text{Hom}_F(K_{j-1}, N)$, there are exactly $n_j = [K_j : K_{j-1}]$ homomorphisms
\[
\phi : K_j \to N \quad \text{such that } \phi|_{K_{j-1}} = \psi.
\]
This will imply that
\[ |\text{Hom}_F(K_j, N)| = n_j |\text{Hom}_F(K_{j-1}, N)|. \]
Combined with the induction hypothesis this gives
\[ |\text{Hom}_F(K_j, N)| = [K_j : K_{j-1}][K_{j-1} : N] = [K_j : N] \]
as desired.

Fix an $F$ homomorphism $\psi : K_{j-1} \to N$. We have that $K_j = K_{j-1}(\alpha_j)$, where $\alpha_j$ has some minimal polynomial $f_j = f_{\alpha_j/K_{j-1}} \in \text{Irred}(K_{j-1})$ of degree $n_j = [K_j : K_{j-1}]$. Note that $f_j$ must divide $g := f_{\alpha_j/F} \in \text{Irred}(F)$ in $K_{j-1}[X]$, whence the image $f'_j = \psi(f_j)$ must divide $\psi(g) = g$ in $N[X]$. Since $N$ is a normal closure of $K : F$ and $g$ has a root $\alpha_j$ in $K$, we must have that $g$ splits over $N$. Therefore its factor $f'_j$ splits over $N$. Note that because $K : F$ is a separable extension the minimal polynomial of $f_j \in K$ is separable, and therefore $f'_j$ is also separable since it is the image of $f_j$ under a homomorphism.

Now recall that there is a bijection
\[ \{ \phi : K_j \to N \mid \phi|_{K_{j-1}} = \psi \} \leftrightarrow \{ \beta \in N \mid f'_j(\beta) = 0 \}. \]
That is, the number of ways to extend $\psi$ to $\phi$ is equal to the number of roots of $f'_j$, which is $n_j = \deg f'_j$ since it is separable. This is exactly what we needed to prove.

Finally we obtain the second technical lemma.

**Proposition.** Let $K : F$ be a finite and separable extension. Then
\[ |\text{Aut}(K : F)| \leq [K : F], \]
with equality if and only if $K : F$ is also normal.

**Proof.** Choose a normal closure $N$ of $K : F$ so that $K \subseteq N$. We have proved that
\[ |\text{Hom}_F(K, N)| = [K : F]. \]

Since $\text{Aut}(K : F) = \text{Hom}_F(K, K) \subseteq \text{Hom}_F(K, N)$ we immediately get the desired inequality.

It remains to prove the equivalence of equality and normality. If $K : F$ is normal then $N = K$, so
\[ \text{Aut}(K : F) = \text{Hom}_F(K, N), \]
whence $|\text{Aut}(K : F)| = [K : F]$.

Conversely suppose $|\text{Aut}(K : F)| = [K : F]$, and choose a normal closure $N$ of $K : F$ so that $K \subseteq N$. The hypothesis on the size of the automorphism group implies that both $\text{Hom}_F(K, N)$ and its subset $\text{Hom}_F(K, K) = \text{Aut}(K : F)$ have the same cardinality $[K : F]$, whence $\text{Hom}_F(K, N) = \text{Hom}_F(K, K)$, i.e., every $F$-homomorphism $\phi : K \to N$ has image contained in $K$, whence $\phi(K) = K$.

Now to show $K : F$ is normal when $|\text{Aut}(K : F)| = [K : F]$, suppose $f \in \text{Irred}(F)$ with a root $\alpha \in K$. We know $f$ splits over the normal closure $N$ of $K : F$ since $N : F$ is normal. So it is enough to show that all the roots of $f$ in $N$ contained in the subfield $K$.

Let $\beta \in N$ be any root of $f$. Following the proof above of the previous proposition, we can first (i) construct an $F$-homomorphism $\psi : F(\alpha) \to N$ sending $\alpha \mapsto \beta$, and then (ii) extend to a homomorphism $\phi : K \to N$ such that $\phi|_{F(\alpha)} = \psi$. Therefore $\beta \in \phi(K)$, the subfield which is the image of $K$ under $\phi$.

But we have already observed that $|\text{Aut}(K : F)| = [K : F]$ implies that $\phi(K) = K$. Therefore $\beta = \phi(\alpha) \in K$ as desired.

**Remark.** The last part of the above proof shows that the normal closure $N$ of a finite extension $K : F$ is generated as a field over $F$ by all the subfields $\phi(K)$ which are images of $K$ under elements $\phi \in \text{Hom}_F(K, N)$. 
39. Solvable groups

We are going to show that (in characteristic 0) that whether a given polynomial \( f \in F[X] \) admits a solution in terms of radicals is entirely determined by a property of its Galois group \( \text{Gal}(f) = \text{Aut}(\Sigma_{f/F} : F) \), namely whether the group is solvable.

A group \( G \) is \textbf{solvable} if there exists a finite sequence of subgroups
\[
\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_{n-1} \subseteq G_n = G
\]
such that (i) each \( G_{i-1} \) is a normal subgroup of \( G_i \), and (ii) the quotient group \( G_i/G_{i-1} \) is abelian.

\textbf{Remark.} Warning: “is a normal subgroup of” is not a transitive relation. It is possible to have a chain of subgroups \( G_1 \subseteq G_2 \subseteq G \) such that \( G_1 \triangleleft G_2 \) and \( G_2 \triangleleft G_3 \), but \( G_1 \not\triangleleft G_3 \).

There is an analogous statement on the field extension side: you can have a chain of extensions \( L_1 \subseteq L_2 \subseteq L_3 \) such that \( L_2 : L_1 \) and \( L_3 : L_2 \) are normal but \( L_3 : L_1 \) is not normal.

\textbf{Example.} Consider the chain of extensions \( \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}((\sqrt{2}), i) \), so that \( L = \mathbb{Q}((\sqrt{2}), i) \) is the splitting field of \( f = X^4 - 2 \in \text{Irred}(\mathbb{Q}) \). Then \( \mathbb{Q}(\sqrt{2}) : \mathbb{Q} \) and \( \mathbb{Q}((\sqrt{2}), i) : \mathbb{Q}(\sqrt{2}) \) are normal extensions (because all degree 2 extensions are normal), but \( \mathbb{Q}((\sqrt{2}), i) : \mathbb{Q} \) is not normal (since \( f \) has a root in it but doesn’t split).

This is parallel to the same phenomenon for the chain of subgroups of \( D_8 \cong \text{Aut}(\mathbb{Q}(\alpha, i) : \mathbb{Q}) \) given (in the notation of an earlier example) by \( \langle s \rangle \leq \langle s, r^2 \rangle \leq D_8 \); so \( \langle s \rangle \) is not normal in \( D_8 \), but the index-2 inclusions are normal (because index-2 subgroups are always normal).

\textbf{Proposition.} Let \( \{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_r = G \) be a chain of subgroups of \( G \), such that \( G_{i-1} \triangleleft G_i \). If each \( G_i/G_{i-1} \) is solvable, then \( G \) is solvable.

\textbf{Proof.} By induction on \( r \), it suffices to consider the case of \( r = 2 \). So consider \( N \triangleleft G \) with both \( N \) and \( G/N \) solvable.

Let \( \{N_i\} \) be a sequence of subgroups of \( N \), with smallest group \( N_0 = \{e\} \), largest group \( N_r = N \), with \( N_{i-1} \triangleleft N_i \) and \( N_i/N_{i-1} \) abelian. Likewise let \( \{Q_j\} \) be a sequence of subgroups of \( Q = G/N \), with smallest element \( Q_0 = \{e\} \), largest element \( Q_s = Q \), with \( Q_{i-1} \triangleleft Q_i \) and \( Q_i/Q_{i-1} \) abelian.

Define \( G_i = N_i \) for \( i = 0, \ldots, r \), and define \( G_{r+j} = \pi^{-1}(Q_j) \) for \( j = 0, \ldots, s \), where \( \pi : G \rightarrow Q = G/N \) is the projection homomorphism. Then \( \{G_i\} \) is a chain of subgroups with \( G_0 = \{e\}, G_{r+s} = G \), each \( G_{i-1} \triangleleft G_i \), and \( G_i/G_{i-1} \) abelian. So \( G \) is solvable. \( \Box \)

\textbf{Proposition.} Let \( G \) be a group with subgroup \( H \). Then

(1) if \( G \) is solvable then \( H \) is solvable, and

(2) if \( G \) is solvable and \( H \) is a normal subgroup, then \( G/H \) is solvable.

\textbf{Proof.} Choose a finite sequence of subgroups \( \{G_i\} \) for \( G \) with \( G_{i-1} \triangleleft G_i \) and \( G_i/G_{i-1} \) abelian, and with largest group equal to \( G \) and smallest group equal to \( \{e\} \).

(1) Let \( H_i = H \cap G_i \). Then the sequence \( \{H_i\} \) has analogous properties relative to \( H \): the largest subgroup in the sequence in \( H \), the smallest is \( \{e\} \), \( H_{i-1} \) is normal in \( H_i \), and \( H_i/H_{i-1} \) is abelian (since it is isomorphic to a subgroup of \( G_i/G_{i-1} \)).

(2) Let \( K_i = G_i/H \), which is a subgroup of \( G \) since \( H \) is normal in \( G \). Then the sequence \( \{K_i\} \) has the properties that: its smallest element is \( H \), its largest element is \( G \), each \( K_{i-1} \) is normal in \( K_i \), and each \( K_i/K_{i-1} \) is abelian (since it is isomorphic to a quotient group of \( G_i/G_{i-1} \)).

Let \( Q = G/H \), and let \( Q_i = K_i/H \), a subgroup of \( Q \). Then the sequence \( \{Q_i\} \) has largest element \( Q \) and smallest element \( \{e\} \), each \( Q_{i-1} \) is normal in \( Q_i \) with abelian quotient group \( Q_i/Q_{i-1} \approx K_i/K_{i-1} \). \( \Box \)

\textbf{Example.} Examples of solvable finite groups include: every abelian group, every dihedral group \( D_n \), the symmetric and alternating groups \( A_n \) and \( S_n \) for \( n = 1, \ldots, 4 \).
A group $G$ is simple if it has exactly two normal subgroups, namely $\{e\}$ and $G$. (This excludes the trivial group.)

Abelian simple groups are exactly cyclic groups of prime order. Non-abelian simple groups are clearly not solvable. We will soon show that $A_n$ is simple for $n \geq 5$, whence, since it is non-abelian, both $A_n$ and $S_n$ are not solvable for $n \geq 5$.

**Remark.** A famous (but very difficult) result in group theory is the Feit-Thompson odd order theorem, which says that every finite group of odd order is solvable. (The original proof was over 200 pages, and modern improvements aren’t really any shorter.)

40. Radical extensions

Let us discuss the following situation. Assume $n \geq 1$, and let $F \subseteq \mathbb{C}$. Consider $a \in F$ and $f = X^n - a \in F[X]$, and let $L = \Sigma_{f/F}$ be the splitting field in $\mathbb{C}$.

If $a = 0$ then $L = F$, so assume $a \neq 0$. Then $D(f) = nX^{n-1}$ is clearly relatively prime to $f$, so $f$ is separable.

Write $\alpha \in \mathbb{C}$ for a chosen root of $f$. Then it is clear that all roots of $f$ are $\{\alpha\zeta^k \mid k = 0, \ldots, n-1\}$, where $\zeta = e^{2\pi i/n}$. Thus

$$L = F(\alpha, \alpha\zeta, \ldots, \alpha\zeta^{n-1}) = F(\zeta, \alpha).$$

We have a chain of extensions

$$F \subseteq F(\zeta) \subseteq F(\zeta, \alpha) = L.$$

Let $G = \text{Aut}(L : F)$ with subgroup $H = \text{Aut}(L : F(\zeta))$. The extension $F(\zeta) : F$ is a splitting field of $X^n - 1$, so is normal. Thus $H \triangleleft G$ and $Q = \text{Aut}(F(\zeta) : F) \approx G/H$.

Any element of $Q = \text{Aut}(F(\zeta) : F)$ must permute the roots of $X^n - 1$, which is the set of $n$th roots of unity. In fact, it will also permute roots of $X^m - 1$ for any $m \mid n$, which means that it will permute the set of primitive $n$th roots of unity. Since the extension is generated by $\zeta$, any such element $\sigma \in Q$ is uniquely determined by

$$\sigma_j(\zeta) = \zeta^j, \quad \text{for some } j \in \mathbb{Z}, \gcd(j, n) = 1.$$

Note: I am not asserting that every such $j$ must give an element $\sigma_j$ of $Q = \text{Aut}(F(\zeta) : F)$; for instance, it could be that $F(\zeta) = F$. Just that any elements of $Q$ which do exist must be of this form.

Note that

$$\sigma_{j+k} = \sigma_j, \quad \sigma_j\sigma_k = \sigma_{j+k} = \sigma_k\sigma_j \quad \text{for all } j, k \in \mathbb{Z}.$$

The second identity is just the calculation $\sigma_j(\sigma_k(\zeta)) = \sigma_j(\zeta^k) = \sigma_j(\zeta)^k = (\zeta^j)^k = \zeta^{jk}$. In particular, $Q$ is an abelian group, and is in fact isomorphic to a subgroup of $(\mathbb{Z}/n)^\times$.

Any element of $H = \text{Aut}(L : F(\zeta))$ must permute the roots of $X^n - a$. Since the extension is generated by $\alpha$, any such element has the form and is uniquely determined by

$$\tau_k(\alpha) = \alpha\zeta^k, \quad \text{for some } k \in \mathbb{Z}.$$

Again, not every such $k$ needs to correspond to an element $\tau_k$ of $H$.

Note that

$$\tau_{k+jn} = \tau_k, \quad \tau_j\tau_k = \tau_{j+k} = \tau_k\tau_j \quad \text{for all } j, k \in \mathbb{Z}.$$

The second identity is just the calculation $\tau_j(\tau_k(\alpha)) = \tau_j(\alpha\zeta^k) = \tau_j(\alpha)\zeta^k = \alpha\zeta^{j+k}$. In particular, $H$ is an abelian group, and is in fact isomorphic to a subgroup of $\mathbb{Z}/n$.

Using the chain of subgroups $\{e\} \subseteq H \subseteq G$, we have proved the following.

**Proposition.** Let $n \geq 1$, let $F \subseteq \mathbb{C}$, and let $L$ be the splitting field of $f = X^n - a \in F[X]$. Then $G = \text{Aut}(L : F)$ is solvable.
Remark. The above proof shows that for a primitive $n$th root of unity $\zeta_n$, the group $\text{Aut}(F(\zeta_n) : F)$ is isomorphic to a subgroup of $\langle \mathbb{Z}/n \rangle^\times$. We will later be able to show that for $F = \mathbb{Q}$ this becomes an equality; in fact, we already know this when $n$ is a prime, since $f_{\zeta_p/Q} = \Phi_p$ is irreducible over $\mathbb{Q}$.

Stewart (Lemma 15.4 in the book) seems to think you need to know that $n$ is prime in order to show that $\text{Aut}(F(\zeta) : F)$ is abelian, but this is clearly not the case.

Remark. Suppose that in the above situation, $G$ is as large as it can be. That is, $|Q| = \phi(n) := |\langle \mathbb{Z}/n \rangle^\times|$ and $|H| = n$, so $|G| = n\phi(n)$. Note that since $L : F(\zeta)$ is a simple extension generated by $\alpha$, this implies $f = X^n - a$ is still irreducible over $F(\zeta)$, i.e., $f = f_{\alpha/F(\zeta)}$, but also $f \in F[X]$.

This implies that $\sigma_j \in \text{Aut}(F(\zeta) : F)$ therefore sends the minimal polynomial $f_{\alpha/F(\zeta)}$ of $\alpha$ over $F(\zeta)$ to itself (since $f_{\alpha/F(\zeta)} = f \in F[X]$), we can extend $\sigma_j$ to an automorphism of $L$ by sending $\alpha$ to any root of $f$. In particular, let’s extend it so that $\sigma_j(\alpha) = \alpha$. So we have identities

$$
\begin{align*}
\sigma_j(\alpha) &= \alpha, \\
\tau_k(\alpha) &= \alpha \zeta^k, \\
\sigma_j(\zeta) &= \zeta^j, \\
\tau_k(\zeta) &= \zeta.
\end{align*}
$$

In particular, we deduce the relation $\sigma_j \tau_k = \tau_k \sigma_j$. This completely describes the structure of the group $G$. The distinct elements of $G$ are given by

$$
\tau_k \sigma_j, \quad k \in \mathbb{Z}/n, \quad j \in \langle \mathbb{Z}/n \rangle^\times,
$$

and the group structure is determined by $\tau_j \tau_k = \tau_{j+k}$, $\sigma_j \sigma_k = \sigma_{jk}$, and $\sigma_j \tau_k = \tau_k \sigma_j$.

The group $G$ is an example of a semi-direct product of $\mathbb{Z}/n$ by $\langle \mathbb{Z}/n \rangle^\times$.

In general, $G$ is only a subgroup of this semi-direct product. In the general case, you can lift $\sigma_j \in Q$ to some element of $G$, but you won’t complete control over what the lift does to $\alpha$.

Exercise. Show that for a prime $p$ the Galois group of $X^p - 2$ over $\mathbb{Q}$ has maximal order $p(p - 1)$.

We are going to have to worry about situations where we adjoin $\alpha = \sqrt[p]{a}$ to some field $F$, but the minimal polynomial $g = f_{\alpha/F}$ of $\alpha$ is not the same as $f = X^n - a$, so that $f$ might not split over the normal closure of $F(\alpha) : F$.

Exercise. Find an example where this happens when $F = \mathbb{Q}$.

It turns out things are ok if $n$ is a prime.

Lemma. Let $F \subseteq \mathbb{C}$, $p$ a prime number. Let $\alpha \in \mathbb{C}$ be such that $a = \alpha^p \in F$, and let $g = f_{\alpha/F} \in F[X]$ be its minimal polynomial over $F$. Then either

1. $\alpha \in F$, or
2. $f = X^p - a$ and $g$ have the same splitting field over $F$.

Proof. Left as an exercise. \qed

Recall that $L : F$ is a **radical extension** if there exist $\alpha_1, \ldots, \alpha_r$ in $L$ and $n_1, \ldots, n_r \geq 1$ such that $L = F(\alpha_1, \ldots, \alpha_r)$ and

$$
\alpha_{n_j}^{n_j} \in F(\alpha_1, \ldots, \alpha_{j-1}) \quad \text{for each} \quad j = 1, \ldots, r.
$$

Note that without loss of generality we can assume that each $n_j$ is prime. This is because, if $\alpha^n \in F$ and $n = p_1 \cdots p_k$, we can let

$$
\beta_1 = \alpha^{p_2 \cdots p_k}, \quad \beta_2 = \alpha^{p_3 \cdots p_k}, \quad \ldots \quad \beta_{k-1} = \alpha^{p_{k-1}}, \quad \beta_k = \alpha.
$$

Then we get a chain of extensions

$$
F \subseteq F(\beta_1) \subseteq F(\beta_2) \subseteq \cdots \subseteq F(\beta_k) = F(\alpha)
$$

with $\beta_j^{p_j} \in F(\beta_{j-1})$. 

\[M 14\text{ Oct}\]
Proposition. For any $F \subseteq L \subseteq \mathbb{C}$ such that $L : F$ is a finite normal radical extension, the group $G = \text{Aut}(L : F)$ is solvable.

Proof. Consider a radical extension $L = F(\alpha_1, \ldots, \alpha_r)$, with $\alpha_j = \alpha_j^{p_j} \in F(\alpha_1, \ldots, \alpha_{j-1})$ for some $p_j \geq 1$ and $j = 1, \ldots, r$, where each $p_j$ is a prime number.

Furthermore assume $\alpha_j \notin F(\alpha_1, \ldots, \alpha_{j-1})$.

Since $L : F$ is a normal extension, we can inductively define a chain of extensions

$$F = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_{r-1} \subseteq L_r = L$$

so that each $L_j$ is the normal closure of $L_{j-1}(\alpha_j) : L_{j-1}$ in $L$. In particular, $F(\alpha_1, \ldots, \alpha_j) \subseteq L_j$.

Therefore each $L_j$ is a splitting field of $f_{\alpha_j} / L_{j-1} \in \text{Irred}(L_{j-1})$. By the previous lemma, for each $j = 1, \ldots, r$ we have either

1. $\alpha_j \in L_{j-1}$, so $L_j = L_{j-1}$, or
2. $L_j : L_{j-1}$ is a splitting field of $X^{p_j} - a_j$.

Thus by construction, each extension $L_j : L_{j-1}$ is a normal extension.

Now let $G = \text{Aut}(L : F)$, and set $G_j = \text{Aut}(L : L_j)$ for $j = 0, \ldots, r$. We obtain a chain of subgroups

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_{r-2} \supseteq G_{r-1} \supseteq G_r = \{e\}$$

with the property that each $G_j$ is a normal subgroup of $G_{j-1}$, since $L_j : L_{j-1}$ is a normal extension. Furthermore, $G_{j-1} \approx \text{Aut}(L : L_{j-1})$ and $G_{j-1} / G_j \approx \text{Aut}(L_j : L_{j-1})$.

If $L_j = L_{j-1}$ then $G_{j-1} = G_j$. Otherwise $L_j : L_{j-1}$ is a splitting field of some $X^{p_j} - a_j$, we have by the earlier proposition that $G_{j-1}/G_j$ is solvable. Therefore $G$ is solvable, since we have found a suitable chain of subgroups $\{G_j\}$ so that each quotient group is solvable. \hfill $\square$

We say that a polynomial $f \in F[X]$ is solvable by radicals if its splitting field $\Sigma$ is contained in an $L$ such that $L : F$ is a radical extension.

Proposition. If $F \subseteq K \subseteq L$ and $L : F$ is a radical extension, then $\text{Aut}(K : F)$ is solvable.

Proof. First I show that any radical extension is contained in a finite normal radical extension.

Since $L : F$ is radical, we have a chain of extensions with $L_0 = F$, $L_r = L$, and $L_j = L_{j-1}(\alpha_j)$ where $\alpha_j^{n_j} \in L_{j-1}$. Inductively define $N_j$ so that $N_0 = F$, and $N_j$ is a normal closure of $N_{j-1}(\alpha_j)$, i.e., $N_j : N_{j-1}$ is a splitting field for $f_{\alpha_j} / N_{j-1}$. Then $N = N_r$ is a normal radical extension containing $L$.

So assume $L : F$ is a finite normal radical extension, with Galois group $G = \text{Aut}(L : F)$ which is solvable. If $K : F$ is also normal then $\text{Aut}(K : F) \approx G / H$, where $G = \text{Aut}(L : F)$ and $H = \text{Aut}(L : K)$. Since $G$ is solvable so is the quotient group $H$.

More generally, $\text{Aut}(K : F) \approx N/H$, where $N \leq G$ is the normalizer of $H = \text{Aut}(L : K)$. Since $N$ is a subgroup of a solvable group it is solvable, whence so is its quotient group $N/H$. \hfill $\square$

## 41. An insolvable quintic

Let $f = X^5 - 6X + 3 \in \mathbb{Q}[X]$. We show this cannot be solved by radicals over $\mathbb{Q}$.

First note that $f$ is irreducible, using Eisenstein’s criterion with $p = 3$. This implies that $f$ is separable.

We have that

$$f(-2) = -17, \quad f(0) = +3, \quad f(1) = -2, \quad f(2) = +23.$$

Therefore by the intermediate value theorem $f$ has at least three real roots, which lie in $(-2, 0)$, $(0, 1)$, and $(1, 2)$ respectively. However $Df = 5X^4 - 6$ has exactly two real roots $\pm \sqrt[4]{5/6}$, which means that the derivative of $f$ can switch signs in at most two places. Therefore $f$ has exactly three real roots.

From Chapter 15.
**Proposition.** Let $p$ be a prime, and $f \in \text{Irred}(\mathbb{Q})$ with $\deg f = p$. If $f$ has exactly two non-real roots in $\mathbb{C}$, then $\text{Gal}(f) \approx S_p$.

We are going to need Cauchy’s theorem.

**Theorem (Cauchy).** If $G$ is a finite subgroup and a prime $p$ divides $|G|$, then $G$ contains an element of order $p$.

**Proof.** This is Theorem 14.15 in the book. I’ll sketch a different proof here.

Let $X = \{ (g_1, \ldots, g_p) \in G^p \mid g_1 \cdots g_p = e \}$. Note that if $(g_1, \ldots, g_p) \in X$ so is $(g_k, \ldots, g_p, g_1, \ldots, g_{k-1})$ for any $k$. Define an equivalence relation on $X$ by

$$(g_1, \ldots, g_p) \sim (h_1, \ldots, h_p)$$

if there exists $k$ such that $(h_1, \ldots, h_p) = (g_k, \ldots, g_p, g_1, \ldots, g_{k-1})$.

There are exactly two kinds of equivalence classes:

- singleton classes $\{(g, \ldots, g)\}$, where $g \in G$ is such that $g^p = e$, and
- non-singleton classes, each of which has size exactly $p$.

Let $s$ be the number of singleton classes. We have $s \geq 1$, since $e^p = e$. If $s > 1$ then we must have an element of order $p$ in $G$.

We see that $|X| = |G|^{p-1}$, since $g_p = g_{p-1}^{-1} \cdots g_1^{-1}$. Thus $p \mid |X|$, whence $p \mid s$. Since $s \geq 1$ this means $s > 1$ as desired.

We are going to need various facts about elements of symmetric groups:

- Disjoint cycles commute.
- Every element is equal to a product of pairwise disjoint cycles, uniquely up to reordering.
- If $c = (a_1 \cdots a_m)$ is a cycle and $g \in S_n$, then $g cg^{-1} = (a_{g(1)} \cdots a_{g(n)})$.
- Even permutations are those which can be written as a product of an even number of transpositions (2-cycles), not necessarily disjoint.

**Proof.** Let $f \in \text{Irred}(\mathbb{Q})$ with $\deg f = p$ and exactly two real roots. Let $\Sigma : \mathbb{Q}$ be the splitting field of $f$, and let $G = \text{Aut}(\Sigma : \mathbb{Q})$. By labelling the roots of $f$ as $\alpha_1, \ldots, \alpha_p$ in some way we can identify $G$ as a subgroup of $S_p$.

Because $f \in \mathbb{Q}[X] \subseteq \mathbb{R}[X]$, complex conjugation $t$ is an automorphism of the splitting field $\Sigma$, so acts on the set of roots. Since there are exactly two non-real roots, it acts as a transposition (a 2-cycle) on the set of roots. Write $\alpha_1$ and $\alpha_2$ for these two non-real roots.

Because $f$ is irreducible, any root $\alpha$ of $f$ gives $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \Sigma$ with $|\mathbb{Q}(\alpha) : \mathbb{Q}| = \deg f = p$. Thus $p \mid |\Sigma : \mathbb{Q}| = |G|$. By Cauchy’s theorem there exists an element of order $p$ in $G$.

In $S_p$ the only elements of order $p$ are $p$-cycles. Pick such a $p$-cycle $g$. Then $\{ g^k(\alpha_1) \mid 1 \leq k \leq p-1 \}$ is the set of all roots other than $\alpha_1$. In particular, there is a $k$ such that $g^k(\alpha_1) = \alpha_2$. Since $p \nmid k$, we see that $c = g^k$ is also a $p$-cycle. Now use this to label the roots so that $\alpha_k := c^{k-1}(\alpha_1)$.

To summarize, we have $G \leq S_p$ with $t, c \in G$, with $t = (1 \, 2)$ and $c = (1 \, 2 \cdots p)$. We will show that $t$ and $c$ generate $S_p$, which implies that $G = S_p$. For this part, $p$ doesn’t need to be prime.

Note that

$$c^{k-1}(1 \, 2)c^{-(k-1)} = (k \, k+1), \quad k = 1, \ldots, p-1,$$

whence the transpositions $(1 \, 2), (2 \, 3), \ldots, (p-1 \, p)$ are all in $G$. From this we get

$$(a \, a+1 \, \cdots \, b) = (a \, a+1)(a+1 \, a+2) \cdots (b-2 \, b-1)(b-1 \, b), \quad a < b.$$ 

and so

$$(a \, b) = (a+1 \, a+2 \cdots b-1 \, b)^{-1}(a+1 \, a+2 \cdots b-1 \, b), \quad a < b.$$

Thus $G$ contains all transpositions, and from this it is easy to see that $G = S_p$.
Thus $\text{Gal}(f) = S_5$. Next I claim that $A_5$ is a simple group, and thus not solvable since it is non-abelian, and therefore $S_5$ is not solvable. Later I’ll prove that $A_n$ is simple for all $n \geq 5$, but first I give a quick proof for $n = 5$.

Conjugacy classes in $S_5$ correspond to cycle-decompositions. The only $S_5$-conjugacy classes contained in $A_5$ are:

- $\{e\}$,
- set of pairs of disjoint 2-cycles $(a \, b)(c \, d)$,
- set of 3-cycles $(a \, b \, c)$,
- set of 5-cycles $(a \, b \, c \, d \, e)$.

Now, although these are conjugacy classes in $S_5$, they can fail to be conjugacy classes in $A_5$.

In general, if $[G : H] = 2$, and if $C \subseteq H$ is a $G$-conjugacy class, one of two things can happen:

1. $C$ is also an $H$-conjugacy class, or
2. $C$ is a disjoint union of two $H$-conjugacy classes, of equal size.

Exercise: show that if $C \subseteq H$ is a $G$-conjugacy class, and there exist $c \in C$ and $g \in G \setminus H$ such that $gc = cg$, then (2) happens, and that if no such $c, g$ exist then (1) happens.

In the case of $A_5$, it turns out that the 5-cycles split into two $A_5$-conjugacy classes, but the other classes don’t split. So these are the $A_5$-conjugacy classes:

- Just $e$: size 1.
- Pair of disjoint 2-cycles: size 15.
- 3-cycles: size 20.
- 5-cycles conjugate to $c$: size 12.
- 5-cycles conjugate to $c^2$: size 12.

A normal subgroup $N \triangleleft A_5$ must have order dividing $|A_5| = 60$, and must be a union of conjugacy classes, one of which must be $\{e\}$. Going through the possible cases shows that you can only have $N = \{e\}$ or $N = A_5$.

42. $A_n$ is simple, $n \geq 5$

I’ll sketch a general proof that $A_n$ is simple for all $n \geq 5$.

1. Show that the set of all 3-cycles generates $A_n$.
2. Show that if $N \triangleleft A_n$ is a normal subgroup which contains a 3-cycle, then it contains every 3-cycle.
3. Show that if $N \triangleleft A_n$ is a non-trivial normal subgroup and $n \geq 5$, then $N$ contains a 3-cycle.

To show (1), recall that the subgroup $A_n$ consists of even permutations, which are exactly those which are a product of an even number of 2-cycles. Any product of two 2-cycles (disjoint or not) can be written as a product of 3-cycles: for distinct elements $a, b, c, d \in \{1, \ldots, n\}$, we have

$$(a \, b)(a \, b) = e, \quad (a \, b)(a \, c) = (a \, c \, b), \quad (a \, b)(c \, d) = (a \, d \, c)(a \, b \, c).$$

To show (2), suppose $N$ contains a 3-cycle. If $n = 3$ this implies $N = A_3$ already, so suppose $n \geq 4$.

I’ll show that if $N$ contains a 3-cycle $(a \, b \, c)$ (and thus also contains $(a \, c \, b) = (a \, b \, c)^{-1}$), it must contain any 3-cycle involving just two of $a, b, c$. To get a 3-cycle involving $a, b, x \notin \{a, b, c\}$, use

$$(a \, x \, b) = (b \, x \, c)(a \, b \, c)(b \, x \, c)^{-1} \in N,$$

since $A_n$ contains the 3-cycle $(b \, x \, c)$. Therefore also $(a \, b \, x) = (a \, x \, b)^{-1} \in N$.

By repeating this trick, we can show that every 3-cycle is in $N$.

Finally we show (3), i.e., that a non-trivial normal $N$ contains a 3-cycle if $n \geq 5$. We start by assuming some element $g \in N$ with $g \neq e$, which we can write as a product of disjoint
cycles: \( g = c_1 \cdots c_k \) with \( k \geq 1 \). I’ll assume the cycles are listed in terms of descending order, so \( \text{order}(c_1) \geq \text{order}(c_2) \geq \cdots \).

We use the following trick. If \( t \in A_n \) is any 3-cycle, then \( tgt^{-1}g^{-1} \in N \). Because cycles which are disjoint commute, we see that if the elements of \( t \) are disjoint from those of \( c_j+1, \ldots, c_k \), then \( tgt^{-1}g^{-1} = t(c_1 \cdots c_j)t^{-1}(c_1 \cdots c_j)^{-1} \).

(a) Suppose \( \text{order}(c_1) = m \geq 4 \). Write \( c_1 = (a_1 \cdots a_m) \), and let \( t = (a_1 a_2 a_3) \). Observe that

\[
\text{order}(c_1) = \text{order}(c_2) = 3, \quad g = (a_1 a_2 a_3)(a_4 a_5 a_6)x \quad \text{with} \quad x \text{ disjoint from} \quad c_1 \quad \text{and} \quad c_2.
\]

Let \( t = (a_2 a_3 a_4) \). Then

\[
tc_1c_2t^{-1} = (a_1 a_3 a_4)(a_2 a_5 a_6)
\]

and thus

\[
tgt^{-1}g^{-1} = t(c_1c_2)t^{-1}(c_1c_2)^{-1} = (a_1 a_4 a_2 a_3 a_5)
\]

is a 5-cycle in \( N \), so \( N \) contains a 3-cycle by (a).

(b) Now suppose \( \text{order}(c_1) = \text{order}(c_2) = 3 \), so \( g = (a_1 a_2 a_3)(a_4 a_5 a_6)x \) with \( x \) disjoint from \( c_1 \) and \( c_2 \). Let \( t = (a_2 a_3 a_4) \). Then

\[
tc_1c_2t^{-1} = (a_1 a_3 a_4)(a_2 a_5 a_6)
\]

and thus

\[
tgt^{-1}g^{-1} = t(c_1c_2)t^{-1}(c_1c_2)^{-1} = (a_1 a_4 a_2 a_3 a_5)
\]

is a 5-cycle in \( N \), so \( N \) contains a 3-cycle by (a).

(c) Now suppose \( \text{order}(c_1) = 3 \) is the only 3-cycle in the decomposition, so \( g = c_1x \) with \( x \) a product of disjoint 2-cycles which are also disjoint from \( c_1 \). Then \( x^2 = e \), so \( g^2 = c_1x = c_1^2x^2 = c_1^2 \) which is a 3-cycle in \( N \).

(d) Now suppose all \( c_i \) are 2-cycles, so \( g = c_1c_2x \), with \( c_1 = (a_1 a_2) \), \( c_2 = (a_3 a_4) \), and \( x \) a product of disjoint 2-cycles also disjoint from the first two. Let \( t = (a_2 a_3 a_4) \). Then

\[
tc_1c_2t^{-1} = (a_1 a_3 a_4)
\]

and thus

\[
h := tgt^{-1}g^{-1} = t(c_1c_2)t^{-1}(c_1c_2)^{-1} = (a_1 a_4)(a_2 a_3) \in N.
\]

Let \( a_5 \notin \{a_1, a_2, a_3, a_4\} \). (This is the place where we use \( n \geq 5 \).) Let \( u = (a_1 a_4 a_5) \). Then

\[
u hu^{-1} = (a_4 a_5)(a_2 a_3) \in N,
\]

and thus

\[
u hu^{-1}h^{-1} = (a_1 a_5 a_4) \in N
\]

is a 3-cycle in \( N \).

Note: \( A_4 \) is not simple, because the subgroup \( N = \{ e, (1 \ 2)(3 \ 4), (1 \ 3)(2 \ 4), (1 \ 4)(2 \ 3) \} \) generated by the products of disjoint 2-cycles is normal. Part (d) of the proof fails here.

43. Finite Galois extensions

A finite Galois extension is a finite normal separable extension \( L : F \). For such an extension, its automorphism group \( G = \text{Aut}(L : F) \) is called its Galois group\(^3\).

We can also characterize finite Galois extension purely in terms of their automorphism group.

**Proposition.** \( L : F \) is a finite Galois extension if and only if there exists a finite subgroup \( G \leq \text{Aut}(L) \) such that \( F = L^G \).

**Proof.** If \( L : F \) is a finite Galois extension, let \( G = \text{Aut}(L : F) \). Then the Galois correspondence tells us that \( |G| = [L : F] < \infty \), and that \( F = L^G \).

Conversely, suppose \( F = L^G \) with \( G \) finite. The first technical lemma says \( [L : F] = |G| \), so the extension is finite. We need to show \( L : F \) is normal and separable. That is, given \( \alpha \in L \), let \( f = f_{\alpha/F} \in \text{Irred}(F) \) be its minimal polynomial. We need to show that \( f \) splits over \( L \) (normal) and has no repeated roots (separable).

---

\(^3\)This is usual practice, as opposed to Stewart, who calls any automorphism group of an extension a Galois group.
Let \( G\alpha = \{ \phi(\alpha) \mid \phi \in G \} \subseteq L \), the set of images of \( \alpha \) under the elements of \( G \). This is a finite set (which could be smaller than \(|G|\), since it is possible for \( \phi(\alpha) = \phi'(\alpha) \) even if \( \phi \neq \phi' \)). Let

\[
g := \prod_{\beta \in G\alpha} (X - \beta) \in L[X].
\]

This is clearly a separable polynomial which splits over \( L \) and has \( \alpha \) as a root since \( \alpha \in G\alpha \).

Note that for every \( \phi \in G \) the image polynomial \( g' = \phi(g) \) just gets its linear factors permuted, so \( g' = g \). Thus \( g \in F[X] \). Therefore the minimal polynomial \( f \) divides \( g \), so \( f \) splits over \( L \) and is separable. \( \square \)

In fact, more is true; the \( g \) of the previous proof is equal to the minimal polynomial.

**Proposition.** Let \( L : F \) be a finite Galois extension with Galois group \( G \). For any \( \alpha \in L \) we have that

\[
f_{\alpha/F} = \prod_{\beta \in G\alpha} (X - \beta).
\]

**Proof.** The proof of the previous proposition shows that \( g = \prod_{\beta \in G\alpha} (X - \beta) \) is in \( F[X] \) and is divisible by \( f = f_{\alpha/F} \). We need to show \( g = f \).

Let \( R = \{ \beta \in L \mid f(\beta) = 0 \} \). Then \( R \subseteq G\alpha \), and \( R \) is non-empty since \( \alpha \in R \). Elements of \( G \) must take roots of \( f \) to roots of \( f_1 \), whence for any \( \phi \in G \) we must have \( \phi(\alpha) \in R \). But this implies that \( R = G\alpha \). Since \( g \) is separable we must have \( f = g \). \( \square \)

**Example.** Let \( L = \mathbb{Q}(i, \sqrt{2}) \), with \( G = \text{Aut}(L : \mathbb{Q}) \approx \mathbb{Z}/2 \times \mathbb{Z}/2 \). We can use the above to compute minimal polynomials of various elements of \( L \):

\[
G i = \{ \pm i \}, \quad f_{i/\mathbb{Q}} = (X - i)(X + i) = X^2 + 1,
\]

\[
G (1 + \sqrt{2}) = \{ 1 \pm \sqrt{2} \}, \quad f_{1 + \sqrt{2}/\mathbb{Q}} = (X - (1 + \sqrt{2}))(X - (1 - \sqrt{2})) = X^2 - 2X - 1,
\]

\[
G (i + \sqrt{2}) = \{ \pm i \pm \sqrt{2} \}, \quad f_{i + \sqrt{2}/\mathbb{Q}} = (X - (i + \sqrt{2}))(X - (-i + \sqrt{2}))(X - (i - \sqrt{2}))(X - (-i - \sqrt{2})) = X^4 - 6X^2 + 1.
\]

We can summarize this as: an orbit \( O \subseteq L \) of the \( G \)-action on \( L \) is precisely the set of roots of some \( f \in \text{Irred}(F) \).

for a finite Galois extension \( L : F \) consider the function

\[
\pi : L \to \text{Irred}(F),
\]

\[
\alpha \mapsto f_{\alpha/F}.
\]

This function is not surjective (unless \( L \) is algebraically closed): the image consists of the irreducible polynomials which have a root in \( L \), which must also split over \( L \). The preimage \( \pi^{-1}(f) \) of an irreducible polynomial in the image is the set of roots of \( f \) in \( L \), which has size \( \deg f \). Each nonempty preimage \( \pi^{-1}(f) \) is an orbit for the action of \( G \) on the set \( L \).

**Example.** Consider \( \pi : \mathbb{C} \to \text{Irred}(\mathbb{R}) \). The fibers (=preimages) of \( \pi \) are either

\[
\{ c \}, \quad c \in \mathbb{R} \quad \mapsto \quad X - c,
\]

or

\[
\{ a \pm bi \}, \quad a, b \in \mathbb{R}, \ b \neq 0 \quad \mapsto \quad X^2 - 2aX + (a^2 + b^2).
\]

Because \( \mathbb{C} \) is algebraically closed, \( \pi \) is surjective. This is the proof that all irreducible polynomials over \( \mathbb{R} \) have degree 1 or 2.
44. Transcendence degree

I need to talk about another numerical invariant of a field extension, called *transcendence degree*. This is an invariant that knows about transcendental elements: we’ll have tr. deg\((L : F) = 0\) iff \(L : F\) is an algebraic extension, and also tr. deg\((L : F) = n\) if \(L = F(t_1, \ldots, t_n)\) is a field of rational functions in \(n\) variables. This is discussed in Chapter 18.1, but I’m going to describe things a little differently.

There is a strong analogy between transcendence degree and vector space dimension, so let me recall how that works (for finite dimensional vector spaces). Given an \(F\)-vector space \(V\), and a sequence of elements \(v_1, \ldots, v_k\) in \(V\), it can be a “spanning set” (every element of \(V\) is an \(F\)-linear combination of the \(v_i\)s), and it can be “linearly independent”. It is a “basis” if and only if it is both a spanning set and is linearly independent. Consider two facts:

1. If \(S = \{v_1, \ldots, v_s\}\) is a spanning set of \(V\), then there is a subset of \(S\) which is a basis.
2. If \(R = \{u_1, \ldots, u_r\}\) is a spanning set of \(V\), and \(T = \{w_1, \ldots, w_t\}\) is a linearly independent subset, then \(r \geq t\).

Fact (1) implies that every vector space with a finite spanning set has a basis. Proof: choose a maximal linearly independent subset \(S'\) of \(S\), and show every element of \(S\) is in the span of \(S'\).

Fact (2) implies that any two bases of \(V\) have the same size. The *dimension* of \(V\) is exactly the size of any basis. Fact (2) is proved as a consequence of the following “exchange property”.

3. Consider a list of elements

\[
 u_1, \ldots, u_r, \ v_1, \ldots, v_s, \ w_1, \ldots, w_t \in V. 
\]

Suppose that (i) \(u_1, \ldots, u_r, v_1, \ldots, v_s\) is a spanning set, and (ii) \(v_1, \ldots, v_s, w_1, \ldots, w_t\) is linearly independent. If \(t \geq 1\), then there exists \(k \in \{1, \ldots, r\}\) such that (i') \(u_1, \ldots, \hat{u}_k, \ldots, u_r, v_1, \ldots, v_s, w_1\) is a spanning set, where “\(\hat{u}_k\)” means “\(u_k\) is not in the list”.

This means that if we start with lists of lengths \(r, s, t\) with these properties, and \(t > 0\), then we produce lists of length \(r - 1, s + 1, t - 1\) with the same properties. In particular, if \(t > 0\) then \(r > 0\) also. By iterating the procedure, if we start with lists of lengths \(r, s, t\) we end up with lists of lengths \(r - t, s + t, 0\), whence \(r \geq t\). In particular, the case of \(s = 0\) gives (2).

Here’s how you prove (3). Consider

\[
 u_1, \ldots, u_r, \ v_1, \ldots, v_s, \ w_1. 
\]

Since the first \(r + s\) vectors in the list are already a spanning set, there must be a linear dependence among the \(r + s + 1\) vectors which involves \(w_1\). (“Involves \(w_1\)” means that \(w_1\) appears with a non-zero coefficient in the dependence.) Since \(v_1, \ldots, v_s, w_1\), are linearly independent, such a linear dependence must also involve some \(u_k\). Thus, \(u_k\) is in the span of \(u_1, \ldots, \hat{u}_k, \ldots, u_r, v_1, \ldots, v_s, w_1\), so this set is a spanning set of \(V\).

Now let’s consider a field extension \(L : F\). Say that a list \(\alpha_1, \ldots, \alpha_k \in L\) is a trans*cent*ent spanning set over \(F\) if the extension

\[
 L : F(\alpha_1, \ldots, \alpha_k) 
\]

is an algebraic extension.

Say that a list \(\alpha_1, \ldots, \alpha_k \in L\) is algebraically independent over \(F\) if there is no non-zero polynomial \(f \in F[X_1, \ldots, X_k]\) such that \(f(\alpha_1, \ldots, \alpha_k) = 0\).

Remark. A single element \(\alpha \in L\) is algebraically independent over \(F\) if and only if it is transcendental over \(F\).

\[\text{M 21 Oct} \text{ transcendent spanning set}\]

\[\text{algebraically independent}\]
Remark. Note that for any list of elements, the function
\[ f \mapsto f(\alpha_1, \ldots, \alpha_k) : F[X_1, \ldots, X_k] \to L \]
is a ring homomorphism. So the $\alpha$s are algebraically independent iff the kernel is $\{0\}$. If they are independent, then we can extend this homomorphism to a homomorphism from the function field
\[ \phi : F(X_1, \ldots, X_k) \to L. \]
This is an isomorphism from the function field to the image of $F(\alpha_1, \ldots, \alpha_k)$. So the list of length $k$ is algebraically independent iff the subfield they generate over $F$ is isomorphic to a field of rational functions on $k$ variables over $F$.

Let’s note a consequence: any element of $c \in F(\alpha_1, \ldots, \alpha_k)$ can be written in the form $g(\alpha_1, \ldots, \alpha_k)/h(\alpha_1, \ldots, \alpha_k)$, where $g, h \in F[X_1, \ldots, X_k]$ are polynomials with $h \neq 0$. (This is actually still true even if the $\alpha$s aren’t algebraically independent.)

Note that any subset of an algebraically independent set is algebraically independent, and that a superset of transcendent spanning set is a transcendent spanning set.

A **transcendence basis** is a list $\alpha_1, \ldots, \alpha_k \in L$ which is both a transcendent spanning set and algebraically independent.

Example. Let $L = F(t_1, \ldots, t_n)$ be a field of rational functions over $F$ in $n$-variables. Then the set $t_1, \ldots, t_n$ a transcendence basis of $L : F$.

Example. Let $L = F(t)$ be a field of rational functions on 1-variable. Let $\alpha = t^m$ for some $m \geq 1$. Then $\alpha$ is a transcendence basis of $L : F$. It is easy to see that $\alpha$ is transcendental, since if $g = \sum c_k X^k \in F[X]$, then $g(\alpha) = \sum c_k \alpha^m$ which can be zero only if $g = 0$. To see that $\alpha$ is a transcendental basis just note that $f = X^m - g \in F(\alpha)[X]$ has $t$ as a root, so $t$ is algebraic over $F(\alpha)$, and thus $L : F(\alpha)$ is algebraic since $L = F(\alpha)(t)$.

Exercise. Show that any $f \in F[t]$ with $\deg f \geq 1$ defines a transcendence basis of $F(t) : F$.

Here’s a linear algebra fact.

Let $V$ be an $F$-vector space, and $v_1, \ldots, v_r \in V$ a linearly independent set of elements of $V$, and $w \in V$ another element. The following are equivalent.

1. $w$ is in the span of $\{v_1, \ldots, v_r\}$.
2. There exist $a_1, \ldots, a_r, b \in F$ with $b \neq 0$ such that $a_1 v_1 + \cdots + a_r v_r + bw = 0$.

Here is the key lemma we will need, which is analogous to our linear algebra fact.

**Lemma** (Key lemma). Let $L : F$ with $\alpha_1, \ldots, \alpha_r \in L$ an algebraically independent set, and also $\beta \in L$. The following are equivalent.

1. $\beta$ is algebraic over $K = F(\alpha_1, \ldots, \alpha_r)$.
2. There exists an $f \in F[X_1, \ldots, X_r, Y] \setminus F[X_1, \ldots, X_r]$ such that $f(\alpha_1, \ldots, \alpha_r, \beta) = 0$.

**Warning.** The analogy to linear algebra is not perfect. In the linear algebra version, you don’t need to require that $v_1, \ldots, v_r$ is linearly independent, but the above lemma isn’t true in the form given unless $\alpha_1, \ldots, \alpha_r$ are algebraically independent.

**Proof.** (2) $\implies$ (1). Pick such an $f \in F[X_1, \ldots, X_r, Y]$, which has the form
\[ f = f_0 + f_1 Y + \cdots + f_d Y^d, \quad f_i \in F[X_1, \ldots, X_r], \quad d \geq 1, \quad f_d \neq 0 \]
since $f \notin F[X_1, \ldots, X_r]$. Plug in $\alpha_1, \ldots, \alpha_r$ to get
\[ g := f(\alpha_1, \ldots, \alpha_r, Y) = c_0 + c_1 Y + \cdots + c_d Y^d \in K[Y], \quad c_i = f_i(\alpha_1, \ldots, \alpha_r) \in K. \]
Then $c_d = f_d(\alpha_1, \ldots, \alpha_r) \neq 0$ since $f_d \neq 0$ and the $\alpha$s are algebraically independent, while $g(\beta) = f(\alpha_1, \ldots, \alpha_r, \beta) = 0$. Thus we get a non-zero polynomial $g \in K[Y]$ with $\beta$ as a root, so $\beta$ is algebraic over $K$. 

LECTURE NOTES FOR 428 59
(1) \implies (2). Let \( g \in K[Y] \) be a non-zero polynomial such that \( g(\beta) = 0 \). We can write
\[
g = c_0 + c_1 Y + \cdots + c_d Y^d \in K[Y], \quad c_d \neq 0, \quad d \geq 1.
\]
Each \( c_i \in K \) has the form
\[
c_i = a_i/b_i, \quad a_i = g_i(\alpha_1, \ldots, \alpha_r), \quad b_i = h_i(\alpha_1, \ldots, \alpha_r), \quad g_i, h_i \in F[X_1, \ldots, X_r].
\]
Now we “clear denominators” by multiplying through by \( b := b_0 \cdots b_d \neq 0 \). That is, let
\[
f = f_0 + f_1 Y + \cdots + f_d Y^d \in F[X_1, \ldots, X_r, Y], \quad f_i \in F[X_1, \ldots, X_r],
\]
where
\[
f_i = g_i \cdot h_0 \cdots \hat{h}_i \cdots h_d,
\]
so that
\[
f_i(\alpha_1, \ldots, \alpha_r) = a_i \cdot b_0 \cdots \hat{b}_k \cdots b_d = c_i b,
\]
so that
\[
f(\alpha_1, \ldots, \alpha_r, Y) = b(c_0 + c_1 Y + \cdots + c_d Y^d) = bg.
\]
Then \( f \) is such that \( f(\alpha_1, \ldots, \alpha_r, \beta) = bg(\beta) = 0 \), but \( f_d(\alpha_1, \ldots, \alpha_r) = bc_d \neq 0 \).

\[\square\]

**Proposition.** Let \( S = \{\alpha_1, \ldots, \alpha_n\} \) be a transcendent spanning set of \( L : F \), and suppose \( T \subseteq S \) is a subset which is algebraically independent. Then there exists a transcendence basis \( B \) with \( T \subseteq B \subseteq S \). In particular, a subset of \( S \) is a transcendence basis of \( L : F \).

**Proof.** The second statement is just the first statement with \( T = \emptyset \).

If \( S \) is algebraically independent we are done. Otherwise, consider all subsets of \( \{\alpha_1, \ldots, \alpha_n\} \) which are algebraically independent and contain the given set \( T \), and choose one of maximal size. By relabelling we can assume that \( \alpha_1, \ldots, \alpha_r \) is algebraically independent, but \( \alpha_1, \ldots, \alpha_{r+1} \) is not, where \( \alpha_{r+1} \) can be any of the remaining \( n-r \) elements. We have \( 0 \leq r < n \) here; note that \( r = 0 \) is allowed, i.e., that there could be no non-empty algebraically independent subset.

Let \( K = F(\alpha_1, \ldots, \alpha_r) \subseteq L \). I will show that \( \alpha_{r+1} \) is algebraic over \( K \). Since the choice of \( \alpha_{r+1} \) among the last \( n-r \) elements of the list is arbitrary, this shows that every \( \alpha_k \) with \( k > r \) is algebraic over \( K \). Thus both extensions
\[
K = F(\alpha_1, \ldots, \alpha_r) \subseteq F(\alpha_1, \ldots, \alpha_n) \subseteq L
\]
are algebraic, whence \( \alpha_1, \ldots, \alpha_r \) is a transcendental spanning set.

Since \( \alpha_1, \ldots, \alpha_{r+1} \) is not algebraically independent, there exists a non-zero \( f \in F[X_1, \ldots, X_{r+1}] \) such that \( f(\alpha_1, \ldots, \alpha_{r+1}) = 0 \). We cannot have \( f \in F[X_1, \ldots, X_r] \), because the set \( \alpha_1, \ldots, \alpha_r \) is algebraically independent. Thus \( f \in F[X_1, \ldots, X_{r+1}] \setminus F[X_1, \ldots, X_r] \), so by the key lemma we must have that \( \alpha_{r+1} \) is algebraic over \( K \) as desired.

\[\square\]

Now we have an exchange lemma.

**Lemma (Exchange lemma).** Let \( L : F \) be an extension, with subsets
\[
R = \{\alpha_1, \ldots, \alpha_r\}, \quad S = \{\beta_1, \ldots, \beta_s\}, \quad T = \{\gamma_1, \ldots, \gamma_t\}
\]
of \( L \) such that (i) \( R \cup S \) is a transcendence basis of \( L : F \), and (ii) \( S \cup T \) is algebraically independent over \( F \). If \( t \geq 1 \) then there exists a proper subset \( R' \subseteq R \) such that (i') \( R' \cup S \cup \{\gamma_1\} \) is a transcendence basis of \( L : F \).

As with the exchange lemma for vector spaces, iterating this implies that \( r \geq t \). The special case \( s = 0 \) says that a transcendent spanning set can never be smaller than an algebraically independent set, so we get what we want.

**Corollary.** If \( L : F \) is an extension with a finite transcendental spanning set, then any two transcendence bases have the same size. have the same size.
Given this, we define \( \text{tr.deg}(L : F) \) to be the size of any transcendence basis.

**Proof of exchange lemma.** Since \( R \cup S \) is a transcendence basis, the set \( R \cup S \cup \{ \gamma_1 \} \) is a transcendental spanning set, which contains the algebraically independent set \( S \cup \{ \gamma_1 \} \). Therefore there exists a transcendence basis of the form \( B = R' \cup S \cup \{ \gamma_1 \} \), where \( R' \subseteq R \).

But since \( R \cup S \) is a transcendence basis, \( \gamma_1 \) is algebraic over \( F(R \cup S) \). Thus \( R \cup S \cup \{ \gamma_1 \} \) is not algebraically independent, so \( B \neq R \cup S \cup \{ \gamma_1 \} \), so \( R' \neq R \).

The consequence we will need is the following.

**Proposition.** Let \( L = F(t_1, \ldots, t_n) \) be a field of rational functions, and suppose the sequence \( \alpha_1, \ldots, \alpha_n \in L \) is a transcendent spanning set of \( L \) over \( F \). Then \( S = \{ \alpha_1, \ldots, \alpha_n \} \) is algebraically independent.

**Proof.** We have that \( \text{tr.deg}(L : F) = n \) since it is a field of rational functions, so any transcendence basis of \( L : F \) has size \( n \). We know \( S \) has a subset which is a transcendence basis, but since this subset must have size \( n \), we see that \( S \) is itself a transcendence basis. \( \Box \)

### 45. Symmetric Polynomials

Consider \( R_n = F[t_1, \ldots, t_n] \), a polynomial ring in \( n \) variables. A **symmetric polynomial** is an element \( f \in R_n \) such that \( f(t_{\sigma(1)}, \ldots, t_{\sigma(n)}) = f(t_1, \ldots, t_n) \) for any relabelling of the \( n \)-variables.

**Example.** In \( R_2 = F[t_1, t_2] \), the polynomial \( t_1 t_2 + 4t_1^3 + 4t_2^3 - t_1^5 t_2 - t_1 t_2^5 \) is symmetric. But \( t_1^3 + t_2^2 \) is not symmetric.

In fact, every \( \sigma \in S_n \) defines a ring homomorphism \( \sigma : R_n \rightarrow R_n \), defined by

\[
\sigma f := f(t_{\sigma(1)}, \ldots, t_{\sigma(n)}).
\]

The symmetric polynomials are the \( f \) such that \( \sigma f = f \) for all \( f \in S_n \). Let

\[
R_n^{S_n} = \{ f \in R_n \mid \sigma f = f, \forall \sigma \in S_n \}
\]

denote the set of symmetric polynomials. It is a subring of \( R_n \).

The **elementary symmetric polynomials** in \( n \)-variables are

\[
\begin{align*}
    s_1 & := t_1 + \cdots + t_n = \sum_{1 \leq i \leq n} t_i, \\
    s_2 & := t_1 t_2 + t_1 t_3 + \cdots + t_{n-1} t_n = \sum_{1 \leq i < j \leq n} t_i t_j, \\
    & \vdots \\
    s_k & := t_1 t_2 \cdots t_k + \cdots + t_{n-k+1} t_{n+k-2} \cdots + t_n = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} t_{i_1} t_{i_2} \cdots t_{i_k}, \\
    & \vdots \\
    s_n & := t_1 t_2 \cdots t_n.
\end{align*}
\]

These are set up so that, in \( R_n[X] \), we have that

\[
(X - t_1) \cdots (X - t_n) = X^n - s_1 X^{n-1} + s_2 X^{n-2} + \cdots \pm s_n = X^n + \sum_{k=1}^{n} (-1)^k s_k X^{n-k}.
\]
For instance,

\[(X - t_1)(X - t_2) = X^2 - (t_1 + t_2)X + (t_1t_2)\]

\[(X - t_1)(X - t_2)(X - t_3) = X^3 - (t_1 + t_2 + t_3)X^2 + (t_1t_2 + t_1t_3 + t_2t_3)X - (t_1t_2t_3),\]

\[(X - t_1)(X - t_2)(X - t_3)(X - t_4) = X^4 - (t_1 + t_2 + t_3 + t_4)X^3 + (t_1t_2 + t_1t_3 + t_1t_4 + t_2t_3 + t_2t_4 + t_3t_4)X^2 - (t_1t_2t_3t_4)X + (t_1t_2t_3t_4)\]

**Warning.** There is an element called \(s_k\) in each \(R_n\) with \(n \geq k\). They are not the same polynomial, despite having the same name: for instance, \(s_1\) has the form

\[s_1 = t_1 \in R_1, \quad s_1 = t_1 + t_2 \in R_2, \quad s_1 = t_1 + t_2 + t_3 \in R_3,\]

and so forth. Watch out for this: in subsequent arguments I will need to talk about \(s_k\)s from different \(R_n\)s in course of a single proof.

The elementary symmetric polynomials “generate” all symmetric polynomials in some sense, according to the following theorem.

**Proposition.** Every symmetric polynomial can be written as a polynomial in the elementary symmetric polynomials. That is, if \(f \in R_n^{S_n}\), then there exists \(g \in F[X_1, \ldots, X_n]\) such that

\[f = g(s_1, \ldots, s_n).\]

**Example.** For any \(n \geq 3\), the element \(f = t_1^3 + \cdots + t_n^3 \in R_n^{S_n}\) can be written \(f = s_1^3 - 3s_1s_2 + 3s_3\).

(When \(n = 2\) we have \(f = s_1^3 - 3s_1s_2 \in R_2^{S_2}\), and when \(n = 1\) we have \(f = s_1^3 \in R_1^{S_1}\).)

I’m going to introduce notation for polynomials in several variables. Let \(k_1, \ldots, k_n \geq 0\), which I think of as a tuple \(k = (k_1, \ldots, k_n)\). I write

\[t^k := t_1^{k_1}t_2^{k_2} \cdots t_n^{k_n} \in R_n\]

for the evident monomial in \(R_n\). Any \(f \in R_n\) can be written uniquely as a finite sum

\[f = \sum_k c_k t^k, \quad c_k \in F,\]

where \(k = (k_1, \ldots, k_n)\) runs over such tuples.

We define the **degree** of \(f\) by

\[\deg f := \max \{ k_1 + \cdots + k_n \mid c_k \neq 0 \},\]

with \(\deg f = -\infty\) if \(f = 0\). This agrees with our usual definition for polynomials in one variable. In general, we have

\[\deg(f + g) \leq \max(\deg f, \deg g), \quad \deg(fg) = \deg f + \deg g.\]

The first is easy to prove, the second is not too hard but more subtle than it looks. I only need the following: \(\deg(t_k f) = \deg(f) + 1\), where \(t_k\) is any one of the variables.

Note that if \(\sigma \in S_n\), then

\[\sigma f = \sum_k c_{k\sigma} t^k\]

where

\[k\sigma = (k_{\sigma(1)}, \ldots, k_{\sigma(n)}).\]

Thus \(f\) is symmetric iff \(c_{k\sigma} = c_k\) for all \(k\).

To prove the proposition, I need to pass between polynomial rings with different numbers of variables. There is a ring homomorphism

\[\pi: F[t_1, \ldots, t_n] \to F[t_1, \ldots, t_{n-1}], \quad \pi(f) := f(t_1, \ldots, t_{n-1}, 0),\]
defined by “setting \( t_n \) to 0”. An \( f \in R_{n}^{S_n} \) is still invariant with respect to the subgroup \( S_{n-1} \leq S_n \), so \( \pi \) restricts to a homomorphism

\[
\pi': R_{n}^{S_n} \rightarrow R_{n-1}^{S_{n-1}}.
\]

Notice that this sends

\[
\pi'(s_k) = s_k \quad \text{if } k = 1, \ldots, n - 1, \quad \pi'(s_n) = 0,
\]

(where the two \( s_k \)'s live in different rings.)

**Lemma.** The kernel of \( \pi' \) is \( \langle s_n \rangle = \{ s_ng \mid g \in R_{n}^{S_n} \} \), where \( s_n = t_1 \cdots t_n \).

**Proof.** Writing \( f = \sum c_k t_k^k \), we have that

\[
\pi(f) = \sum_{\substack{k = (k_1, \ldots, k_n) \\ k_n = 0}} c_k t_k^k,
\]

so \( f \in \text{Ker} \ \pi \) iff \( c_k = 0 \) whenever \( k_n = 0 \). The polynomial \( f \) is symmetric iff \( c_k = c_{k\sigma} \) for all \( \sigma \in S_n \).

Thus for \( f \in R_{n}^{S_n} \), we have \( f \in \text{Ker} \ \pi' \) iff \( c_k = 0 \) whenever there exists \( j \in \{1, \ldots, n\} \) such that \( k_j = 0 \). Thus if \( f \in \text{Ker} \ \pi' \) then we can write

\[
f = \sum_{\substack{k = (k_1, \ldots, k_n) \\ k_n \geq 1}} c_k t_k^k.
\]

For each \( k \) in this expression, \( t_k^k \) is divisible by \( s_n \), so \( f \) is divisible by \( s_n \). \( \square \)

The following examples illustrate the idea of the proof of the proposition on symmetric functions.

**Example.** Consider \( f = t_1^3 + t_2^3 \in R_{2}^{S_2} \). Under \( \pi' \) this goes to \( t_1^3 = s_1^3 \in R_{1}^{S_1} \), so by the lemma \( g := f - s_1^3 \in R_{2}^{S_2} \) must be divisible by \( s_2 \). In fact,

\[
g = f - s_1^3 = (t_1^3 + t_2^3) - (t_1 + t_2)^3 = -3t_1^2 t_2 - 3t_1 t_2^2 = -3(t_1 + t_2)(t_1 t_2) = -3s_1 s_2.
\]

Thus \( f = s_1^3 - 3s_1 s_2 \in R_{2}^{S_2} \).

**Example.** Now consider \( f' = t_1^3 + t_2^3 + t_3^3 \in R_{3}^{S_3} \). Under \( \pi' \) this goes to \( f = t_1^3 + t_2^3 \in R_{2}^{S_2} \), so by the previous example and the lemma \( g' := f' - (s_1^3 - 3s_1 s_2) \in R_{3}^{S_3} \) must be divisible by \( s_3 \). In fact

\[
g' = f' - (s_1^3 - 3s_1 s_2) = (t_1^3 + t_2^3 + t_3^3) - (t_1 + t_2 + t_3)^3 + 3(t_1 + t_2 + t_3)(t_1 t_2 + t_1 t_3 + t_2 t_3) = 3t_1 t_2 t_3 = 3s_3.
\]

Thus \( f' = s_1^3 - 3s_1 s_2 + 3s_3 \in R_{3}^{S_3} \).

**Example.** Now consider \( f'' = t_1^3 + t_2^3 + t_3^3 + t_4^3 \in R_{4}^{S_4} \). Under \( \pi' \) this goes to \( f' = t_1^3 + t_2^3 + t_3^3 \in R_{3}^{S_3} \), so by the previous example and the lemma \( g'' := f - (s_1^3 - 3s_1 s_2 + 3s_3) \in R_{4}^{S_4} \) must be divisible by \( s_4 \). In fact, since \( g'' \) can only have degree at most 3 but \( \text{deg} \ s_4 = 4 \), we must have \( g'' = 0 \). Thus

\[
f'' = s_1^3 - 3s_1 s_2 + 3s_3 \in R_{4}^{S_4}, \quad \text{and the same formula holds in } R_{n}^{S_n} \text{ for all } n \geq 3.
\]

**Proof of proposition on symmetric polynomials.** Let \( f \in R_{n}^{S_n} \). We show that \( f \) can be written as a polynomial in the elementary symmetric polynomials by induction double induction: firstly on the number of variables \( n \), and then secondly by induction on degree of \( f \) in \( R_{n}^{S_n} \).

If \( n = 1 \), then every polynomial is symmetric, and since \( t_1 = s_1 \) we have \( f(t_1) = f(s_1) \).

Suppose \( n \geq 2 \), and consider \( f \in R_{n}^{S_n} \). Let \( f' := \pi'(f) \in F[t_1, \ldots, t_{n-1}]^{S_{n-1}} \). By the inductive hypothesis on number of variables, there exists \( K \in F[X_1, \ldots, X_{n-1}] \) such that

\[
f' = K(s_1, \ldots, s_{n-1}) \in R_{n-1}^{S_{n-1}}
\]
where \( s_1, \ldots, s_{n-1} \in R_{n-1}^{S_n} \) are the elementary symmetric polynomials in \( n - 1 \) variables.

Now consider
\[
g := f - K(s_1, \ldots, s_{n-1}) \in R_n^{S_n},
\]
where in this formula \( s_1, \ldots, s_{n-1} \in R_n^{S_n} \) are the elementary symmetric polynomials in \( n \)-variables. We have that
\[
\pi'(g) = f' - K(\pi'(s_1), \ldots, \pi'(s_{n-1})) = 0,
\]
so \( g \in \text{Ker} \pi' \), so by the lemma \( g = s_ng' \) for some \( F[t_1, \ldots, t_n]^{S_n} \). Thus
\[
f = s_ng' + K(s_1, \ldots, s_{n-1}).
\]
Since \( g' \) has smaller degree than \( f \), it can be written as a polynomial in the \( s_i \)s by the inductive hypothesis. \( \square \)

We’ve just shown that the function \( F[X_1, \ldots, X_n] \to R_n^{S_n} \) which sends \( f \mapsto f(s_1, \ldots, s_n) \) (which is a homomorphism of rings) is surjective. In fact, it’s a bijection, which we can see by using the ideas about algebraic independence we talked about earlier.

**Theorem.** The ring \( R_n^{S_n} \subseteq F[t_1, \ldots, t_n] \) of symmetric polynomials in \( n \) variables over \( F \) is isomorphic to a polynomial ring in \( n \)-variables, with generators corresponding to the elementary symmetric polynomials \( s_1, \ldots, s_n \).

Thus, for every symmetric polynomial \( f \in R_n^{S_n} \) there is a unique polynomial \( g \in F[X_1, \ldots, X_n] \) such that \( g(s_1, \ldots, s_n) = f \).

**Proof.** We have
\[
F[X_1, \ldots, X_n] \xrightarrow{g \mapsto g(s_1, \ldots, s_n)} R_n^{S_n} \subseteq R_n \subseteq L_n = F(t_1, \ldots, t_n).
\]
We need to show that \( g(s_1, \ldots, s_n) = 0 \) implies \( g = 0 \). Because \( R_n^{S_n} \subseteq L_n \), this amounts to the statement that \( s_1, \ldots, s_n \) is algebraically independent over \( F \). Since \( \text{tr} \deg(L_n : F) = n \), it suffices to show that the \( s_1, \ldots, s_n \) are a transcendental spanning set for \( L_n : F \), i.e., that each of \( t_1, \ldots, t_n \) is algebraic over \( K_n = F(s_1, \ldots, s_n) \subseteq L_n \). But this is clear, since the \( t_k \) are roots of the polynomial
\[
f = \prod_{k=1}^{n} (X - t_k) = X^n - s_1X^{n-1} + \cdots + (-1)^{n-1}s_{n-1}X + (-1)^ns_n \in K_n[X].
\]
\( \square \)

### 46. The General Polynomial

Fix \( n \geq 1 \). We have
\[
R_n = F[t_1, \ldots, t_n] \subseteq L_n = F(t_1, \ldots, t_n),
\]
the polynomial ring as a subring of the field of rational functions. These contain the elementary symmetric polynomials \( s_1, \ldots, s_n \in R_n \), so we get a subfield
\[
K_n = F(s_1, \ldots, s_n) \subseteq L_n.
\]
The extension \( L_n : K_n \) is a splitting field for the polynomial
\[
f = X^n + \sum_{k=1}^{n}(-1)^ks_kX^{n-k} = \prod_{j=1}^{n}(X - t_j) \in K_n[X].
\]

The symmetric group \( S_n \) acts on the ring \( R_n \) by permuting the variables, and this action extends to an action of \( S_n \) on \( L_n \). We have inclusions of fields
\[
K_n \subseteq L_n^{S_n} \subseteq L_n,
\]
since elementary symmetric polynomials are fixed by the \( S_n \) action. The subfield \( L_n^{S_n} \) is the field of **symmetric rational functions**.
Proposition. We have \( K_n = L^{S_n} \), so \([L_n : K_n] = n! \) and \( \text{Aut}(L_n : K_n) = S_n \).

Proof. The extension \( L_n : L^{S_n} \) is a Galois extension with Galois group \( S_n \), so \([L_n : L^{S_n}] = |S_n| = n! \).

On the other hand, \( L_n : K_n \) is a splitting field for \( f \in K_n[X] \) with \( \deg f = n \), so \([L_n : K_n] \leq n! \).

The tower law \([L_n : K_n] = [L_n : L^{S_n}][L^{S_n} : K_n] \) implies \([L^{S_n} : K_n] = 1 \), so \( K_n = L^{S_n} \). The Galois correspondence implies that \( \text{Aut}(L_n : K_n) = \text{Aut}(L_n : L^{S_n}) = S_n \). \( \square \)

We regard \( f = X^n - s_1X^{n-1} + \cdots + (-1)^n s_n \in K_n[X] \) as the \textbf{general polynomial} of degree \( n \) over \( K_n \). If we can solve \( f \) in terms of radicals over \( K \), then we have a “formula” for roots of an \( n \)th degree polynomial.

Since \( S_n \) is not solvable if \( n \geq 5 \), we see that there is no “\( n \)th root formula” in these cases.

Example (The general quadratic). Suppose characteristic \( F \) is not 2. Then \( f = X^2 - s_1X + s_2 \in K_2[X] \) has roots

\[
t_1, t_2 = \frac{s_1 \pm \sqrt{s_1^2 - 4s_2}}{2} \in L_2.
\]

Explicitly, this means \((2t_k - s_1)^2 = s_1^2 - 4s_2 \) for \( k = 1, 2 \). In particular,

\[
L_2 = K_2(\sqrt{s_1^2 - 4s_2}),
\]

so \( L_2 : K_2 \) is a radical extension.

We have

\[
\Delta := s_1^2 - 4s_2 = t_1^2 - 2t_1t_2 + t_2^2 = (t_1 - t_2)^2.
\]

This quantity is called the \textbf{discriminant} of the general quadratic. We have \( L = K(\sqrt{\Delta}) \).

Example (The general cubic). Suppose characteristic \( F \) is not 2 or 3, and that \( F \) contains a primitive 3rd root of unity \( \omega \). (For instance, \( F = \mathbb{C} \).

Let \( K = K_3 = F(s_1, s_2, s_3) \) and \( L = L_3 = F(t_1, t_2, t_3) \).

Consider \( f = X^3 - s_1X^2 + s_2X - s_3 \in K[X] \), with roots \( t_1, t_2, t_3 \in L \). Define elements

\[
\ell_0 = \frac{1}{3}(t_1 + t_2 + t_3), \\
\ell_1 = \frac{1}{3}(t_1 + \omega t_2 + \omega^2 t_3), \\
\ell_2 = \frac{1}{3}(t_1 + \omega^2 t_2 + \omega t_3)
\]

in \( L \), so that

\[
t_1 = \ell_0 + \ell_1 + \ell_2, \\
t_2 = \ell_0 + \omega^2 \ell_1 + \omega \ell_2, \\
t_3 = \ell_0 + \omega \ell_1 + \omega^2 \ell_2.
\]

The Galois group \( G = \text{Aut}(L : K) \approx S_3 \) acts in the obvious way on \( \{t_1, t_2, t_3\} \). Using this you can compute how it acts on \( \ell_0, \ell_1, \ell_2 \). Note that

\[
\ell_0, \ell_1 \ell_2, \ell_1^2 + \ell_2^2, (\ell_1^3 - \ell_2^3)^2 \in L^{S_3} = K.
\]

Since each of can be written as a symmetric rational function (in fact, as a symmetric polynomial) in \( t_1, t_2, t_3 \), you can (tediously) write these in terms of \( s_1, s_2, s_3 \):

\[
\ell_0 = \frac{1}{3}s_1, \\
\ell_1 \ell_2 = \frac{1}{9}s_1^2 - \frac{1}{3}s_2, \\
\ell_1^3 + \ell_2^3 = \frac{2}{27}s_1^3 - \frac{1}{3}s_1 s_2 + s_3, \\
(\ell_1^3 - \ell_2^3)^2 = (\ell_1^3 + \ell_2^3)^2 - 4(\ell_1 \ell_2)^3
\]

\[
= -\frac{1}{27}s_1^3 s_2^2 + \frac{4}{27}s_1^3 s_3 + \frac{4}{27}s_1^3 s_3 - \frac{2}{3}s_1 s_2 s_3 + s_3^2.
\]

Note: for a depressed cubic (which has \( s_1 = 0 \)) these formulas simplify quite a bit.
We have the following diagram of extensions and corresponding Galois groups

\[
\begin{array}{c}
L \\
\downarrow \\
K(t_1) \quad K(t_2) \quad K(t_3) \\
\downarrow \\
K(\ell_1^3) \\
\downarrow \\
K \\
\end{array}
\quad \begin{array}{c}
\{e\} \\
\downarrow \\
\langle (1 3) \rangle \\
\downarrow \\
\langle (1 2) \rangle \\
\downarrow \\
S_3
\end{array}
\]

The extension \( K(\ell_1^3) : K \) is degree 2, generated by roots of the resolvent quadratic

\[ X^2 - (\ell_1^3 + \ell_2^3)X + \ell_1^3\ell_2^3 \in K[X]. \]

Since \( \ell_1^3, \ell_2^3 \in K \), we can also generate this extension by adjoining a squareroot:

\[ K(\ell_1^3) = K(\ell_1^3 - \ell_2^3) = K(\sqrt{\Delta}). \]

It turns out that

\[ (\ell_1^3 - \ell_2^3)^2 = -\Delta/27, \quad \Delta = (t_1 - t_2)^2(t_1 - t_3)^2(t_2 - t_3)^2. \]

The quantity \( \Delta \) is called the **discriminant** of the general cubic, so \( K(\ell_1^3) = K(\sqrt{\Delta}) \) (since \( \sqrt{-3} = 2\omega + 1 \in K \)).

The extension \( L : K(\ell_1^3) \) is degree 3. We have \( L = K(t_1, t_2, t_3) = K(\ell_1, \ell_2) = K(\ell_1) \), so \( L \) is generated over \( K(\ell_1^3) \) by a cube root. It is the splitting field for

\[ (X - \ell_1)(X - \omega^2 \ell_1)(X - \omega^4 \ell_1) = X^3 - \ell_1^3 \in K(\ell_1^3)[X]. \]

**Example (The general quartic).** Suppose characteristic \( F \) is not 2 or 3, and \( F \) contains primitive 3rd and 4th roots of unity. Let \( K = K_4 \) and \( L = L_4 \), and consider \( f = X^4 - s_1 X^3 + s_2 X^2 - s_3 X + s_4 \in K[X] \), with roots \( t_1, t_2, t_3, t_4 \in L \).

The group \( S_4 \) has 30 subgroups, which means I’m not going to write down the whole subgroup lattice. The key part is

\[
\begin{array}{c}
L \\
\downarrow \\
K(y_1, y_2, y_3) \\
\downarrow \\
K(\sqrt{\Delta}) \\
\downarrow \\
K \\
\end{array}
\quad \begin{array}{c}
\{e\} \\
\downarrow \\
V \\
\downarrow \\
A_4 \\
\downarrow \\
S_4
\end{array}
\]

Here \( V = \{e, (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)\} \). We define

\[
y_1 = (t_1 + t_2)(t_3 + t_4), \\
y_2 = (t_1 + t_3)(t_2 + t_4), \\
y_3 = (t_1 + t_4)(t_2 + t_3).
\]

Then \( S_4 \) permutes the set \( \{y_1, y_2, y_3\} \), and these elements are fixed exactly by elements of the subgroup \( V \). The elements \( y_1, y_2, y_3 \) are roots of the resolvent cubic

\[ X^3 - (y_1 + y_2 + y_3)X^2 + (y_1y_2 + y_1y_3 + y_2y_3)X - (y_1y_2y_3) \in K[X] \]

whose coefficients can be written explicitly as polynomials in \( s_1, s_2, s_3, s_4 \). The subfield \( L^{A_4} \) is generated by the squareroot of the discriminant \( \Delta \) of this cubic. It happens that

\[ \Delta = (t_1 - t_2)^2(t_1 - t_3)^2(t_1 - t_4)^2(t_2 - t_3)^2(t_2 - t_4)^2(t_3 - t_4)^2, \]

the **discriminant** of the general quartic.
Each of the extensions in the tower above are obtained by adjoining roots. The lower two extensions are exactly the ones corresponding to the resolvent cubic, while $L = K(\sqrt{y_1}, \sqrt{y_2}, \sqrt{y_3})$ since one can show that you can write the roots $t_1, t_2, t_3, t_4$ in terms of squareroots of expressions involving the $y$s. (See Chapter 18.5.)

Explicitly, the roots are

$$t_1, t_2, t_3, t_4 = \left( s_1 \pm \sqrt{s_1^2 - 4y_1} \pm \sqrt{s_1^2 - 4y_2} \pm \sqrt{s_1^2 - 4y_3} \right) / 4,$$

where the signs on the three squareroots must be chosen so that

$$\sqrt{s_1^2 - 4y_1} \sqrt{s_1^2 - 4y_2} \sqrt{s_1^2 - 4y_3} = s_1^2 - 4s_1s_2 - 3s.$$

This is true because

$$s_1^2 - 4y_1 = (t_1 + t_2 - t_3 - t_4)^2, \quad s_1^2 - 4y_2 = (t_1 - t_2 + t_3 - t_4)^2, \quad s_1^2 - 4y_3 = (t_1 - t_2 - t_3 + t_4)^2,$$

as you can compute explicitly.

**Remark.** There is a general procedure for describing $L^H_n$ for any $H \leq G = S_n$. The idea is: given $\alpha \in L_n$, define

$$H_\alpha := \{ g \in S_n \mid g(\alpha) = \alpha \}, \quad G_\alpha = \{ g(\alpha) \in L \mid g \in G \},$$

and note that $|G_\alpha| = [G : H]$. Then the minimal polynomial of $\alpha$ over $K_n$ is $g = \prod_{\beta \in G_\alpha} (X - \beta) \in K_n[X]$, with $\deg g = [G : H_\alpha]$, and whence $[K_n(\alpha) : K_n] = [G : H_\alpha]$, and so

$$L^H_n = F(\alpha).$$

So to give an “explicit” construction for $L^H_n$, it suffices to find an element $\alpha \in L_n$ whose stabilizer subgroup is exactly $H$.

For a normal subgroup $N \leq S_n$ we can do the following if we want to find a polynomial for which $L_n^N : K_n$ is a splitting field: given $\alpha \in L_n$, let $N_\alpha = \{ g \in S_n \mid g(\beta) = \beta, \forall \beta \in G_\alpha \}$. Then

$$L^N_n = F(\beta, \beta \in G_\alpha)$$

is the splitting field over $K_n$ of the polynomial $g = \prod_{\beta \in G_\alpha} (X - \beta) \in K_n[X]$.

For instance, in the quartic, it turns out that $\alpha = y_1$ leads to $G_\alpha = \{ y_1, y_2, y_3 \}$, and $N_\alpha = V$.

“Cayley’s theorem” says that every finite group $G$ is isomorphic to a subgroup of some symmetric group. To see this, note that for any $g \in G$, the left-multiplication-by-$g$ function $x \mapsto gx$ is a permutation of the set $G$. To turn this into a subgroup of a symmetric group, suppose $|G| = n$, and label the elements of $G$ as $x_1, \ldots, x_n$. For each $g \in G$ define $\sigma_g \in S_n$ by the formula $gx_k = x_{\sigma_g(k)}$. Then $G' = \{ \sigma_g \mid g \in G \}$ is a subgroup of $S_n$, and is isomorphic to the group $G$ by the homomorphism $g \mapsto \sigma_g$. (Exercise: check that it is an isomorphism.)

Therefore we have the the following consequence.

**Proposition.** Every finite group $G$ arises (up to isomorphism) as the Galois group of some finite Galois extension.

**Proof.** Identify $G$ with a subgroup of some $S_n$. Let $L_n = F(t_1, \ldots, t_n)$ be some ring of rational functions in $n$-variables, and let $K = L_n^G$. Then $L_n : K$ is a finite Galois extension with Galois group $G$. \qed
47. The discriminant of a polynomial

Let \( f = \prod (X - t_k) = X^n + \sum (-1)^k s_k X^{n-k} \in K_n[X] \) be the general polynomial of degree \( n \), with roots \( t_1, \ldots, t_n \in R_n = F[t_1, \ldots, t_n] \subseteq L_n = F(t_1, \ldots, t_n) \). The discriminant of \( f \) is the polynomial

\[
\Delta = \prod_{1 \leq i < j \leq n} (t_i - t_j)^2 \in R_n^{S_n},
\]

which is actually a symmetric polynomial in \( n \)-variables.

We have seen some examples:

\[
\begin{align*}
\Delta_2 &= (t_1 - t_2)^2 = s_1^2 - 4s_2, \\
\Delta_3 &= (t_1 - t_2)^2(t_1 - t_3)^2(t_2 - t_3)^2 = s_1^2 s_2^2 - 4s_3^2 - 4s_1s_3 + 18s_1s_2s_3 - 27s_3^2.
\end{align*}
\]

The discriminant the square of an element

\[
\delta = \prod_{1 \leq i < j \leq n} (t_i - t_j) \in R_n
\]

which is not symmetric in general. However, \( \delta \) is fixed by the altering group.

**Proposition.** Suppose characteristic is not 2. For any \( \sigma \in S_n \), we have \( \sigma(\delta) = \pm \delta \), with \( \sigma(\delta) = \delta \) if and only if \( \delta \in A_n \).

**Proof.** We have \( \sigma(\delta) = \prod_{1 \leq i < j \leq n} (t_{\sigma(i)} - t_{\sigma(j)}) \). The factors are the same as those of \( \delta \), except for a sign: whenever \( i < j \) but \( \sigma(i) > \sigma(j) \), \( t_{\sigma(i)} - t_{\sigma(j)} \) is the negative one of the factors of \( \delta \).

For instance, if \( \sigma = (1 2) \), then \( \sigma(i) > \sigma(j) \) for \( i < j \) only if \( i = 1, j = 2 \), so \( (1 2)\delta = -\delta \).

Define \( \phi: S_n \to \{ \pm 1 \} \) by the formula

\[
\sigma(\delta) = \phi(\sigma) \delta.
\]

This defines a homomorphism of groups \( \phi: S_n \to \{ \pm 1 \} \), since

\[
\phi(\tau \sigma) \delta = \tau \sigma(\delta) = \tau (\phi(\sigma) \delta) = \phi(\sigma) \phi(\tau) \delta.
\]

We have \( \phi((1 2)) = -1 \), so \( \phi((1 2)\sigma^{-1}) = -1 \) for all \( \sigma \in S_n \), so \( \phi \) takes all transpositions to \(-1\).

The claim is now straightforward: \( \phi(\sigma) = +1 \) if \( \sigma \) is an even permutation. \( \square \)

**Corollary.** If characteristic is not 2, then \( F(t_1, \ldots, t_n)^{A_n} = K_n(\sqrt{\Delta}) \) where \( K_n = F(s_1, \ldots, s_n) \).

**Proof.** By the Galois correspondence we have \( [L_n^{A_n} : K_n] = 2 \), and we know \( \delta \in L_n^{A_n} \) but \( \delta \notin K_n \). \( \square \)

Because \( \delta \) and \( \Delta \) are polynomial expressions in the roots, we can apply them to the roots of any polynomial. Thus, if \( f \in F[X] \) is a monic polynomial, with roots \( \alpha_1, \ldots, \alpha_n \) (possibly repeated), then we have its discriminant

\[
\Delta_f := \Delta(\alpha_1, \ldots, \alpha_n) \in F.
\]

The discriminant is the square of an element

\[
\delta_f := \delta(\alpha_1, \ldots, \alpha_n)
\]

in the splitting field of \( F \).

**Example.** Let \( f = X^2 + bX + c \in F[X] \). Then \( s_1 = -b, s_2 = c \), so \( \Delta_f = b^2 - 4c \in F \), with a squareroot \( \delta \) in its splitting field. The roots of \( f \) are \((-b \pm \delta)/2\). Note that we have a repeated root iff \( \Delta_f = 0 \).

**Example.** Let \( f = X^3 + pX + q \in F[X] \) be a depressed cubic, where \( p, q \in F \). Then \( s_1 = 0, s_2 = p, s_3 = -q \), and so its discriminant is

\[
\Delta_f = -4p^3 - 27q^2 \in F.
\]

**Proposition.** If \( f \in F[X] \) is a monic polynomial of degree \( n \), then \( f \) is separable iff \( \Delta_f \neq 0 \).
**Proof.** Let \( L : F \) be a splitting field for \( f \) and write \( f = \prod_{k=1}^{n} (X - \alpha_k) \). Then \( \Delta_f = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \), and this is 0 exactly if \( \alpha_i = \alpha_j \) for some \( i \neq j \).

**Proposition.** Let \( F \) be a field not of characteristic 2. Let \( f \in F[X] \) be a separable polynomial, let \( L : F \) be a splitting field with Galois group \( \text{Aut}(L : F) \), and let \( \alpha_1, \ldots, \alpha_n \) be a labelling of the roots of \( f \), which identifies \( \text{Aut}(L : F) \approx G \) with a subgroup \( G \leq S_n \).

Then \( G \leq A_n \) iff \( \Delta(f) \) is the square of an element of \( F \).

**Example.** If \( f = X^3 - 2 \in \mathbb{Q}[X] \), then \( \Delta_f = -4p^3 - 27q^2 = -27(-2)^2 = -2^2 3^3 \), which is not a square of a rational number (since it is negative). So \( G \leq S_3 \) is not a subgroup of \( A_3 \), which implies either \( G = S_3 \) or \( G = \langle (a b) \rangle \) for some 2-cycle. But if \( G = \langle (a b) \rangle \) then \( f \) would be reducible over \( \mathbb{Q} \), and since it is irreducible we must have \( G = S_3 \).

**Example.** If \( f = X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X] \), then \( s_1 = -1, s_2 = -2, s_3 = 1 \), so
\[
\Delta_3(f) = s_1^2 s_2^2 - 4 s_3^2 - 4 s_1 s_2 s_3 - 27 s_3^2 = (-1)^2(-2)^2 - 4(-2)^3 - 4(-1)^3(1) + 18(-1)(-2)(1) - 27(1)^3
\]
\[
= 4 + 32 + 4 + 36 - 27 = 49 = 7^2.
\]
Since \( f \) is irreducible over \( \mathbb{Q} \) (it has no root in \( \mathbb{Q} \) by the rational root test), we must have \( G = A_3 \).

(This is the polynomial whose roots are \( \zeta^k + \zeta^{-k}, k = 1, 2, 3 \), where \( \zeta = e^{2\pi i/7} \). So its splitting field \( L \) is a subfield of \( \mathbb{Q}(\zeta) \), which has Galois group \( \text{Aut}(\mathbb{Q}(\zeta) : \mathbb{Q}) \approx (\mathbb{Z}/7)^\times \approx \mathbb{Z}/6 \).

### 48. Classifying radical extensions

We showed that if \( L : F \) is a finite normal and separable radical extension then \( \text{Aut}(L : F) \) is a soluble group. We will show a converse. This is Chapter 18.4.

Let \( L : F \) be an extension with \( F = L^G \) for some finite \( G \leq \text{Aut}(L) \). (E.g., a finite Galois extension.) Given \( \alpha \in L \) we define the **norm** of \( \alpha \) to be
\[
N(\alpha) = N_{L,F}(\alpha) = \prod_{g \in G} g(\alpha),
\]
the product of all elements of the Galois group applied to \( \alpha \). Note that \( N(\alpha) \in L^G = F \). Note that the function \( N : L \to F \) is product preserving: \( N(\alpha \beta) = N(\alpha)N(\beta) \). It gives a group homomorphism \( N : L^\times \to F^\times \). Also note that \( N(\sigma(\alpha)) = N(\alpha) \) for any \( \sigma \in G \): the norms of Galois conjugate elements are the same.

**Example.** Consider \( \mathbb{C} : \mathbb{R} \). Then
\[
N(a + bi) = (a + bi)(a - bi) = a^2 + b^2, \quad a, b \in \mathbb{R}.
\]
Remember that this gives a formula for the multiplicative inverse in \( \mathbb{C} \):
\[
(a + bi)^{-1} = \frac{a - bi}{a^2 + b^2}.
\]

**Example.** Consider \( L = \mathbb{Q}(\gamma, \omega) : \mathbb{Q} \), where \( \gamma = \sqrt[3]{2} \) and \( \omega = e^{2\pi i/3} \). This is a Galois extension with Galois group \( G = \langle \sigma \rangle \) of order 3, with \( \sigma(\gamma) = \omega \gamma \). Let \( u = a + b\gamma + c\gamma^2 \in L \), with \( a, b, c \in \mathbb{Q}(\omega) \). Then
\[
N(u) = (a + b\gamma + c\gamma^2)(a + b\omega \gamma + c\omega \gamma^2)(a + b\omega^2 \gamma + c\omega^2 \gamma^2)
\]
\[
= (a + b\gamma + c\gamma^2)(a^2 + b^2 \gamma^2 + 2c^2 \gamma - ab \gamma - ac \gamma^2 - 2bc)
\]
\[
= a^3 + 2b^3 + 4c^3 - 6abc.
\]
This gives a formula for multiplicative inverse in $L$:

$$(a + b\gamma + c\gamma^2)^{-1} = \frac{(a^2 - 2bc) + (2c^2 - ab)\gamma + (b^2 - ac)\gamma^2}{a^3 + 2b^3 + 4c^3 - 6abc}.$$  

Note that the denominator is in $\mathbb{Q}(\omega)^\times$.

A cyclic extension is a finite Galois extension with cyclic Galois group.

**Theorem** (Hilbert’s Theorem 90). Let $L : F$ be a finite Galois extension with cyclic Galois group $G$, generated by some $\tau \in G$. Let $a \in L$. Then $N(a) = 1$ iff there exists $b \in L^\times$ such that $a = b/\tau(b)$.

**Proof.** Suppose $|G| = n$.

$\iff$: If $a = b/\tau(b)$, then

$$N(a) = \prod_{k=0}^{n-1} \tau^k(a) = \prod_{k=0}^{n-1} \tau^k(b)/\tau^{k+1}(b) = 1.$$  

$\implies$: Suppose $N(a) = 1$. Define

$$\lambda_0 = 1, \quad \lambda_1 = a, \quad \lambda_2 = a\tau(a), \quad \lambda_3 = a\tau(a)^2(a), \ldots, \quad \lambda_{n-1} = a\tau(a)\cdots\tau^{n-2}(a).$$  

Thus $\tau(\lambda_k) = \lambda_{k+1}/a$ for $k = 0, \ldots, n-2$ and also $\tau(\lambda_{n-1}) = N(a)/a = \lambda_0/a$. If we think of the $\lambda_k$ as being indexed by $k \in \mathbb{Z}/n$, then we can just say $\tau(\lambda_k) = \lambda_{k+1}/a$ for all $k$.

Consider any $c \in L$, and set

$$b := \sum_{k=0}^{n-1} \lambda_k \tau^k(c) = \lambda_0 c + \lambda_1 \tau(c) + \lambda_2 \tau^2(c) + \cdots + \lambda_{n-1} \tau^{n-1}(c) = c + a \tau(c) + a\tau(a) \tau^2(c) + a\tau(a)^2 \tau^3(c) + \cdots + (a\tau(a)\cdots\tau^{n-2}(a))\tau^{n-1}(c).$$  

Then

$$\tau(b) = \tau(\lambda_0)\tau(c) + \tau(\lambda_1)\tau^2(c) + \cdots + \tau(\lambda_{n-2})\tau^{n-1}(c) + \tau(\lambda_{n-1})\tau^n(c) = a^{-1}[\lambda_0 c + \lambda_1 \tau(c) + \cdots + \lambda_{n-2} \tau^{n-2}(c) + \lambda_{n-1} \tau^{n-1}(c)] = a^{-1}b.$$  

Therefore, as long as $b \neq 0$, we have that $a = b/\tau(b)$.

It remains to show that we can choose $c \in L$ so that $b \neq 0$. If not, then

$$0 = \lambda_0 \tau^0(c) + \lambda_1 \tau^1(c) + \cdots + \lambda_{n-1} \tau^{n-1}(c) \quad \forall c \in L.$$  

This implies a linear relation $0 = \lambda_0 \tau^0 + \cdots + \lambda_{n-1} \tau^{n-1}$ in $\text{Hom}_F(L, L)$. By linear independence of field homomorphisms we must have all $\lambda_i = 0$, but we know $\lambda_0 = 1 \neq 0$, so that is impossible. $\blacksquare$

The following classifies all cyclic extensions $L : F$, assuming $F$ contains “enough” roots of unity.

**Proposition.** Let $L : F$ be a finite Galois extension with cyclic Galois group $G$ of order $n$. Suppose that $F$ contains a primitive $n$th root of unity $\zeta$. Then there exists $\alpha \in L$ such that $L = F(\alpha)$ and $c = \alpha^n \in F$. Furthermore $L$ is the splitting field of $X^n - c \in F[X]$, which is irreducible over $F$.

**Proof.** Let $\tau$ be a generator of $G$. Since $\zeta \in F = L^G$, we have

$$N(\zeta) = \prod_{k=0}^{n-1} \tau^k(\zeta) = \prod_{k=0}^{n-1} \zeta = \zeta^n = 1.$$  

By Hilbert’s Theorem 90, there exists $\alpha \in L$ such that $\zeta = \alpha/\tau(\alpha)$. That is, $\tau(\alpha) = \zeta^{-1}\alpha$. Iterating this gives

$$\tau^k(\alpha) = \zeta^{-k}\alpha, \quad k = 0, \ldots, n-1.$$
Because $\zeta$ is a primitive $n$th root of unity, the list of elements $1, \zeta^{-1}, \ldots, \zeta^{-(n-1)}$ are distinct. Note that $\alpha \neq 0$ since its norm is non-zero, so the $\zeta^{-k}\alpha$ are distinct elements of $L$ for $k = 0, \ldots, n-1$.

The element $c := \alpha^n$ satisfies $\tau(c) = c$, so $c \in F$. Thus $f = X^n - c \in F[X]$, and $F(\alpha) : F$ is a splitting field of $f$. Thus $F(\alpha) : F$ is a normal extension, so each element of $G$ induces an automorphism of $F(\alpha) : F$. But the above formulas show that the $\tau^0, \ldots, \tau^{n-1}$ have different values on $\alpha$, so that $|\text{Aut}(F(\alpha) : F)| = |G|$. Therefore $F(\alpha) = L$. Because $G$ acts transitively on the roots of $f$ we must have $f \in \text{Irred}(F)$.

Note: the book proves a version of this (Theorem 18.19) assuming $n$ is prime. My version doesn’t need this restriction\footnote{In my version of the proposition I assume that $F$ contains a primitive $n$th root of unity. The book’s version only assumes that $X^n - 1$ splits in $F$. These are not exactly the same condition because of separability issues in positive characteristic, as we will soon see. If the characteristic $p > 0$, then $X^n - 1$ is separable as long as $p \nmid n$, in which case one of the roots (in its splitting field) will be a primitive $n$th root of unity, a fact we will prove later.} However, I only need the prime case in what follows.

**Remark.** The hypothesis about having a primitive root of unity in $F$ is necessary. In particular, if $L : F$ is a cyclic Galois extension of prime degree $p$ such that $F$ does not contain a primitive $p$th root of unity, then there is no $\alpha \in L \setminus F$ such that $\alpha^p \in F$. (Exercise: prove this.)

An example is the splitting field $L$ of $f = X^3 + X^2 - 2X - 1 \in \text{Irred}(Q)$. As we have seen, $G = \text{Aut}(L : Q)$ is cyclic of order 3. In fact, $L \subseteq Q(\zeta_7)$, where $\zeta_k^7 + \zeta_k^{-6}$ for $k = 1, 2, 3$ are the roots of $f$. However, there is no $\alpha \in L \setminus Q$ such that $\alpha^3 \in Q$.

I’m going to need the following.

**Lemma.** Let $K, N \subseteq M$ be subfields, with subfield $F \subseteq K \cap N$, such that $N : F$ is a finite normal extension. Let $NK \subseteq M$ be the composite field.

$$
\begin{align*}
\text{M} & \quad \text{F} \\
\text{NK} & \quad \text{N} \\
\text{K} & \quad \text{finite normal} \\
\text{F} & \quad \text{normal}
\end{align*}
$$

Then

- $NK : K$ is also a finite normal extension, and
- $\text{Aut}(NK : K)$ is isomorphic to a subgroup of $\text{Aut}(N : F)$, (whence $[NK : K] | [N : F]$).

**Proof.** Since $N : F$ is a finite normal extension, it is the splitting field of a polynomial $f \in F[X]$. So $N : F$ is generated by the roots of $f$, and so the composite field $NK$ is also generated over $K$ by the roots of $f \in F[X] \subseteq K[X]$, i.e., $NK : K$ is a splitting field of $f$, so its a finite normal extension.

Next, note that if $\phi \in \text{Aut}(KN : K)$, then $\phi|K = \text{id}_K$ and $\phi$ permutes the roots of $f$. This implies that $\phi(N) = N$, since $N : F$ is the splitting field of $f$. Thus we can define a function $\text{Aut}(NK : K) \rightarrow \text{Aut}(N : F)$, $\phi \mapsto \phi|N$ which is a homomorphism of groups. Also note that if $\phi|N = \text{id}_N$, then $\phi = \text{id}$ since we also know $\phi|K = \text{id}_K$ and $NK$ is a composite field. Thus $\text{Aut}(NK : K) \rightarrow \text{Aut}(N : F)$ is an injective homomorphism, so gives an isomorphism of groups between $\text{Aut}(NK : K)$ and a subgroup of $\text{Aut}(N : F)$.

**Proposition.** Let $F \subseteq \mathbb{C}$ and let $L : F$ be a finite Galois extension with solvable Galois group $G$. Then there exists a finite extension $R : L$ such that $R : F$ is a radical extension.
Proof. We work by induction on \([L : F] = |G|\), where the case of \([L : F] = 1\) is obvious. I’m going to use that we are in characteristic 0, so that all normal extensions are Galois extensions.

If \(|G| > 1\), choose a proper normal subgroup \(H \leq G\) of maximal order. Maximality means that \(G/H\) must be simple. Since \(G\) is solvable so is \(G/H\), so \(G/H\) must be cyclic of some prime order \(p\). Let \(K = L^H\). Since \(H\) is normal \(K : F\) is a cyclic Galois extension of degree \(p\). Let \(\zeta\) be a primitive \(p\)th root of unity, and consider

\[
\begin{align*}
L(\zeta) & \to L \\
K(\zeta) & \to L \\
F(\zeta) & \to K \\
& \to p \\
& \to F
\end{align*}
\]

Clearly \(F(\zeta) : F\) is a radical extension. I’ll show that \(K(\zeta) : F(\zeta)\) is also a radical extension, and that there exists an extension \(R : L(\zeta)\) such that \(R : K(\zeta)\) is radical. These will imply that the composite extension \(R : F\) is radical.

I apply the Lemma to each of the two parallelograms.

- \(K : F\) is a finite normal extension and \(K(\zeta) = KF(\zeta)\), so \([K(\zeta) : F(\zeta)]\) divides \([K : F] = p\). Therefore either (i) \(K(\zeta) = F(\zeta)\), or (ii) \(K(\zeta) : F(\zeta)\) is a cyclic extension of order \(p\) where \(F(\zeta)\) contains a primitive \(p\)th root of unity, so is a radical extension.

- \(L : K\) is a finite normal extension, and its Galois group \(\text{Aut}(L : K) = H\) is a subgroup of \(G\) and so is solvable. Since \(L(\zeta) = LK(\zeta)\) we have that \(L(\zeta) : K(\zeta)\) is a finite Galois extension with \(\text{Aut}(L(\zeta) : K(\zeta))\) isomorphic to a subgroup of \(H\), and so solvable. Since \(|H| < |G|\), by induction there exists \(R : L(\zeta)\) such that \(R : K(\zeta)\) is a radical extension.

Thus each of \(F \subseteq F(\zeta) \subseteq K(\zeta) \subseteq R\) are radical extensions, so \(R : F\) is a radical extension containing \(L : F\).

Exercise. The previous proposition requires that \(L : F\) be a Galois extension. This is necessary. Give an example of a finite extension \(L : \mathbb{Q}\) such that \(\text{Aut}(L : \mathbb{Q})\) is solvable, but \(L : \mathbb{Q}\) is not contained in any radical extension of \(\mathbb{Q}\).

49. Artin-Schreier theorem

The extension \(C : \mathbb{R}\) is special: it’s a finite extension such that the big field is algebraically closed. It turns out that all such extensions look kind of like \(C : \mathbb{R}\).

Theorem (Artin-Schreier). Suppose \(C : F\) is a field extension with \(1 < |C : F| < \infty\), and \(C\) algebraically closed. Then \(F\) has characteristic 0, and \(C = F(i)\) where \(i^2 = -1\).

I’m going to prove this under the hypothesis that \(F\) has characteristic 0. This hypothesis will be used in two places in the proof. It can be removed, but I don’t want to do it now.

Proof, assuming characteristic 0. Clearly \(C : F\) is a normal extension, and is separable since characteristic is 0. So it is a Galois extension, and must have a non-trivial Galois group \(G = \text{Aut}(C : F)\).

First, I’ll do a special case: \(G\) is cyclic of prime order \(p\). I’ll show that the only possibility is \(p = 2\), and in that case we have \(C = F(i)\).

Suppose \(|G| = |C : F| = p\) with \(p\) prime, so that \(G\) is cyclic: \(G = \langle \sigma \rangle\). Since \(C\) is algebraically closed, \(X^p - 1\) splits over \(C\). Because \(C\) does not have characteristic \(p\), this polynomial is separable.
and so $C$ contains a primitive $p$th root of unity $\zeta$. We know that $[F(\zeta) : F] \leq p - 1$ since $\zeta$ is a root of $\Phi_p$. The tower law $p = [C : F] = [C : F(\zeta)][F(\zeta) : F]$ then implies $\zeta \in F$.

Therefore by previous results $C = F(\gamma)$ for some $\gamma$ with $\gamma^p \in F$ (e.g., by Hilbert 90 there is a $\gamma$ such that $\sigma(\gamma)/\gamma = \zeta$ since $N(\zeta) = \zeta^p = 1$). Since $C$ is algebraically closed there exists $\beta \in C$ with $\beta^p = \gamma$. Let $\omega = \sigma(\beta)/\beta$. Then

$$\omega^{p^2} = \sigma(\beta^{p^2})/\beta^{p^2} = \sigma(\gamma^p)/\gamma^p = 1, \quad \omega^p = \sigma(\beta^p)/\beta^p = \sigma(\gamma)/\gamma \neq 1$$

because $\gamma^p \in F$ but $\gamma \notin F$. That is, $\omega$ is a primitive $p^2$ root of unity. This implies $\omega^p \in F$, since $\omega^p$ is a $p$th root of unity so is equal to $\zeta^j$ for some $j$.

Write $\sigma(\omega) = \omega^a$ for some $a \in \mathbb{Z}$. Since $\omega^p \in F$ we have

$$\omega^p = \sigma(\omega^p) = \omega^{pa} \quad \implies \quad pa \equiv p \mod p^2 \quad \implies \quad a \equiv 1 \mod p.$$ 

So write $a = 1 + pk$ for some $k \in \mathbb{Z}$.

By Hilbert Theorem 90, $\omega = \sigma(\beta)/\beta$ implies $N(\omega) = 1$. Therefore

$$1 = N(\omega) = \omega \sigma(\omega) \cdots \sigma^{p-1}(\omega) = \omega^{1+a+a^2+\cdots+a^{p-1}} = \omega^{1+(1+kp)+(1+kp)^2+\cdots+(1+kp)^{p-1}}.$$ 

So the exponent in the last line must be divisible by $p^2$. The binomial formula tells us

$$a^m = (1 + kp)^m \equiv 1 + mkp \mod p^2.$$ 

Thus, modulo $p^2$:

$$0 \equiv 1 + a + \cdots + a^{p-1} \equiv \sum_{m=0}^{p-1} (1 + mkp) \mod p^2 \equiv p + kp(0 + 1 + \cdots + (p - 1)) \equiv p + kp \frac{p(p - 1)}{2}.$$ 

If $p$ is odd, $p$ divides $p(p - 1)/2$ so we get $0 \equiv p \mod p^2$ which is impossible.

If $p = 2$ then we must have $0 \equiv 2 + 2k \mod 4$, so $k$ is odd and so $a = 1 + 2k \equiv -1 \mod 4$. Then $\omega = i$ and $\sigma(i) = -i$, so $i \notin F$ and thus $C = F(i)$.

We return to the general case of $1 < |G| < \infty$. If a prime $p$ divides $|G|$, then by Cauchy’s theorem there exists a subgroup $H \leq G$ of order $p$, whence a Galois extension $C : C^H$ with $\text{Aut}(C : C^H) = H$, which is impossible by the above analysis if $p$ is odd. Therefore $G$ must be a 2-group, i.e., that $|G| = 2^k$ for some $k$. We need to show $|G| = 2$, so we assume 4 divides the order and derive a contradiction.

It is the case that every non-trivial 2-group contains an element of order 2 in the center (see proof below). So we can form $N \leq H \leq G$ with $|N| = 2$ generated by a central element (and so $N$ is normal), and $|H| = 4$, where $H$ is the preimage under $G \twoheadrightarrow G/H$ of a subgroup of order 2 in $G/H$, which exists because $G/H$ is a non-trivial 2-group. Let $K = C^N$ and $F = C^H$, and consider
By what we just proved, $C = K(i)$ since $C : K$ is a Galois extension of degree 2. This means $i \notin K$, so $i \notin F$ and thus $[F(i) : F] = 2$, and therefore $[C : F(i)] = 2$ by the tower law. But we showed that any subfield of $C$ of index 2 does not contain $i$, a contradiction. 

**Proposition.** If $G$ is a finite $p$-group (i.e., $|G| = p^k$ for some prime $p$ and $k \geq 1$), then $G$ contains an element of order $p$ in its center.

**Proof.** Central elements $x$ of $G$ are exactly those whose conjugacy class $\text{Cl}(x) = \{ gxg^{-1} \mid g \in G \}$ has size 1. The order of a conjugacy class $\text{Cl}(x)$ is equal to the index $[G : H_x]$ of the centralizer subgroup $H_x = \{ g \in G \mid gxg^{-1} = x \}$, and so is a divisor of $|G|$. Since $|G| = p^k$ this means the number of singleton conjugacy classes (= number of elements in the center) must be divisible by $p$, and since there is at least one such ($\text{Cl}(e) = \{ e \}$), there are at least $p$ such. So the center of $G$ is non-trivial, and so contains an element of order $p$ by Cauchy’s theorem.

It turns out that any field as in the previous proposition “looks like” the real numbers in some ways. For instance, it is ordered.

**Proposition.** Let $C : R$ be a field extension of degree 2, with $C$ algebraically closed. Then the set $R^2 \subseteq R$ of squares in $R$ is closed under addition and does not contain $-1$.

In particular, $R$ is an ordered field, with $(R^\times)^2$ as the set of positive elements.

**Proof.** Because $C = F(i) \neq F$ we see that $-1$ is not a square of an element of $R$.

Suppose $a, b \in R$. Because $C$ is algebraically closed, we have $a + bi = (c + di)^2$ for some $c, d \in R$. Then

$$a^2 + b^2 = (a + bi)(a - bi) = (c + di)^2(c - di)^2 = [(c + di)(c - di)]^2 = (c^2 + d^2)^2,$$

so a sum of squares in $R$ is a square of an element of $R$. Furthermore, if $a, b \neq 0$ then $a^2 + b^2 \neq 0$ (since otherwise $b^2 = -a^2$ whence $-1 = (b/a)^2$, but $-1$ is not a square in $R$). Thus the set $(R^\times)^2$ of squares of non-zero elements is also closed under addition.

It is obvious that $(R^\times)^2$ is closed under multiplication.

Finally, we have that for all $a \in R$, exactly one of: $a = 0$, $a \in (R^\times)^2$, or $-a \in (R^\times)^2$ is true. If $a \neq 0$, then $a = (c + di)^2$ for some $c, d \in R$, whence $a = (c^2 - d^2) + (2cd)i$, which implies either (i) $d = 0$, so $a = c^2$, or (ii) $c = 0$, so $-a = d^2$. We can’t have both $a, -a \in (R^\times)^2$ since that would imply $-1 = (-a)/a \in (R^\times)^2$ which is not the case.

\[ \square \]

See [https://kconrad.math.uconn.edu/blurbs/galoistheory/artinschreier.pdf](https://kconrad.math.uconn.edu/blurbs/galoistheory/artinschreier.pdf) for more info, including the positive characteristic case.

50. Real closed field

A **real closed field** is an ordered field $R$ such that (i) every positive element of $R$ has a square root in $R$, and (ii) every polynomial of odd degree over $R$ has a root in $R$.

**Example.** The real numbers are a real closed field. The proofs of (i) and (ii) use the intermediate value theorem: $f(x) = x^2 - a$ with $a > 0$ has $\lim_{x \to \pm\infty} f(x) = +\infty$, and $f(0) < 0$, whence $f$ has roots, while $g(x)$ of odd degree is such that $\lim_{x \to +\infty} g(x)$ and $\lim_{x \to -\infty} g(x)$ are infinite with opposite signs.

**Example.** The field $F = \mathbb{Q}_{\text{alg}} \cap \mathbb{R}$ consisting of real numbers which are algebraic is real closed.

Note that $R$ must have characteristic 0 since it is ordered. Since $-1$ cannot be a square of an element of $R$, we see that $R$ is not algebraically closed. Given a real closed $R$, define $C := R(i)$ to be the splitting field of $X^2 + 1 \in R[X]$. Since $-1$ is not a square in $R$ we have $[C : R] = 2$.

**Lemma.** Let $R$ be a real closed field, and let $C = R(i)$. Then every element of $C$ has a square root in $C$.
Proof. First note that every element \(a \in R\) has a square root in \(C\): by hypothesis if \(a \geq 0\), while if \(a < 0\) then \(a = (bi)^2\) with \(b^2 = -a\). For \(u = a + bi \in C\) with \(a, b \in R\) and \(b \neq 0\), choose a square root \(r = \sqrt{a^2 + b^2} \in R\). Then
\[
\sqrt{\frac{a + r}{2}} + \sqrt{\frac{a - r}{2}} \in C
\]
is a square root of \(u\), where the signs on the square roots are chosen so that
\[
\sqrt{\frac{a + r}{2}} \sqrt{\frac{a - r}{2}} = \sqrt{-\frac{b^2}{4}} = \frac{bi}{2}.
\]
(This is basically the same thing as the “half-angle formula” from trigonometry: \(\cos^2(\theta/2) = (1 + \cos \theta)/2\) and \(\sin^2(\theta/2) = (1 - \cos \theta)/2\), so \(e^{i\theta/2} = \sqrt{(1 + \cos \theta)/2 + i\sqrt{(1 - \cos \theta)/2}}\) if \(-\pi \leq \theta \leq \pi\).)

Proposition. A field \(R\) is a real closed field iff \(C := R(i)\) is algebraically closed and \(i \notin R\).

Proof. \(\iff\): If \(i \notin R\) and \(C = R(i)\) algebraically closed, then we have already proved that \(R\) is an ordered field, with \((R^\times)^2\) the set of positive elements. By definition positive elements have a square root. All \(f \in \text{Irred}(R)\) must have degree 1 or 2 since \([C : R] = 2\), so any odd degree \(f \in R[X]\) must have a linear factor.

Now we prove the converse, that any real closed field \(R\) has \(C = R(i)\) as its algebraic closure. I will use two facts from group theory (proved below). Recall that a \(p\)-group is a finite group with order \(p^k\) for some \(k\).

- For every prime \(p\), every finite group \(G\) has a subgroup \(P \leq G\) which is a \(p\)-group, and such that \(p \nmid |G : P|\). (First Sylow theorem.)
- Every non-trivial \(p\)-group has a subgroup of index \(p\).

In fact, I only need these facts for \(p = 2\).

Any finite extension \(K : C\) gives a finite extension \(K : R\), which in turn is contained in some finite Galois extension \(L : R\) with \(C \subseteq L\). So to show \(C\) is algebraically closed it suffices to show \([L : R] = 2\) for any such extension. Choose such an extension and let \(G = \text{Aut}(L : R)\) and \(H = \text{Aut}(L : C)\).

Since there are no irreducible polynomials over \(R\) of odd degree greater than 1, every non-trivial simple algebraic extension \(R(\alpha) : R\) has even degree, and so every non-trivial finite extension over \(R\) has even degree. Thus every proper subgroup \(K \leq G\) must have even index. Since \(G\) has a 2-Sylow subgroup \(P \leq G\) of odd index (by the first Sylow theorem), we can only have \(G = P\), i.e., \(|G| = 2^k\).

Therefore the subgroup \(H\) is also a 2-group, and thus if \(|H| > 1\) there is \(K \leq H\) with \(|H : K| = 2\), and thus a degree 2 extension \(C = L^H \subseteq L^K\). But this is impossible because every quadratic polynomial in \(C\) splits as we showed above.

Since the reals are clearly a real closed field, this gives another proof of the algebraic closure of \(C\).

Proposition. If \(|G| = p^m\) (\(p\) prime) and \(m \geq 1\), then there exists a normal subgroup of index \(p\) in \(G\).

Proof. Induction on \(m\). If \(m = 1\) then \(\{e\}\) is the index \(p\) normal subgroup. Earlier, I showed every non-trivial \(p\)-group has an element of order \(p\) in its center, which generates a normal subgroup \(N \triangleleft G\) of order \(p\). The quotient group \(G/N\) has order \(p^{m-1}\), and by induction contains a normal subgroup \(\overline{H} \leq G/N\) of index \(p\). Then \(H = \pi^{-1}\overline{H}\) has index \(p\) in \(G\) and is normal in \(G\), where \(\pi : G \to G/N\) is the projection homomorphism.

As a consequence, every \(p\)-group is a solvable group, since we can inductively choose a chain of subgroups \(G > G_1 > G_2 > \cdots\) such that each is normal in the next with quotient group cyclic of order \(p\).
Theorem (First Sylow theorem). Let $G$ be a finite group of order $n = p^k m$, where $p$ is prime and $p \nmid m$. Then there exists a subgroup $P \leq G$ such that $|P| = p^k$, i.e., such that $|P|$ has order a power of $p$ and $p \nmid [G : P]$

Proof. This is an induction on the order $n$, with the case $n = 1$ being obvious, as is the case $k = 0$, so we may assume $p \mid n$.

Consider the conjugacy class $\text{Cl}(x) = \{ gxg^{-1} \mid g \in G \}$ of an element $x \in G$. The collection of conjugacy classes partition $G$ into pairwise disjoint subsets. Furthermore, each $|\text{Cl}(x)|$ is equal to the index of some subgroup of $G$: in fact, $|\text{Cl}(x)| = |G| / |H_x|$, where $H_x = \{ g \in G \mid gxg^{-1} = x \}$ is the centralizer subgroup of $x$. In particular, $|\text{Cl}(x)| = 1$ iff $x$ is in the center of $G$, i.e., if $gx = xg$ for all $g \in G$.

There are two cases.

1. There exists a proper subgroup $G' < G$ such that $p$ does not divide $[G : G']$, so $|G'| = p^k m' < n$ with $p \nmid m'$. Then induction on order provides a subgroup $P \leq G'$ with $|P| = p^k$.
2. There does not exist any such subgroup $G'$. Then all proper subgroups $G' < G$ have $p \mid [G : G']$. As a consequence, every conjugacy class $\text{Cl}(x)$ in $G$ with $|\text{Cl}(x)| > 1$ has $p \mid |\text{Cl}(x)|$. Since $p \mid n$ and $\text{Cl}(e) = \{ e \}$, there must be some $x \neq e$ in the center of $G$. Let $N = \langle x \rangle$. This is a non-trivial normal subgroup, so we can form $G := G/N$. Since $|G| < n$ by induction it has a subgroup $\overline{P} \leq G$ of index prime to $p$. Let $P \leq G$ be the preimage of $\overline{P}$ under the projection $G \to G/N$. Then $[G : P] = [G : \overline{P}]$ and $|P| = p |\overline{P}|$ has prime power order as desired.

Example. A Puiseux series over $F$ in some variable $X$ is an expression of the form

$$f = \sum_{k \geq k_0} c_k X^{k/n}, \quad n \geq 1, \quad k_0 \in \mathbb{Z}.$$ 

Let $F\{X\}$ denote the set of Puiseux series. This set naturally a commutative ring. In fact, it is a field.

If $F = \mathbb{R}$, then $\mathbb{R}\{X\}$ is a real closed field. Positive elements are non-zero series $f = \sum c_k X^{k/n}$ such that the smallest non-zero $c_k$ is positive. We have that $\mathbb{R}\{X\}(i) = \mathbb{C}\{X\}$, and $\mathbb{C}\{X\}$ is algebraically closed by the “Newton-Puiseux theorem”.

51. POSITIVE CHARACTERISTIC AND FROBENIUS

Now I’m going to talk about field extensions in positive characteristic. We have established the Galois correspondence for field extensions in all characteristics, which includes positive characteristic. But this correspondence only holds for separable extensions, and extensions can fail to be separable in positive characteristic. This material is from Chapter 17.5.

Proposition. Suppose $F$ is a field of positive characteristic $p$. Then the function $\phi : F \to F$ defined by

$$\phi(a) = a^p$$

is a homomorphism of fields.

Proof. We have that $\phi(1) = 1$ and $\phi(ab) = (ab)^p = a^p b^p = \phi(a) \phi(b)$. Furthermore,

$$\phi(a + b) = (a + b)^p = \sum_{j=0}^{p} \binom{p}{j} a^{p-j} b^j.$$ 

The binomial coefficient $\binom{p}{j}$ is the integer $\frac{p(p-1)\cdots(p-j+1)}{j!}$. If $0 < j < p$ then $p$ divides $\binom{p}{j}$. □
The map $\phi(a) = a^p$ is called the **Frobenius homomorphism**.

In particular, for elements $a, b$ in a field $F$ of characteristic $p > 0$, we always have

$$(a + b)^p = a^p + b^p.$$  

**Example.** In $F = \mathbb{F}_p$, the Frobenius is the identity map: $a^p = a$ by Fermat’s little theorem.

**Example.** Let $K = \mathbb{F}_2[X]/(X^2 + X + 1)$. This is a field because the polynomial is irreducible over $\mathbb{F}_2$. It has four elements: $0, 1, \gamma, \gamma + 1$, where $\gamma = X$. We have $\gamma^2 = \gamma + 1$.

Thus the Frobenius $\phi: K \to K$ is a non-trivial automorphism, which sends $\phi(\gamma) = \gamma^2 = \gamma + 1$. In fact, $\text{Aut}(K : \mathbb{F}_2) = \{e, \phi\}$.

**Example.** Let $K = \mathbb{F}_2[X]/(X^3 + X + 1)$. This is a field because the polynomial is irreducible over $\mathbb{F}_2$. It has 8 elements: $a + b\gamma + c\gamma^2$ with $a, b, c \in \mathbb{F}_2$, where $\gamma = X$ satisfies $\gamma^3 = \gamma + 1$. We have that $\text{Aut}(K : \mathbb{F}_2) = \{e, \phi, \phi^2\}$, with $\phi(\gamma) = \gamma^2$ and $\phi^2(\gamma) = \gamma^4 = \gamma^2 + \gamma$.

The image $\phi(K) \subseteq K$ is a subfield. In fact, $\phi(K) = \mathbb{F}_2(\gamma)$.

The Frobenius doesn’t have to be an isomorphism.

**W 6 Nov**

**Example.** Let $K = \mathbb{F}_p(t)$ be a function field. Then $\phi: K \to K$ is not an isomorphism: the element $t$ is not in the image of $\phi$. The Frobenius is identity on elements of $\mathbb{F}_p$, so $\phi(g(t))/h(t)) = g((tp))/h(tp)$, where $g, h \in \mathbb{F}_p[t]$ are polynomials. If $t = g(tp)/h(tp)$, then $t(h(tp)) = g(tp)$ is an equality of polynomials, but it impossible for degree reasons: $1 + p \deg(h) = p \deg(g)$ has no solution.

Because it is a field homomorphism the Frobenius is always injective. There is an immediate consequence: if $F$ is a field of characteristic $p > 0$, then elements $a \in F$ can have *at most* one $p$th root in $F$, or in any extension of $F$. Thus, $a^p = b^p$ implies $a = b$ in fields of characteristic $p > 0$.

(More consisely: $a^p - b^p = (a - b)^p$.)

This means that there are no primitive $p$th roots of unity in characteristic $p$, and in fact no primitive $n$th roots of unity whenever $p \mid n$. (If $n = mp$, then $a^{mp} = 1$ implies $a^m = 1$.)

In fact, we can completely understand how a polynomial like $X - a$ factors in a field of characteristic $p$.

**Proposition.** Let $K$ be a field of characteristic $p$, and let $f = X^{p^n} - a \in K[X]$. Then either

1. $f = (X^{p^{n-1}} - b)^p$ for some $b \in K$ such that $a = b^p$, or
2. $f = X^{p^n} - a$ is irreducible in $K[X]$.

**Proof.** I’ll show that if $f$ is reducible then $a$ is a $p$th power.

So suppose $f = gh$ over $K$ with $\deg g, \deg h \leq \deg f$. Let $L : K$ be an extension containing a root $c$ of $f$, so that $c^{p^n} = a$, and thus $f = (X - c)^{p^n}$ over $L$. Then over $L$ we must have $g = (X - c)^r$ for some $0 < r < p^n$. Write $r = p^km$, with $p \mid m$ and $0 \leq k < n$. Then

$$g = (X - c)^r = ((X - c)^p)^m = (X^{p^k} - c^p)^m = X^{p^km} - mc^{p^k}X^{p^k(m-1)} + \cdots,$$

which implies $mc^{p^k} \in K$ and thus $c^{p^k} \in K$ since $p \mid m$. But since $k < n$ we have $b := c^{p^{n-1}} \in K$, and thus $a = c^{p^n} = b^p$ is a $p$th power of an element of $K$.

In particular: either $a \in K^p$ or $X^p - a \in \text{Irred}(K)$, but not both.

### 52. Positive characteristic, separable extensions, perfect fields

Recall that a polynomial $f \in F[X]$ is separable when $f$ and $Df$ are relatively prime. In characteristic $p > 0$, we can have $Df = 0$ even if $f \neq 0$, which means we have some polynomials which are “unexpectedly” not separable. For instance, $X^p - a$ is never separable in characteristic $p > 0$.

In characteristic 0, all irreducible polynomials are separable. In characteristic $p > 0$ we have the following.
Proposition. Let $F$ be a field of characteristic $p > 0$, and consider $f \in \text{Irred}(F)$. Then $f$ is not separable iff $Df = 0$ iff $f$ has the form $f = \sum c_k X^{pk}$, with $c_k \in F$ iff $f = g(X^p)$ for some $g \in F[X]$.

Proof. Write $f = \sum a_k t^k$ with $a_k \in F$. Then $Df = \sum ka_k t^{k-1} = 0$ if and only if each $ka_k = 0$ in $F$. Which only happens if $a_k = 0$ when $p \nmid k$. Which happens exactly when $f = g(X^p)$, where $g = \sum_k a_{pk} X^k$.

Recall that given an extension $L : F$, an element $\alpha \in L$ is separable if it is algebraic over $F$ and $f_{\alpha/F}$ is a separable polynomial. The extension $L : F$ is separable if all elements of $L$ are separable.

Example (Example of inseparable algebraic extension). Let $L = \mathbb{F}_p(t)$, a function field over $\mathbb{F}_p$. Let $K = \mathbb{F}_p(t^p)$ be the subfield generated by $t^p$. Since $t^p$ is transcendental, $K$ is also isomorphic to a function field. I’ll write $u = t^p$, so $K = \mathbb{F}_p(u)$. We know that

- $u = t^p$ is not the $p$th power of an element of $K$, so
- $f = X^p - u \in K[X]$ is an irreducible polynomial over $K = \mathbb{F}_p(u)$, but
- $f = f_{t/K}$ is not separable.

In fact, over $L$ the polynomial $f$ factors as $(X - t)^p$.

Here is a characterization of separable elements.

Lemma. Let $K : F$ be an extension of fields of characteristic $p > 0$, and $\alpha \in K$. Then $\alpha$ is separable over $F$ if and only if $\alpha \in F(\alpha^p)$, iff $F(\alpha^p) = F(\alpha)$.

Proof. Note that $F(\alpha^p) \subseteq F(\alpha)$ always, so the statements $\alpha \in F(\alpha^p)$ and $F(\alpha^p) = F(\alpha)$ are equivalent to each other.

Suppose $\alpha$ is separable over $F$. In particular it is algebraic over $F$. Let $f = f_{\alpha/F(\alpha^p)}$. Since $(X - \alpha)^p = X^p - \alpha^p \in F(\alpha^p)[X]$, we must have that $f$ divides it, so $f = (X - \alpha)^k$ for some $k$. Since $\alpha$ is separable over $F$, we have $k = 1$, i.e., $f = X - \alpha$, so $\alpha \in F(\alpha^p)$.

Now suppose that $\alpha$ is not separable over $F$. If $\alpha$ is transcendental over $F$, then $F(\alpha)$ is isomorphic to a field of rational functions over $F$, and I proved that $\alpha \notin F(\alpha^p)$. So suppose $\alpha$ is algebraic over $F$.

Let $g = f_{\alpha/F} \in \text{Irred}(F)$. Then $D(g) = 0$ since $\alpha$ is not separable, so $g(X) = h(X^p)$ for some $h \in K[X]$. Then $\alpha^p$ is root of $h$, so $f_{\alpha^p/F}$ divides $h$. We get

$$[F(\alpha^p) : F] = \deg(f_{\alpha^p/F}) \leq \deg(h) = \deg(g)/p < \deg(g) = [F(\alpha) : F],$$

so $F(\alpha^p) \neq F(\alpha)$.

It is most convenient to be in a situation when every irreducible polynomial is separable. A field $F$ is perfect if every $f \in \text{Irred}F$ is separable.

Proposition. $F$ is perfect iff every finite extension $K : F$ is a separable extension.

Proof. Suppose $F$ is perfect, and let $K : F$ be a finite extension. For every $\alpha \in K$, $f_{\alpha/F}$ is irreducible, so separable, so $\alpha$ is a separable element. So $K : F$ is a separable extension.

Conversely, suppose every finite extension $K : F$ is separable. Let $f \in \text{Irred}F$, and form an extension $K = F(\alpha)$ with $f_{\alpha/F} = f$. Then $\alpha$ is a separable element, so $f$ is a separable polynomial.

Corollary. A field $F$ is perfect iff either (i) it is characteristic 0, or (ii) it is characteristic $p > 0$ and $F^p = F$ (i.e., every element of $F$ is a $p$th power of an element of $F$).

Proof. We have already proved case (i): every irreducible polynomial in characteristic 0 is separable, so every field of characteristic 0 is perfect.

Case (ii), $\implies$. Let $a \in F$, and consider $f = X^p - a \in F[X]$. We showed earlier that either (1) $f = (X - b)^p$ for some $b \in F$ or (2) $f$ is irreducible over $F$. Since $f$ is clearly not separable, case (2) is impossible if $F$ is perfect, and thus $a = b^p \in F^p$.  

\[\text{F 8 Nov}\]

perfect field
Case (ii), $\iff$. Suppose $F = F^p$. Given a finite extension $K : F$, consider the Frobenius maps:

$$
\begin{array}{c}
K \\
\phi_K \downarrow \\
F \\
\sim \\
\phi_F \\
F
\end{array}
$$

This describes a map $K : F \to K : F$ of field extensions. Since $\phi_F$ is an isomorphism, $\phi_F(F) = F$, so we have

$$[K : F] = [\phi(K) : \phi(F)] = [\phi(K) : F].$$

Then the Tower Law applied to $F \subseteq \phi(K) \subseteq K$ implies $[K : \phi(K)] = 1$.

Apply this to a simple extension $K = F(\alpha)$. We have that $\phi(K) = \phi(F)(\alpha^p) = F(\alpha^p)$ in general, and so $F(\alpha^p) = K = F(\alpha)$, so $\alpha$ is separable over $F$.

For every finite field $K$, the Frobenius $\phi : K \to K$ must be an isomorphism, so finite fields are perfect. On the other hand, $F_p(t)$ is not perfect.

We need to prove the following: if $f \in F[X]$ is a separable polynomial, then its splitting field $\Sigma : F$ is a separable extension, and thus a finite Galois extension. In particular, in finite characteristic the Galois correspondence applies exactly to splitting fields of separable polynomials.

\begin{proposition}
Let $L : F$ be a field extension, and let $L' \subseteq L$ be the subset of elements which are separable over $F$. Then $L'$ is a subfield of $F$.
\end{proposition}

\begin{proof}
In characteristic 0, separable elements are the same as algebraic elements, and we have proved this. So suppose characteristic is $p > 0$.

Let $\alpha, \beta \in L'$. We want to show $\alpha + \beta, \alpha \beta, -\alpha, \alpha^{-1} \in L'$.

Since $\alpha$ is separable over $F$, $\alpha \in F(\alpha^p)$, from which it is easy to see that $-\alpha \in F((-\alpha)^p) = F(\alpha^p)$ and $\alpha^{-1} \in F(\alpha^{-p}) = F(\alpha^p)$, whence $-\alpha$ and $\alpha^{-1}$ are separable.

Next we show $\alpha + \beta$ is separable over $F$. We have a diagram of extensions

$$
\begin{array}{c}
F(\alpha, \beta) \\
\uparrow n \\
F(\alpha + \beta) \\
\downarrow k \\
F(\alpha^p + \beta^p)
\end{array}
$$

Because $\alpha$ and $\beta$ are separable over $F$, $F(\alpha, \beta) = F(\alpha^p, \beta^p)$. By the Tower Law, $n' = nk$, so to show $k = 1$ it suffices to show $n' \leq n$.

Let $f = f_{\beta/F(\alpha + \beta)} \in F(\alpha + \beta)[X]$. Apply the Frobenius $\phi : F(\alpha + \beta) \to F(\alpha + \beta)$ to get $f' := \phi(f) \in F(\alpha^p + \beta^p)[X]$, and therefore $f'(\beta^p) = \phi(f(\beta)) = 0$. Thus the minimal polynomial $g = f_{\beta/F(\alpha^p + \beta^p)}$ divides $f'$, so $\deg g \leq \deg f' = \deg f$, i.e., $n' \leq n$ as desired.

The proof that $\alpha \beta$ is separable over $F$ is almost the same: WLOG we can assume both $\alpha$ and $\beta$ are non-zero, and then carry out the same argument using $F(\alpha, \beta) = F(\alpha \beta, \beta)$, which is $F(\alpha^p, \beta^p) = F(\alpha^p \beta^p, \beta^p)$.

\end{proof}

\begin{corollary}
Suppose $L = F(\alpha_1, \ldots, \alpha_n)$ such that each $\alpha_k$ is separable over $F$. Then $L : F$ is a separable extension.

In particular, if $f \in F[X]$ is a separable polynomial, then $L = \Sigma_f/F : F$ separable extension.
\end{corollary}

\begin{corollary}
An extension $L : F$ is a finite Galois extension if and only if $L$ is the splitting field of a separable polynomial $f \in F[X]$.
\end{corollary}
53. Finite fields

A field $F$ of characteristic $0$ must be infinite, since $\mathbb{Q} \subseteq F$. So finite field must have characteristic $p > 0$. (The converse isn’t true, e.g., $\mathbb{F}_p(t)$.)

If $K$ is finite and characteristic $p > 0$, then $[K : \mathbb{F}_p] < \infty$. So $[K : \mathbb{F}_p] = n$ whence $|K| = p^n$. In particular, the size of $K$ determines its characteristic.

Construction of field with $p^n$ elements. Let $f = X^{p^n} - X \in \mathbb{F}_p[X]$ for some $n \geq 1$. This is a separable polynomial, since $Df = -1 \neq 0$ is a unit so relatively prime to $f$.

Form $K = \Sigma_f/\mathbb{F}_p$, the splitting field of $f$. Let

$$R := \{ \alpha \in K \mid f(\alpha) = 0 \} = \{ \alpha \in K \mid \alpha^{p^n} = \alpha \} \subseteq K,$$

the set of roots of $f$ in $K$. Since $f$ is separable, $|R| = p^n$. Since $f = X(X^{p^n-1} - 1)$, the elements of $R$ are either 0, or $(p^n - 1)$st roots of unity.

Recall the Frobenius homomorphism $\phi : \mathbb{F}_p \to K$. This is injective, and since $K$ is finite it must be an isomorphism: $\phi \in \text{Aut}(K) = \text{Aut}(\mathbb{F}_p)$. Consider its $n$-fold iterate $\phi^n$. Since $\phi^n(x) = x^{p^n}$, we see that $R = \{ a \in K \mid \phi^n(a) = a \} = K^{\langle \phi^n \rangle}$, the fixed set of the subgroup of $\langle \phi^n \rangle \leq \text{Aut}(K : \mathbb{F}_p)$.

Since $R$ is the fixed set of a subgroup it is actually a subfield of $K$. Since $R$ consists of the roots of $f$ it is generated by the roots of $f$, so it is a splitting field of $f$. Thus $R = K$.

Thus, we have constructed a field $K$ of order $p^n$ as the splitting field of $f = X^{p^n} - X$ over $\mathbb{F}_p$, whose elements are exactly all the roots of $f$. This field is conventionally denoted $\mathbb{F}_{p^n}$ (by most pure mathematicians, especially number theorists), or $GF(p^n)$ (for “Galois field”, typically by people using finite fields in applications such as cryptography).

Every finite field is isomorphic to one of these.

**Proposition.** If $K$ is a finite field with $p^n$ elements, then $K$ is isomorphic to $\mathbb{F}_{p^n}$.

**Proof.** Clearly $K$ must have characteristic $p$, and $[K : \mathbb{F}_p] = n$.

Let $\phi$ be the Frobenius of $K$. Since $K$ is finite, $\phi$ must be an isomorphism, so $\phi \in \text{Aut}(K : \mathbb{F}_p)$. Since $|K : \mathbb{F}_p| = n$, we must have $\phi^n = \text{id}$, so for every $a \in K$ we have $a^{p^n} = \phi^n(a) = a$. Thus every element of $K$ is a root of $f = X^{p^n} - X \in \mathbb{F}_p[X]$. Since there are exactly $p^n = \deg f$ elements in $K$ it is clear that $K : \mathbb{F}_p$ is a splitting field of $f$, so $K \approx \mathbb{F}_{p^n}$ by uniqueness of splitting fields up to isomorphism.

**Proposition.** $\text{Aut}(\mathbb{F}_{p^n} : \mathbb{F}_p)$ is a cyclic group of order $n$, generated by the Frobenius. The intermediate fields correspond exactly to positive integers $k \mid n$, and so are isomorphic to $\mathbb{F}_{p^k}$ for $k \mid n$.

**Proof.** The group $G = \text{Aut}(\mathbb{F}_{p^n} : \mathbb{F}_p)$ must have order $|G| \leq [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, so order($\phi$) $= k \leq n$. But since $\phi^k = \text{id}$, this means that every element $a \in \mathbb{F}_{p^n}$ satisfies $\phi^k(a) = a$, i.e., $a^{p^k} = a$, so is a root of $X^{p^k} - X$. Since this polynomial can have at most $p^k$ roots but $|\mathbb{F}_{p^n}| = p^n$, we must have $k = n$.

Subgroups of $\text{Aut}(\mathbb{F}_{p^n} : \mathbb{F}_p) = \langle \phi \rangle$ are $\langle \phi^k \rangle$ with $k \mid n$, and we have

$$\langle \mathbb{F}_{p^n} \rangle^{\langle \phi^k \rangle} \approx \mathbb{F}_{p^k},$$

since elements in the fixed field are exactly roots of $X^{p^k} - X = 0$.

In particular, if $k \mid n$ then there is a unique subfield of $\mathbb{F}_{p^n}$ which is isomorphic to $\mathbb{F}_{p^k}$, and $\text{Aut}(\mathbb{F}_{p^n} : \mathbb{F}_{p^k}) = \langle \phi^k \rangle \approx \mathbb{Z}/p^{n-k}$.

**Warning.** Do not confuse $\mathbb{F}_{p^n}$ with $\mathbb{Z}/p^n$. The first is always field. The second is a commutative ring, but is not a field unless $n = 1$. 
54. More on roots of unity

The above shows that the non-zero elements of finite fields are always roots of unity. It turns out that \( \mathbb{F}_p^n \) is always a cyclic group of order \( p^n - 1 \).

**Theorem.** Let \( F \) be a field. Any finite subgroup \( G \leq F^\times \) of its group of units is cyclic.

**Proof.** For any \( n \geq 1 \), the polynomial equation \( X^n - 1 = 0 \) can have at most \( n \) distinct roots in \( F \). Therefore each set \( \{ g \in G \mid g^n = 1 \} \) has size \( \leq n \) for any \( n \geq 1 \). The claim follows from the following proposition.

**Proposition.** Let \( G \) be a finite abelian group. If for every prime \( p \) the set \( \{ x \in G \mid x^p = 1 \} \) has no more than \( p \) elements, then \( G \) is cyclic.

**Example.** Here is a special case which illustrates the proof of the proposition.

Suppose \( p \) is a prime number and \( G \) an abelian group such that \( |G| = p^2 \) and \( |K| \leq p \) where \( K = \{ x \in G \mid x^p = 1 \} \). The order of elements of \( G \) must divide \( p^2 \), and \( K \) consists of exactly the elements with order 1 and \( p \). Since \( G \neq K \), any \( b \in G \setminus K \) has order \( p^2 \) and so is a cyclic generator of \( G \).

**Proof.** We work by induction on \( n = |G| \), where the case of \( n = 1 \) is trivial. Note that every subgroup of \( G \) also satisfies the hypothesis of the proposition, so the inductive hypothesis implies that every proper subgroup of \( G \) is cyclic.

If \( n > 1 \) then there exists an element \( g \in G \) with order \( m > 1 \). Choosing a prime \( p \) dividing \( m \), we see that \( \text{order}(g^{m/p}) = p \). Therefore the set \( K = \{ x \in G \mid x^p = 1 \} \) where \( c = g^{m/p} \) has exactly \( p \) elements by the hypothesis on \( G \), and so is a cyclic generator \( K = \langle c \rangle \).

The function \( \phi : G \to G \) defined by \( \phi(x) = x^p \) is a homomorphism since \( G \) is abelian, and its kernel is \( K \). We write \( G^p = \{ x^p \mid x \in G \} \) for the image of \( \phi \), which is also a subgroup of \( G \). By the homomorphism theorem \( G^p \cong G/K \) so \( |G^p| = n/p \). The hypothesis on \( G \) necessarily also applies to any subgroup such as \( G^p \), so by induction we have that \( G^p \) is cyclic. Choose a generator \( a \) of \( G^p \), so \( G^p = \langle a \rangle \).

To prove that \( G \) is cyclic it suffices to produce:

\[ b \in G \setminus G^p \quad \text{such that} \quad b^p = a. \]

For then \( \langle b \rangle \supseteq G^p \), whence \( \langle b \rangle = G \) since \( G^p \) has prime index in \( G \).

The homomorphism \( \phi \) defines a surjective homomorphism \( G \to G^p \) to its image which is “\( p \)-to-1”, i.e., for every \( g \in G^p \) the preimage set

\[ \phi^{-1}(g) = \{ y \in G \mid y^p = g \} \]

has size \( p \). In particular, \( \phi^{-1}(a) = \{ y \in G \mid y^p = a \} \) has size \( p \); we want an element \( b \in \phi^{-1}(a) \) which is not in \( G^p \). There are two cases to consider, depending on the image of the subgroup \( G^p \) under the \( p \)th power map \( \phi \).

1. If \( \phi(G^p) = G^p \), then the restriction \( \phi|G^p \) of \( \phi \) to \( G^p \) gives a bijective homomorphism \( G^p \to G^p \). Thus \( \phi^{-1}(a) \) contains exactly one element from \( G^p \), and hence exactly \( p - 1 > 0 \) elements not from \( G^p \). We can take any of these \( p - 1 \) elements to be \( b \).

(2) If \( \phi(G^p) \neq G^p \), then \( \phi(G^p) \) is a proper subgroup of \( G^p \), and so does not contain its generator \( a \). Therefore \( \phi^{-1}(a) \) consists of exactly \( p \) elements not from \( G^p \). We can take any of these \( p \) elements to be \( b \).

**Corollary.** For any finite field \( F \) the group \( F^\times \) of units in \( F \) is cyclic. In particular, for any prime \( p \) the group \( \mathbb{F}_p^\times = (\mathbb{Z}/p)^\times \) is a cyclic group of order \( p - 1 \).
It is not otherwise obvious that \((\mathbb{Z}/p)^{\times}\) is cyclic. Nor is it obvious how to find a cyclic generator of it other than by trial and error.

This has a consequence for finite fields.

**Corollary.** Every extension \(K : F\) with \(K\) finite is a simple extension.

Thus, there exists an irreducible polynomial \(g \in \text{Irred}(F_p)\) of degree \(n\) such that \(F_p^n \approx F_p[X]/(g)\). In fact, there are many such. All of them divide \(X^{p^n} - X\).

**Example.** Over \(F_2\) we can factor \(X^4 - X = X(X - 1)(X^2 + X + 1)\). Thus \(F_4 \approx F_2[X]/(X^2 + X + 1)\). Note that this is basically the same as the factorization of \(X^4 - X\) over \(\mathbb{Q}[X]\), which is actually a product of elements of \(\mathbb{Z}[X]\), and so which can be reduced modulo 2.

Over \(F_3\) we can factor
\[
X^9 - X = X(X + 1)(X + 2)(X^2 + 1)(X^2 + X + 2)(X^2 + 2X + 2).
\]
The last three factors have no root in \(F_3\), so must be irreducible over it, so each gives a polynomial describing \(F_3\).

Let \(a \in F_9\) be a root of \(X^2 + 2X + 2\), so \(a^2 = a + 1\). We can compute all the powers of \(a\) in the basis \(\{1, a\}\), as well as their the minimal polynomials over \(F_3\):

<table>
<thead>
<tr>
<th>(k)</th>
<th>(a^k)</th>
<th>(f_{a^k/F_3})</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>(X + 2)</td>
</tr>
<tr>
<td>1</td>
<td>(a)</td>
<td>(X^2 + 2X + 2)</td>
</tr>
<tr>
<td>2</td>
<td>(a + 1)</td>
<td>(X^2 + 1)</td>
</tr>
<tr>
<td>3</td>
<td>(2a + 1)</td>
<td>(X^2 + 2X + 2)</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>(X + 1)</td>
</tr>
<tr>
<td>5</td>
<td>2(a)</td>
<td>(X^2 + X + 2)</td>
</tr>
<tr>
<td>6</td>
<td>2(a + 2)</td>
<td>(X^2 + 1)</td>
</tr>
<tr>
<td>7</td>
<td>(a + 2)</td>
<td>(X^2 + X + 2)</td>
</tr>
</tbody>
</table>

So \(\text{order}(a) = 8\), and \(F_9^8 = \langle a \rangle\). Is there a pattern here? Note that \(a^k\) and \(a^{3k}\) always share the same minimal polynomial, which is not surprising since \(\phi(x) = x^3\) is an automorphism fixing \(F_3\).

Note also that over \(\mathbb{Q}\) we have an irreducible factorization
\[
X^9 - X = X(X + 1)(X - 1)(X^2 + 1)(X^4 + 1).
\]
Here \(X^2 + 1\) is the minimal polynomial for primitive 4th roots of unity, while \(X^4 + 1\) is the minimal polynomial for primitive 8th roots of unity. These factors are in \(\mathbb{Z}[X]\), and we can reduce them modulo 3 to get an identity in \(F_3[X]\). There the last factor reduces further into a product of quadratics.

This is a general observation: any \(f \in \text{Irred}(F_p)\) of degree \(n\) has as roots \(a, a^p, a^{p^2}, \ldots, a^{p^{n-1}}\) for some \(a \in F_{p^n}\), all of which are distinct.

55. **Cyclotomic polynomials**

I’ll return to characteristic zero. I want to understand the extension \(\mathbb{Q}(\zeta_n) : \mathbb{Q}\), which is a Galois extension since it is a splitting field of \(X^n - 1\). To do so we need to understand the minimal polynomials of roots of unity over \(\mathbb{Q}\).

Let \(\epsilon\) be any primitive \(n\)th root of unity in \(\mathbb{C}\), and consider its minimal polynomial \(f_\epsilon := f_\epsilon/\mathbb{Q}\) over the rationals. Because \(f_\epsilon\) divides \(X^n - 1\) which is monic with integer coefficients, Gauss’s lemma implies that \(f_\epsilon \in \mathbb{Z}[X]\). We will show that every primitive \(n\)th root of unity is a root of \(f_\epsilon\). That is, all primitive \(n\)th roots of unity share the same minimal polynomial over \(\mathbb{Q}\).

This uses the following lemma, the idea for which comes from observation made earlier: if \(\epsilon\) is a root of unity in a field of characteristic \(p > 0\), then \(\epsilon\) and \(\epsilon^p\) must have the same minimal polynomial over \(F_p\).
Lemma. Let $\epsilon \in \mathbb{C}$ be an $n$th root of unity, and let $p$ be a prime not dividing $n$. Then $f_{\epsilon/\mathbb{Q}}(\epsilon^p) = 0$.

Proof. Let $f = f_{\epsilon/\mathbb{Q}}$ and $g = f_{\epsilon^p/\mathbb{Q}}$, which are both in $\mathbb{Z}[X]$. They are both divisors of $X^n - 1$ in $\mathbb{Z}[X]$, and hence in $\mathbb{Q}[X]$. Since $X^n - 1$ is separable and $f, g$ are monic irreducible factors, we must have either (1) $f = g$, or (2) $f \neq g$, so $X^n - 1 = fgh$ for some $h \in \mathbb{Z}[X]$. We want to show (1) (which proves the claim). So I will assume (2) and derive a contradiction.

Let $G := g(X^p) \in \mathbb{Z}[X]$. Then $G(\epsilon) = g(\epsilon^p) = 0$, so $f | G$, so $G = fk$ for some $k \in \mathbb{Z}[X]$, since $G$ is also monic polynomial with integer coefficients.

Now we can reduce everything modulo $p$, by taking images under the homomorphism $\pi: \mathbb{Z}[X] \to \mathbb{F}_p[X]$ which sends integer coefficients to integers modulo $p$. Write $\overline{f}, \overline{g}, \overline{h}, k, \overline{G}$ for the images of $f, g, h, k, G$ under $\pi$. Note that since $f, g$ are monic of positive degree, $\overline{f}, \overline{g}$ are also monic of positive degree (but they might not be irreducible over $\mathbb{F}_p$). We have

$$\overline{g}^p = \overline{G} = \overline{f} \overline{k}, \quad X^n - X = \overline{f} \overline{g} \overline{h}.$$

The first identity implies that $\overline{f}, \overline{g}$ must have some irreducible factor $m \in \text{Irred}(\mathbb{F}_p)$ in common, since neither is a unit. The second identity then implies that $m^2 | X^n - 1$. But $X^n - 1 \in \mathbb{F}_p[X]$ is separable, since $D(X^n - 1) = nX^{n-1}$ and $p \nmid n$. So we have a contradiction. □

Proposition. Let $\zeta \in \mathbb{C}$ be a primitive $n$th root of unity. Then every primitive $n$th root of unity is a root of $f = f_{\zeta/\mathbb{Q}}$.

Proof. Every primitive $n$th root of unity can be written as $\zeta^k$ with $\gcd(k, n) = 1$ and $k \geq 1$. Factor $k = p_1 \cdots p_r$ into primes, where no $p_i$ divides $n$. Then using the lemma and induction we have that $\zeta^{p_1}, \zeta^{p_1p_2}, \zeta^{p_1p_2p_3}, \ldots$ are all roots of $f$, whence $f(\zeta^k) = 0$. □

We write $\Phi_n := f \in \mathbb{Z}[X]$ for the minimal polynomial of one primitive $n$th root of unity, and hence of all primitive $n$th roots of unity. Note that

$$X^n - 1 = \prod_{d | n} \Phi_d,$$

so that we can compute the $\Phi_n$ by induction on $n$, using polynomial long division.

The degree of $\Phi_n$ is the Euler $\phi$-function

$$\phi(n) := |(\mathbb{Z}/n)^\times| = \text{number of } d \in \{1, 2, \ldots, n\} \text{ such that } \gcd(d, n) = 1.$$

$$\Phi_1 = X - 1, \quad \Phi_2 = X + 1, \quad \Phi_3 = X^2 + X + 1, \quad \Phi_4 = X^2 + 1, \quad \Phi_5 = X^4 + X^3 + X^2 + X + 1, \quad \Phi_6 = X^2 - X + 1, \quad \Phi_7 = X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X + 1, \quad \Phi_8 = X^4 + 1,$$

$$\Phi_9 = X^6 + X^3 + 1, \quad \Phi_{10} = X^5 - X^4 + X^3 - X^2 + X - 1, \quad \Phi_{11} = X^{11} + X^{10} + X^9 + \cdots + X^2 + X + 1, \quad \Phi_{12} = X^4 - X^2 + 1, \quad \Phi_{13} = X^{13} + X^{12} + X^{11} + \cdots + X^2 + X + 1, \quad \Phi_{14} = X^7 - X^6 + X^5 - X^4 + X^3 - X^2 + X - 1, \quad \Phi_{15} = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1, \quad \Phi_{16} = X^8 + 1.$$

Exercise. Show that:

1. if $m$ is odd and $m > 1$, then $\Phi_{2m} = \Phi_m(-X)$, and
2. if $p | m$ where $p$ is prime, then $\Phi_{pm} = \Phi(X^p)$.

Use this to show that you can reduce the problem of computing cyclotomic polynomials to the case when $n$ is a product of distinct odd primes.
Remark. It’s not true that every coefficient in $\Phi_n$ must be in $\{-1, 0, 1\}$. The first counterexample is:

$$
\Phi_{105} = X^{48} + X^{47} + X^{46} - X^{43} - X^{42} - 2X^{41} - X^{40} - X^{39} + X^{36} + X^{35} + X^{34}
+ X^{33} + X^{32} + X^{31} - X^{28} - X^{26} - X^{24} - X^{22} - X^{20} + X^{17} + X^{16} + X^{15}
+ X^{14} + X^{13} - X^{12} - X^9 - X^8 - 2X^7 - X^6 - X^5 + X^2 + X + 1.
$$

We can now calculate the Galois group of every cyclotomic extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.

**Theorem.** There is an isomorphism of groups

$$
\text{Aut}(\mathbb{Q}(\zeta_n) : \mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n)^\times,
$$

which sends an automorphism $\sigma$ to the unique congruence class $k$ modulo $n$ such that

$$
\sigma(\epsilon) = \epsilon^k
$$

for every $n$th root of unity $\epsilon$.

**Proof.** We know that any automorphism $\sigma$ of $\mathbb{Q}(\zeta_n)$ permutes the primitive $n$th roots of unity, so $\sigma(\zeta_n) = \zeta_n^k$ for some $k$ relatively prime to $n$ (and $k$ is unique modulo $n$.) Since every root of unity is a power of $\zeta_n$, we see that $\sigma(\epsilon) = \epsilon^k$ for every $n$th root of unity.

We thus get a well-defined function $\text{Aut}(\mathbb{Q}(\zeta_n) : \mathbb{Q}) \rightarrow (\mathbb{Z}/n)^\times$, which is injective and is easily seen to be a homomorphism (since $(\epsilon^a)^b = \epsilon^{ab}$). To show that it is surjective it suffices to note that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = |(\mathbb{Z}/n)^\times|$, a consequence of the fact that $\Phi_n$ is irreducible. \hfill $\Box$

Typically, I write $\sigma_k \in \text{Aut}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ corresponding to $k \in (\mathbb{Z}/n)^\times$, so we have the formula $\sigma_k(\epsilon) = \epsilon^k$ for every $n$th root of unity $\epsilon$.

**Remark.** For a more general subfield $F \subseteq \mathbb{C}$, the above argument only constructs an injective homomorphism $\text{Aut}(F(\zeta_n) : F) \rightarrow (\mathbb{Z}/n)^\times$. We need irreducibility of $\Phi_n$ over $F$ to show that it is an isomorphism.

### 56. The Group $(\mathbb{Z}/n)^\times$

What is the structure of the abelian group $\text{Aut}(\mathbb{Q}(\zeta_n) : \mathbb{Q}) \approx (\mathbb{Z}/n)^\times$? First we compute its order. $|(\mathbb{Z}/n)^\times| = \phi(n)$, where $\phi(n)$ = number of elements of $\{1, \ldots, n\}$ not dividing $n$.

Thus:

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
|-----|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|
| $\phi(n)$ | 1 | 1 | 2 | 2 | 4 | 2 | 6 | 4 | 6 | 4  | 10  | 4  | 12  | 6  | 8  | 8  | 16  |

**Proposition.** We have that

1. $\phi(mn) = \phi(m)\phi(n)$ if $\gcd(m, n) = 1$.
2. $\phi(p^k) = p^k - p^{k-1}$ if $p$ is prime.

**Proof.**

1. (1) amounts to producing a bijection $(\mathbb{Z}/mn)^\times \xrightarrow{\sim} (\mathbb{Z}/m)^\times \times (\mathbb{Z}/n)^\times$. Such a function is given by $[x]_{mn} \mapsto ([x]_m, [x]_n)$, which is a bijection by the “Chinese Remainder Theorem”.

2. (2) is straightforward: the set of “non-divisors” of $p^k$ is

$$
\{1, 2, 3, \ldots, p^k - 2, p^k - 1, p^k\} \setminus \{p, 2p, 3p, \ldots, (p^{k-1} - 2)p, (p^{k-1} - 1)p, p^k\}.
$$

The first identity comes from an isomorphism groups.

**Proposition.** If $\gcd(m, n) = 1$, then $(\mathbb{Z}/mn)^\times \approx (\mathbb{Z}/m)^\times \times (\mathbb{Z}/n)^\times$.

**Proof.** The bijection of the CRT is a homomorphism of groups. \hfill $\Box$

It remains to describe the structure of $(\mathbb{Z}/p^k)^\times$.
Proposition. We have that

1. \((\mathbb{Z}/p^k)\) \(\cong \mathbb{Z}/(p-1) \times \mathbb{Z}/p^{k-1}\) if \(k \geq 1\) and \(p\) an odd prime.

   In fact, \((\mathbb{Z}/p^k) \cong \langle [a^{p^{k-1}}] \rangle \times \langle [1 + p] \rangle\), where \(a\) represents any generator of \((\mathbb{Z}/p)\).

2. \((\mathbb{Z}/2^k)\) \(\cong \mathbb{Z}/2 \times \mathbb{Z}/2^{k-2}\) if \(k \geq 2\).

   In fact, \((\mathbb{Z}/2^k) \cong \langle [-1] \rangle \times \langle [5] \rangle\).

Example.

\((\mathbb{Z}/5^2)\) \(\cong \langle [2] \rangle \approx \mathbb{Z}/4\).

\((\mathbb{Z}/5^3)\) \(\cong \langle [7] \rangle \times \langle [6] \rangle \approx \mathbb{Z}/4 \times \mathbb{Z}/5\).

\((\mathbb{Z}/5^4)\) \(\cong \langle [57] \rangle \times \langle [6] \rangle \approx \mathbb{Z}/4 \times \mathbb{Z}/25\).

In general,

\((\mathbb{Z}/5^k)\) \(\cong \langle [2^{5^{k-1}}] \rangle \times \langle [1 + p] \rangle \approx \mathbb{Z}/(p-1) \times \mathbb{Z}/5^{p^{k-1}}\),

where we use powers of 2 because it represents a generator of \((\mathbb{Z}/5)\).

I'll do the odd prime case first.

Proof for \(p\) odd. Let \(k \geq 1\). I define the following two subgroups of \(G = (\mathbb{Z}/p^k)^\times\):

\[ A := \{ [a^{p^{k-1}}] \mid a \in \mathbb{Z}, p \nmid a \}\]

and

\[ B := \{ [1 + pm] \mid m \in \mathbb{Z} \}\]

I will show

1. \(A \approx (\mathbb{Z}/p)^\times\), so \(A\) is cyclic of order \(p-1\), with generator \([a^{p^{k-1}}]\) for any \(c\) representing a generator of \((\mathbb{Z}/p)^\times\).

2. \(B\) is cyclic of order \(p^{k-1}\), with generator \([1 + p]\).

3. \(A \cap B = \{ [1] \}\).

4. \(AB = G\).

Since \(G\) is abelian, the function \(A \times B \rightarrow G\) sending \((a, b) \mapsto ab\) is a homomorphism, so (3) and (4) imply that this map gives an isomorphism \(G \approx A \times B\). Combined with (1) and (2) this gives the claim.

To do this, I also need the following fact.

Claim. Let \(x, y \in \mathbb{Z}\) and \(r \geq 1\). Then

\[ x \equiv y \mod p^r, \]

implies

\[ x^p \equiv y^p \mod p^{r+1}. \]

Proof of Claim: The first congruence means we can write \(y = x + mp^r\) for some \(m \in \mathbb{Z}\), and the binomial formula gives

\[ y^p = (x + mp^r)^p = x^p + \binom{p}{1} x^{p-1} mp^r + \binom{p}{2} x^{p-2} m^2 p^{2r} + \cdots + \binom{p}{p-1} x m^{p-1} p^{(p-1)r} + m^p p^r. \]

Since \(p \mid \binom{p}{j}\) when \(0 < j < p\), and \(p^{r+1} \mid p^r\) since \(r \geq 1\) and \(p \geq 2\), we see that \(x^p \equiv y^p \mod p^{r+1}\).

Proof of (1). There is a homomorphism

\[ \pi: (\mathbb{Z}/p^k)^\times \rightarrow (\mathbb{Z}/p)\,^\times, \quad [a]_{p^k} \mapsto [a]_p. \]

I claim that the restriction of \(\pi\) to \(A \subseteq (\mathbb{Z}/p^k)^\times\) gives an isomorphism \(A \cong (\mathbb{Z}/p)^\times\). Fermat’s little theorem says \(a^p \equiv a \mod p\), so iterating it says \(a^{p^{k-1}} \equiv a \mod p\) when \(k \geq 1\). Thus \(A \to (\mathbb{Z}/p)^\times\) is surjective.
To see it’s injective, suppose \(a, b\) are such that \(a^{p^{k-1}} \equiv b^{p^{k-1}} \mod p\). By Fermat’s little theorem, this implies \(a \equiv b \mod p\). Using the Claim above, we get that \(a^p \equiv b^p \mod p^2\), \(a^{p^2} \equiv b^{p^2} \mod p^3\), \ldots, and so by induction that \(a^{p^{k-1}} \equiv b^{p^{k-1}} \mod p^k\), i.e., \([a^{p^{k-1}}]_{p^k} = [b^{p^{k-1}}]_{p^k}\).

In particular, if \(c\) represents a generator of \((\mathbb{Z}/p^k)^\times\), then \(\pi\) sends \([c^{p^{k-1}}] \in A\) to \([c] \in (\mathbb{Z}/p)^\times\), so \(A = ([c^{p^{k-1}}])\).

Proof of (2). It is easy to see that \(|B| = p^{k-1}\). If \(k = 1\) there is nothing to prove, so suppose \(k \geq 2\). Let \(a = 1 + p\). I’ll show that \([a]\) has order \(p^{k-1}\) in \((\mathbb{Z}/p^k)^\times\), which will show that \(B\) is a cyclic group.

It is clear that the order of \([a]\) in \(B\) divides \(p^{k-1}\). I will prove that
\[
a^{pr} = (1 + p)^{pr} \equiv 1 + p^{r+1} \mod p^{r+2}, \quad \text{for all } r \geq 0
\]
by induction on \(r\), where the \(r = 0\) case is obvious. If for some \(r \geq 1\) we know that \(a^{p^{r-1}} \equiv 1 + p^r \mod p^{r+1}\), then the Claim above implies
\[
a^{pr} \equiv (1 + p^r)^p \mod p^{r+2}.
\]
The binomial formula then gives
\[
(1 + p^r)^p = \sum_{j=0}^{p} \binom{p}{j} p^j p^r = 1 + \binom{p}{1} p^r + \binom{p}{2} p^{2r} + \cdots + p^{pr} \equiv 1 + \binom{p}{1} p^r \equiv 1 + p^r \mod p^{r+2}.
\]
This is because:
- when \(2 \leq j < p\) we have \(p | \binom{p}{j}\), and since \(r \geq 1\) we have \(r + 2 \leq 1 + jr\) so \(p^{r+2} | (\binom{p}{j}) p^j r^j\), while
- when \(j = p\) we have \(r + 2 \leq pr\) since \(p \geq 3\) and \(r \geq 1\).

This shows in particular that \(\langle a \rangle \cap [1 + p^{k-1}]_{p^k} = [1]_{p^k}\) but \([a^{p^{k-2}}]_{p^k} = [1 + p^{k-1}]_{p^k} \neq [1]_{p^k}\) in \((\mathbb{Z}/p^k)^\times\), so \([a]\) has order \(p^{k-1}\).

Proof of (3). Note that \(B\) is the kernel of \(\pi : G \to (\mathbb{Z}/p)^\times\), and recall that \(\pi\) restricts to a bijection \(A \to (\mathbb{Z}/p)^\times\). Thus only one element of \(B = \ker \pi\) is contained in \(A\), so \(A \cap B = \{1\}\).

Proof of (4). Suppose \([x] \in G\). Set \(a = x^{p^{k-1}}\), so \([a] \in A\). Then \(x \equiv y \mod p\), so \([b] := [x][a]^{-1} \in \ker \pi = B\). Then \([x] = [a][b]\) with \([a] \in A\) and \([b] \in B\) as desired.

\[\square\]

Proof for \(p = 2\). Let \(k \geq 2\). I define the following subgroups of \(G = (\mathbb{Z}/2^k)^\times\):
\[
A := \{[1], [-1]\},
\]
and
\[
B := \{[1 + 4m] \mid m \in \mathbb{Z}\}.
\]

Now
1. \(A \cong \mathbb{Z}/2\) clearly.
2. \(B\) is cyclic of order \(2^{k-2}\). This is proved just as for odd primes, by showing that \([5] = [1 + 4]\) has order \(2^{k-2}\) in \(B\). To do this it suffices to show that
\[
5^{2r} = (1 + 2^2)^{2r} \equiv 1 + 2^{r+2} \mod 2^{r+3}, \quad \text{for all } r \geq 1,
\]
which can be proved by induction on \(r\), with the case \(r = 0\) obvious. If for some \(r \geq 1\) we know \(5^{2r-1} \equiv 1 + 2^{r+1} \mod 2^{r+2}\), then the Claim implies
\[
5^{2r} \equiv (1 + 2^{r+1})^2 \equiv 1 + 2^{r+1} + 2^{2r+2} \equiv 1 + 2^{r+2} \mod 2^{r+3},
\]
since \(r \geq 1\) implies \(2r + 2 \geq r + 3\).
3. and (4) Proof just like for odd primes.

\[\text{\footnote{This is the exact place in the proof where we need } p \text{ to be an odd prime.}\]
57. Constructible regular polygons

Recall that a number $\alpha \in \mathbb{C}$ is constructible (by ruler and compass) if there exists a finite sequence of extensions such that

$$\mathbb{Q} = L_0 \subset L_1 \subset \cdots \subset L_r = L, \quad [L_k : L_{k-1}] = 2, \quad \alpha \in L.$$ Earlier I called such an extension $L : \mathbb{Q}$ a 2-radical extension.

One consequence: if $\alpha$ is constructible, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^d$ for some $d$, since $\mathbb{Q}(\alpha) \subseteq L$ for some $L$ is as above. The converse isn’t true, however.

Remark. Let $L : F$ be a finite extension of subfields of $\mathbb{C}$, and consider the following 3 statements.

1. $L : F$ is a 2-radical Galois extension.
2. $L : F$ is a 2-radical extension.
3. $[L : F]$ is a power of 2.

It is clear that (1) $\implies$ (2) $\implies$ (3). However, neither of the reverse implications are true.

For instance, $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ is 2-radical but not Galois, so (2) does not imply (1).

Here’s how to get an example showing that (3) does not imply (2). Consider $L : F$ where $L$ is the splitting field of some irreducible degree 4 polynomial $f \in \text{Irred}(F)$, and let $\alpha$ be one of the roots of $f$. Then if $G = \text{Aut}(L : F)$, then $F(\alpha) = L^H$ for a subgroup $H \leq G$ of index 4. The extension $F(\alpha) : F$ is 2-radical if and only if there exists $F \subseteq K \subseteq F(\alpha)$ with $[K : F] = 2$, which exists iff $H \leq K \leq G$ with $[G : K] = 2$.

If $G \approx S_4$, this is impossible, since $A_4$ is the only index 2 subgroup of $S_4$, and $A_4$ has no index 2 subgroups. It is also impossible if $G \approx S_4$, again because $A_4$ has no index 2 subgroup.

It turns out that for Galois extensions, these three are equivalent, so for such extensions being 2-radical is determined by the degree of the extension.

Proposition. Let $L : F$ be a finite Galois extension of subfields of $\mathbb{C}$. Then $L : F$ is 2-radical iff $[L : F] = 2^d$ for some $d$.

Proof. $\implies$ is clear.

$\iff$. Suppose $L : F$ is finite Galois and $[L : F] = 2^d$. Let $G = \text{Aut}(L : F)$, so $|G| = 2^d$. We have proved that any non-trivial 2-group contains a normal subgroup of index 2, and therefore (by an induction argument) that any 2-group is solvable. So there exists $G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_d = \{e\}$ such that each $[G_i : G_{i+1}] = 2$, and therefore $L_i = L^{G_i}$ so that each $[L_{i+1} : L_i] = 2$. Thus $L : F$ is 2-radical.

As a consequence, we can now show that any subextension of a 2-radical extension is 2-radical. To prove this, we also need an observation we have made before: if $K_1 : F$ and $K_2 : F$ are 2-radical extensions, then so is the composite extension $K_1 K_2 : F$.

Proposition. If $F \subseteq K \subseteq L \subseteq \mathbb{C}$ and $L : F$ is 2-radical, then $K : F$ is 2-radical.

Proof. First I’ll show that without loss of generality we can assume $L : F$ is a Galois extension, by showing that any 2-radical extension is contained in a 2-radical Galois extension.

Let $L : F$ be 2-radical, and consider its normal closure $N : F$. Then $N$ is generated over $F$ by the collection of all subfields $g(L) : F$ where $g \in G = \text{Aut}(N : F)$. That is, $L$ is the composite field of the collection of fields $\{g(L)\}_{g \in G}$. Each $g(L) : F$ is $F$-isomorphic to $L : F$, and so is 2-radical, and therefore the composite extension $N : F$ is 2-radical.

Now assume $L : F$ is Galois, let $G = \text{Aut}(L : F)$, and let $H = \text{Aut}(L : K)$ so $K = L^H$. To show $K : F$ is 2-radical, it suffices to construct a chain of subgroups $H = G_k < G_{k-1} < \cdots < G_1 < G_0 = G$ with each $[G_i : G_{i+1}] = 2$. Then $F = L^{G_0} \subseteq L^{G_1} \subseteq \cdots \subseteq L^{G_k} = K$ exhibits $K : F$ as a 2-radical extension. This is a consequence of the following extension of the first Sylow theorem. \[\square\]
Proposition. Let $p$ be a prime, $G$ a finite $p$-group, and $H < G$ a proper subgroup. Then there is a subgroup $K$ with $H < K \leq G$ and $[H : K] = p$.

Proof. We argue by induction on $|G| = p^d$, with the case $d = 0$ being trivially true. So suppose $d = 1$, and $H < G$ a proper subgroup. We know that $G$ contains a non-trivial element $c$ of order $p$ in the center, and thus a normal subgroup $Z = \langle c \rangle$ of order $p$. There are two cases.

1. If $Z \not\subseteq H$, then $K := HZ$ is a subgroup of $G$ of order $p|H|$ containing $H$.
2. If $Z \subseteq H$, then $H/Z < G/Z$ is a proper subgroup, so by the induction hypothesis there is a subgroup $\overline{K}$ such that $H/Z < \overline{K} \leq G/Z$ with $[\overline{K} : H/Z] = p$. Let $K = \pi^{-1}\overline{K}$ be the preimage of $K$ under the projection $\pi: G \to G/Z$.

This finally gives a proof of Theorem 7.11 in Stewart, whose proof given there is incorrect.

Corollary. Let $\alpha \in \mathbb{C}$. Then $\alpha$ is constructible iff $\mathbb{Q}(\alpha) : \mathbb{Q}$ is 2-radical.

Proof. By definition, $\alpha$ is constructible iff there exists a finite 2-radical extension $K : \mathbb{Q}$ such that $\alpha \in K$. By what we have just proved, if $K : \mathbb{Q}$ is 2-radical so is the subextension $\mathbb{Q}(\alpha) : \mathbb{Q}$. The converse is obvious.

Constructing a regular $n$-gon by ruler and compass amounts to showing that $\zeta_n = e^{2\pi i/n}$ is constructible. Since it generates a Galois extension over $\mathbb{Q}$, we get the following.

Corollary. $\zeta_n$ is constructible if and only if $\phi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ is a power of 2.

So when is $\phi(n)$ a power of 2? First, write $n = 2^k m$ with $m$ odd. Then

$$\phi(n) = \begin{cases} 
\phi(m) & \text{if } k = 0, 1, \\
2^{k-2}\phi(m) & \text{if } k \geq 2.
\end{cases}$$

So we can reduce to the case of $n$ odd. (Geometrically, this amounts to the fact that you can always bisect an angle by ruler and compass, so if you can construct an $n$-gon then you can construct a $2n$-gon.)

For $n = p^k$ with $p$ an odd prime and $k \geq 1$, we have $\phi(p^k) = p^{k-1}(p-1)$. Thus the regular $p^k$-gon is constructible iff $k = 1$ and $p-1$ is a power of 2.

Corollary. A primitive $n$th root of unity is constructible if and only if

$$n = 2^k p_1 \cdots p_r, \quad r \geq 0, k \geq 0,$$

where the $p_i$ are distinct Fermat primes. (Recall that a Fermat prime is a prime number of the form $2^m + 1$, and that only five are known: 3, 5, 17, 257, 65537.)

58. Inverse Galois problem for $\mathbb{Q}$

Here is a question: Is every finite group $G$ isomorphic to the Galois group of some Galois extension $L : \mathbb{Q}$? This is called the inverse Galois problem, and it is unsolved.

Note: this is not the same as asking for an extension $L : F$ with Galois group $G$. That can always be done as we have shown.

We can prove the inverse Galois problem for cyclic groups.

Proposition. Every finite cyclic group is the Galois group of some Galois extension over $\mathbb{Q}$.

Proof. Given $n \geq 1$, factor it as $n = p_1^{k_1} \cdots p_r^{k_r}$, with $p_1, \ldots, p_r$ distinct primes, with $k_1, \ldots, k_r \geq 1$. Let

$$m = p_1^{k_1'} \cdots p_r^{k_r'},$$

where $k_i' = k_i + 1$ if $p_i$ is odd, and $k_i' = k_i + 2$ if $p_i = 2$. I claim that $G := \text{Aut}(\mathbb{Q}(\zeta_m) : \mathbb{Q}) = (\mathbb{Z}/m)^\times$ contains subgroup $H$ such that $G/H$ is cyclic of order $n$, in which case $L := \mathbb{Q}(\zeta_m)^H$ is such that $L : \mathbb{Q}$ is Galois with $\text{Aut}(L : \mathbb{Q}) \approx G/H \approx \mathbb{Z}/n$. □
Something more is true.

Every finite abelian group isomorphic to a quotient group of the form \((\mathbb{Z}/m)^\times / H\), and thus is isomorphic to the Galois group of some Galois extension over \(\mathbb{Q}\).

This is much harder to prove. For instance, suppose you want to get the product group \((\mathbb{Z}/3)^d\) for some large \(d\). You can get one of the factors as a quotient of \((\mathbb{Z}/9)^\times\). But the other factors must come from cyclotomic extensions involving different primes. For instance, you can get \(\mathbb{Z}/3\) as a quotient of \((\mathbb{Z}/q)^\times\) whenever \(q\) is a prime such that \(q \equiv 1 \mod 3\), since \((\mathbb{Z}/q)^\times \approx \mathbb{Z}/(q-1)\).

It turns out there are infinitely many such primes \((7, 13, 19, 31, 37, 43, 61, \ldots)\), as a consequence of the following.

**Theorem** (Dirichlet’s theorem on arithmetic progressions). Let \(a, n \in \mathbb{Z}\) with \(n > 1\) and \(\gcd(n, a) = 1\). Then there exist infinitely many prime numbers in the congruence class \([a]_n = \{a + nx \mid x \in \mathbb{Z}\} = \{y \in \mathbb{Z} \mid y \equiv a \mod n\}\).

This gives a recipe for producing any finite abelian group as the Galois group of an extension over \(\mathbb{Q}\).

1. The structure theorem for finite abelian groups says that any such is isomorphic to \(G \approx (\mathbb{Z}/n_1)^\times \times \cdots \times (\mathbb{Z}/n_k)^\times\).
2. For each \(n_j \geq 1\), there exist infinitely many primes \(p\) such that \(n_j \mid p - 1\), i.e., such that \(p \in [1]_{n_j}\), by Dirichlet’s theorem. Some \(p\) might work for several of the numbers in the list \(n_1, \ldots, n_k\), but because there are infinitely many, we can choose distinct primes \(p_1, \ldots, p_k\) such that \(p_i - 1 \mid n_i\).
3. There exists a subgroup \(H_i \subseteq (\mathbb{Z}/p_i)^\times \approx \mathbb{Z}/(p_i - 1)\) of index \(n_i\), so \((\mathbb{Z}/p_i)^\times / H_i \approx \mathbb{Z}/n_i\) gives the desired extension.

59. Abelian extensions

An abelian extension is a finite Galois extension \(L : F\) such that \(\text{Aut}(L : F)\) is abelian.

As we have noted, we have a bunch of abelian extensions of \(\mathbb{Q}\) given by the cyclotomic extensions \(\mathbb{Q}(\zeta_n) : \mathbb{Q}\). There is a famous theorem, which classifies abelian extensions of \(\mathbb{Q}\), which I will not prove.

**Theorem** (Kronecker-Weber). Every abelian extension \(L : \mathbb{Q}\) is a subextension of some \(\mathbb{Q}(\zeta_n) : \mathbb{Q}\).

This is a deep theorem, and well beyond what we can prove in this class. However, I will soon prove a very special case: that every quadratic extension of \(\mathbb{Q}\) is contained in a cyclotomic extension.

The cyclotomic extensions of \(\mathbb{Q}\) have two interesting features.

- They are obtained by adjoining elements of finite order from a certain abelian group, namely the group \(\mathbb{C}^\times\) of complex numbers under multiplication.
- They are obtained by adjoining values of the transcendental function \(f(z) := e^{2\pi iz}\) evaluated on some elements of \(\mathbb{Q} \subseteq \mathbb{C}\). (An analytic function is transcendental if it does not satisfy any algebraic equation.)

Question: suppose \(K\) is a field which is a finite extension of \(\mathbb{Q}\). (Such fields are called **number fields**.) Is there a recipe for constructing abelian extensions of \(K\), similar to that for \(\mathbb{Q}\)? This question is called Hilbert’s 12th problem, or “Kronecker’s Jugendtraum” (= “dream of his youth”). It has been completely solved only for a very small number of fields (e.g., for “quadratic imaginary fields” \(\mathbb{Q}(\sqrt{-d})\) where \(d\) is a positive squarefree integer).

For instance, for \(K = \mathbb{Q}(i)\), it works more or less like this:

- There is an abelian group \(E\), whose underlying set is
  \[ E := \{O\} \cup \{(a, b) \in \mathbb{C}^2 \mid b^2 = a^3 + a\}, \]
and whose group law \((a, b) + (a', b') := (f(a, b, a', b'), g(a, b, a', b'))\) is given by a certain pair of rational functions \(f\) and \(g\) which I won’t write down. Then every abelian extension \(L : \mathbb{Q}(i)\) is obtained by adjoining the coordinates \((a, b)\) of elements in some finite subgroup \(G \leq E\).

(The group \(E\) is an example of what is called an elliptic curve.)

- There is a transcendental function \(f\) on the complex numbers which satisfies the differential equation \((f'(z))^2 = f(z)^3 + f(z)\). Every abelian extension \(L : \mathbb{Q}(i)\) is obtained by adjoining to \(\mathbb{Q}(i)\) numbers \(f(z)\) and \(f'(z)\) with \(z \in H\), where \(H \subseteq \mathbb{C}\) is a subgroup defined by \(H = \lambda \mathbb{Q}(i) \subseteq \mathbb{C}\) for a certain value \(\lambda \in \mathbb{C}\).

See [http://web.math.rochester.edu/people/faculty/chaessig/CMpaper.pdf](http://web.math.rochester.edu/people/faculty/chaessig/CMpaper.pdf) for a brief introduction to some of these ideas.

### 60. Quadratic Extensions of \(\mathbb{Q}\) and Roots of Unity

For any field \(F\) of \(\text{char} \neq 2\), we see that any degree 2 extension of \(F\) is isomorphic to \(F(\sqrt{a})\) for some \(a \in F\). In fact, we can classify such extensions completely.

**Proposition.** For \(F\) not of characteristic 2, there is a bijective correspondence

\[
\text{(non-zero elements of } F^\times/(F^\times)^2) \longleftrightarrow \text{(isomorphism classes of degree 2 extensions } L : F),
\]

given by \(a \mapsto L = K(\sqrt{a})\).

**Proof.** We have seen that every degree 2 extension arises this way. Clearly if \(b = ac^2\) for \(a, b, c \in F\) then \(\sqrt{b} = \pm c\sqrt{a}\), so \(F(\sqrt{b}) \cong F(\sqrt{a})\).

Conversely if \(F(\sqrt{a})\) and \(F(\sqrt{b})\) are degree 2 over \(F\) and \(F\)-isomorphic, then there is a squareroot of \(b\) in \(F(\sqrt{a})\). That is, there are \(u, v \in F\) such that

\[
\sqrt{b} = u + v\sqrt{a}, \quad \implies \quad b = (u + v\sqrt{a})^2 = (u^2 + v^2a) + 2uv\sqrt{a}.
\]

Since \([F(\sqrt{a}) : F] = 2\) but \(b \in F\), we must have \(2uv = 0\), which implies either \(b = u^2\) (so \([F(\sqrt{b}) : F] = 1\), which is not possible) or \(b = v^2a\). \(\square\)

**Remark.** You can show that any finite subgroup \(\Delta \leq (F^\times)/(F^\times)^2\) gives rise to a finite extension \(F(\sqrt{\Delta}) : F\) of degree \(|\Delta|\), where \(F(\sqrt{\Delta})\) is the field obtained by adjoining squareroots of representatives of all elements of \(\Delta\). Furthermore, it is a Galois extension with Galois group isomorphic to the set of group homomorphisms \(\text{Hom}(\Delta, \{\pm 1\})\), where the group structure is defined by pointwise multiplication: \((\alpha\beta)(x) := \alpha(x)\beta(x)\) for \(x \in \Delta\) and \(\alpha, \beta \in \text{Hom}(\Delta, \{\pm 1\})\). The isomorphism is given by a map

\[
\text{Aut}(F(\sqrt{\Delta}) : F) \to \text{Hom}(\Delta, \{\pm 1\})
\]

which sends an automorphism \(\sigma\) to the function \(\alpha : \Delta \to \{\pm 1\}\) defined by the formula

\[
\sigma(\sqrt{a}) = \alpha([a]) \sqrt{a},
\]

where \([a] \in \Delta \leq F^\times/(F^\times)^2\) is represented by \(a \in F^\times\), with \(\sqrt{a} \in F(\sqrt{\Delta})\) a choice of squareroot.

When \(K = \mathbb{Q}\), this implies that quadratic extensions are in bijective correspondence with squarefree (non-zero) integers: integers \(d\) which are not divisible by the square of a positive integer (other than 1). These look exactly like

\[
d = \pm p_1 \cdots p_r, \quad r \geq 0, \quad p_1, \ldots, p_r \text{ distinct primes}.
\]

**Theorem.** Every quadratic extension of \(\mathbb{Q}\) is contained in a cyclotomic extension. That is, if \(d\) is any integer, then there exists \(n \geq 1\) such that \(\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta_n)\).
We can assume that $d$ is squarefree. Note that if $d = d_1 \cdots d_r$, and if $\mathbb{Q}(\sqrt{d_i}) \subseteq \mathbb{Q}(\zeta_{n_i})$ for some $n_i$, then
\[
\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_r}) \subseteq \mathbb{Q}(\zeta_{n_1}, \ldots, \zeta_{n_r}) \subseteq \mathbb{Q}(\zeta_n)
\]
where $n = n_1 \cdots n_r$. Therefore it suffices to prove the theorem for the special cases of (i) $d = -1$, and (ii) $d = p$ or $d = -p$ for each prime $p$.

Of course, we know that $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i) = \mathbb{Q}(\zeta_4)$. We also know that $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$ since $\zeta_8 = (1 + i)/\sqrt{2}$, whence $\zeta_8 + \zeta_8^{-1} = \sqrt{2}$.

Thus to prove the theorem it suffices to prove the following, where we write
\[
p^* := (-1)^{(p-1)/2}p, \quad p \text{ an odd prime.}
\]

**Proposition.** For each odd prime $p$ we have $\sqrt{p^*} \in \mathbb{Q}(\zeta_p)$.

Thus, $\sqrt{-3} \in \mathbb{Q}(\zeta_3)$, $\sqrt{5} \in \mathbb{Q}(\zeta_5)$, $\sqrt{-7} \in \mathbb{Q}(\zeta_7)$, etc.

Recall that $G = \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \approx (\mathbb{Z}/p)^\times$ is cyclic of order $p - 1$, and therefore when $p$ is odd has exactly one subgroup $H$ of index 2. So there is a unique quadratic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_n)$, namely $\mathbb{Q}(\zeta_n)^H$. We need to identify what this is.

Let $\zeta = \zeta_p$ be a fixed primitive $p$th root of unity. Let
\[
\delta_p := \prod_{1 \leq i < j \leq p-1} (\zeta^i - \zeta^j), \quad \Delta_p := \delta_p^2 = \prod_{1 \leq i < j \leq p-1} (\zeta^i - \zeta^j)^2.
\]
Thus $\Delta$ is the discriminant of the cyclotomic polynomial $\Phi_p(X) = X^{p-1} + \cdots + X + 1$. The element $\delta_p$ satisfies $\sigma(\delta_p) = \pm \delta_p$, where the sign depends on whether $\sigma$ permutes the set $R = \{\zeta, \zeta^2, \ldots, \zeta^{p-1}\}$ of roots of the cyclotomic polynomial $\Phi_p$ by an even or odd permutation: $\sigma(\delta_p) = \delta_p$ iff it permutes $R$ by an even permutation.

Since $\Phi_p$ is irreducible, the Galois group $G$ acts transitively on $R$. The group $G$ is cyclic, which thus implies that a generator $\tau$ of $G$, viewed as a permutation of $R$, must be a single cycle. So $\tau$ is cycle of even length $p - 1$, so is an odd permutation, so $\tau(\delta_p) = -\delta_p$. Thus $\sigma_p(\delta_p) = \delta_p$ iff $\sigma \in H = \langle \tau^2 \rangle$. We have thus proved that
\[
\mathbb{Q}(\zeta_p)^H = \mathbb{Q}(\delta_p).
\]

We will show that, for an odd prime $p$,
\[
\Delta_p = (-1)^{(p-1)/2}p^{p-2} = p^{a^2}, \quad a = p^{(p-3)/2},
\]
whence $\mathbb{Q}(\zeta_p)^H = \mathbb{Q}(\delta_p) = \mathbb{Q}(\sqrt{p^*})$.

Suppose that $f$ is any monic polynomial over a field $F$, which factors as $f = \prod_{1 \leq i \leq n} (X - \alpha_i)$ over its splitting field. I’ll describe a formula for the discriminant.

**Proposition.** Suppose $f = \prod_{i=1}^{n} (X - \alpha_i)$. Then its discriminant is
\[
\Delta_f = (-1)^n (n-1)/2 \prod_{i=1}^{n} f'(\alpha_i)
\]
where $f' = Df$.

**Proof.** We have that
\[
\Delta_f = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 = (-1)^{(n-1)/2} \prod_{1 \leq i \leq n} \prod_{1 \leq j \leq n \atop j \neq i} (\alpha_i - \alpha_j),
\]
because of the $n(n-1)$ pairs $(i, j)$ with $1 \leq i, j \leq n$ and $i \neq j$, exactly half are such that $i > j$.

On the other hand,
\[
f'(X) = \sum_{1 \leq i \leq n} \prod_{1 \leq j \leq n \atop j \neq i} (X - \alpha_j).
\]
Plugging in a root gives

\[ f'(\alpha_i) = \prod_{1 \leq j \leq n \atop j \neq i} (\alpha_i - \alpha_j), \]

and therefore

\[ \Delta_f = (-1)^{n(n-1)/2} \prod_{1 \leq i \leq n \atop i \neq j} \prod_{1 \leq j \leq n \atop j \neq i} (\alpha_i - \alpha_j) \]

\[ = (-1)^{n(n-1)/2} \prod_{1 \leq i \leq n} f'(\alpha_i). \]

To apply this to \( f = \Phi_p \), consider the equation \((X - 1)\Phi_p(X) = X^p - 1\). Taking derivatives on both sides gives \( \Phi_p(X) + (X - 1)\Phi'_p(X) = pX^{p-1} \), and plugging in a root gives \((\zeta^i - 1)\Phi'_p(\zeta^i) = p\zeta^{(p-1)i}\). Therefore \( \Phi'_p(\zeta^i) = p\zeta^{-i}/(\zeta^i - 1) \), so, since \( n = \deg \Phi_p = p - 1 \), we have

\[ \Delta_{\Phi_p} = (-1)^{(p-1)(p-2)/2} \prod_{1 \leq i \leq p-1} \Phi'_p(\zeta^i) \]

\[ = (-1)^{(p-1)/2} \prod_{1 \leq i \leq p-1} \frac{p\zeta^{-i}}{\zeta^i - 1} \]

\[ = (-1)^{(p-1)/2} p^{p-1} \prod_{1 \leq i \leq p-1} \zeta^{-i} \prod_{1 \leq i \leq p-1} (\zeta^i - 1). \]

We have that \( \prod_{1 \leq i \leq p-1} \zeta^{-i} = \zeta^{-(1+2+\cdots+(p-1))} = \zeta^{-(p-1)/2} = 1. \) To compute \( \prod_{1 \leq i \leq p-1} (\zeta^i - 1) \), note that the \( \zeta^i - 1 \) are the roots of

\[ \Phi_p(X + 1) = (X + 1)^{p-1} + (X + 1)^{p-2} + \cdots + (X + 1) + 1 \]

\[ = X^{p-1} + \left( \binom{p}{1} X^{p-2} + \cdots + \binom{p}{p-2} \right) X + \binom{p}{p-1}. \]

Therefore \( \prod_{1 \leq i \leq p-1} (\zeta^i - 1) = \binom{p}{p-1} = p. \)

Thus

\[ \Delta_{\Phi_p} = (-1)^{(p-1)/2} p^{p-2} = p^{*}(p(p-3)/2)^2, \]

so \( \mathbb{Q}(\delta_p) = \mathbb{Q}(\sqrt{p^*}). \)

61. Quadratic Residues

We have shown that \( \sqrt{p^*} \in \mathbb{Q}(\zeta_p) \), and have given a formula: \( \sqrt{p^*} = \pm \delta_p/p^{(p-3)/2} \). This formula is a bit complicated to evaluate, but when we do, we get a surprisingly simple result, when we choose to write elements of \( \mathbb{Q}(\zeta_p) \) in terms of the \( \mathbb{Q} \)-basis \( \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1} \) of \( \mathbb{Q}(\zeta_p) \). (In the following, the left-hand side is only up to a sign, which I haven’t determined.)

\[ \pm \sqrt{-3} = \zeta_3 - \zeta_3^2, \]

\[ \pm \sqrt{5} = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4, \]

\[ \pm \sqrt{-7} = \zeta_7 + \zeta_7^2 - \zeta_7^3 + \zeta_7^4 - \zeta_7^5 - \zeta_7^6, \]

\[ \pm \sqrt{-11} = \zeta_{11} - \zeta_{11}^2 + \zeta_{11}^3 + \zeta_{11}^4 - \zeta_{11}^5 - \zeta_{11}^6 - \zeta_{11}^7 - \zeta_{11}^8 + \zeta_{11}^9 + \zeta_{11}^{10}, \]

\[ \pm \sqrt{-13} = \zeta_{13} - \zeta_{13}^2 + \zeta_{13}^3 + \zeta_{13}^4 - \zeta_{13}^5 - \zeta_{13}^6 - \zeta_{13}^7 - \zeta_{13}^8 + \zeta_{13}^9 + \zeta_{13}^{10} - \zeta_{13}^{11} + \zeta_{13}^{12}. \]
Notably, the coefficients are always ±. There is also a pattern among these coefficients: \( \zeta^k \) gets a “+” sign if and only if \( \zeta^k = \zeta^{\ell^2} \) for some \( \ell \).

Given a prime \( p \), we say that \( a \in \mathbb{Z} \) is a \textbf{quadratic residue} mod \( p \) if there exists \( b \in \mathbb{Z} \) such that \( b^2 \equiv a \mod p \).

Note that the set of quadratic residues mod \( p \) is closed under multiplication. Also, any integer divisible by \( p \) is trivially a quadratic residue mod \( p \). We often exclude the integers divisible by \( p \) from the discussion, since they do not provide elements of the group \( \mathbb{Z}/p \mathbb{Z} \).

There is a notation used for talking about quadratic residues, called the \textbf{Legendre symbol}:

\[
\left( \frac{a}{p} \right) = \begin{cases} 
0 & \text{if } p \nmid a, \\
+1 & \text{if } p \mid a \text{ and } a \text{ is a quadratic residue mod } p, \\
-1 & \text{if } p \nmid a \text{ and } a \text{ is not a quadratic residue mod } p. 
\end{cases}
\]

For an odd prime \( p \), exactly half the congruence classes in \( \mathbb{Z}/p \mathbb{Z} \) are quadratic residues.

**Lemma.** For an odd prime \( p \), the subset \( R \subseteq (\mathbb{Z}/p \mathbb{Z})^\times \) of congruence classes which are quadratic residues is the unique subgroup of index 2. It is:

1. the image of the homomorphism \( a \mapsto a^2: (\mathbb{Z}/p \mathbb{Z})^\times \to (\mathbb{Z}/p \mathbb{Z})^\times \), and
2. the kernel of the homomorphism \( a \mapsto a^{(p-1)/2}: (\mathbb{Z}/p \mathbb{Z})^\times \to \mathbb{Z}/p \mathbb{Z} \).

**Proof.** The kernel of \( a \mapsto a^2 \) is \( \{ \pm 1 \} \), and its image is \( R \), so it factors through an isomorphism

\[
(\mathbb{Z}/p \mathbb{Z})^\times /\{ \pm 1 \} \cong R \subseteq (\mathbb{Z}/p \mathbb{Z})^\times.
\]

In particular, the image \( R \) is a subgroup of order \((p - 1)/2\), and so of index 2. It is the unique such subgroup since \( (\mathbb{Z}/p \mathbb{Z})^\times \) is cyclic.

The kernel \( a \mapsto a^{(p-1)/2} \) is exactly the subgroup \( R \), again because \( (\mathbb{Z}/p \mathbb{Z})^\times \) is cyclic. \( \square \)

A consequence of this is that, for odd primes \( p \),

\[
\sigma_k(\delta_p) = \left( \frac{k}{p} \right) \delta_p, \quad k \in (\mathbb{Z}/p \mathbb{Z})^\times,
\]

where \( \delta_p = \prod_{1 \leq i < j \leq p-1}(\zeta_i - \zeta_j) \) and \( \sigma_k \in \text{Aut}(\mathbb{Q}(\zeta_p) : \mathbb{Q}) \) as in the previous section. This is exactly because the quadratic residues \( R \subseteq (\mathbb{Z}/p \mathbb{Z})^\times \) form exactly the unique index 2 subgroup of \( (\mathbb{Z}/p \mathbb{Z})^\times \approx \text{Aut}(\mathbb{Q}(\zeta_p) : \mathbb{Q}) \), and we showed \( \sigma(\delta_p) = \delta_p \) iff \( \sigma \) is in this subgroup.

Here is a kind of “formula” for the Legendre symbol.

- For \( p = 2 \) we have
  \[
  \left( \frac{a}{2} \right) = \begin{cases} 
0 & \text{if } 2 \mid a, \\
+1 & \text{if } 2 \nmid a.
\end{cases}
\]

- For an odd prime \( p \), we have
  \[
  \left( \frac{a}{p} \right) = a^{(p-1)/2},
\]

where we are somewhat abusive with notation, in that we identify the elements \{0, +1, −1\} of \( \mathbb{F}_p \) with the corresponding elements of \( \mathbb{Z} \).

From the above considerations, we can read of the following fact.

**Proposition.** The Legendre symbol is multiplicative. That is

\[
\left( \frac{xy}{p} \right) = \left( \frac{x}{p} \right) \left( \frac{y}{p} \right)
\]

for all \( x, y \in \mathbb{Z} \).

**Proof.** When \( p = 2 \) there is not much to prove. For odd prime we have \( (ab)^{(p-1)/2} = a^{(p-1)/2}b^{(p-1)/2} \). Alternately, use that \( \left( \frac{a}{p} \right) = \chi(a) \), and \( \chi: (\mathbb{Z}/p \mathbb{Z})^\times \to \{ \pm 1 \} \) is a homomorphism. \( \square \)
The Legendre symbol is telling us about some quadratic extensions of finite fields.

**Proposition.** The polynomial $X^2 - a \in \mathbb{F}_p[X]$ is irreducible if and only if $(\frac{-a}{p}) = -1$.

**Proof.** Straightforward.

The computation of $(\frac{-1}{p})$ is easy.

**Proposition.** For $p$ odd we have that

$$(\frac{-1}{p}) = (-1)^{(p-1)/2}.$$  

That is, $-1$ is a quadratic residue modulo an odd prime $p$ if $p \equiv 1 \mod 4$, and not if $p \equiv -1 \mod 4$.

**Proof.** This is just the formula we gave above for odd primes, together with the fact that the powers of the integer $-1$ can only be $\pm 1$, so we can read off which one it is from its residue mod $p$.

Alterate proof: $\mathbb{F}_p^\times$ is a cyclic group of order $p - 1$, and $-1$ is the unique element of order 2 in it. Thus it is a quadratic residue if there is an element of order 4 in $\mathbb{F}_p^\times$, i.e., iff $4 \mid p - 1$. $\square$

Thus, $X^2 + 1 \in \mathbb{F}_p[X]$ is irreducible iff $p \equiv -1 \mod 4$. Thus, only for $p = 3, 7, 11, 19, \ldots$ do we have $\mathbb{F}_{p^2} = \mathbb{F}_p[i]$, where $i^2 = -1$.

Here is a striking consequence of this: a proof of a very special case of Dirichlet’s theorem on primes in arithmetic progressions.

**Corollary.** There are infinitely many primes which are congruent to 1 modulo 4. (E.g., 5, 13, 17, 29, 37, 41, \ldots)

**Proof.** Let $p_1, \ldots, p_r$ be any list of primes which are congruent to 1 mod 4. I will produce a new prime congruent to 1 mod 4 which is not on this list. Since I can do this for any finite list, this implies there must be an infinite number of them.

Let $n = (2p_1 \cdots p_r)^2 + 1$. Factor this as $n = q_1 \cdots q_s$ where each $q_i$ is prime (the $q_i$s need not be distinct). It clear that each $q_i$ is not in the list \{2, $p_1, \ldots, p_r$\}, since $n \equiv -1 \mod p_i$. The congruence

$$(2p_1 \cdots p_r)^2 \equiv -1 \mod q_i,$$

implies that $-1$ is a quadratic residue mod $q_i$, so $q_i \equiv 1 \mod 4$ as desired. $\square$

Here’s another one.

**Proposition.** A odd prime $p$ can be written $p = a^2 + b^2$ for integers $a, b \in \mathbb{Z}$ if and only if $p \equiv 1 \mod 4$.

**Proof.** $\Longrightarrow$: If $p = a^2 + b^2$, then since $a^2, b^2 \equiv 0, 1 \mod 4$ we can only have $p \equiv 0, 1, 2 \mod 4$.

$\Longleftarrow$: This uses the fact that the ring of Gaussian integers

$$\mathbb{Z}[i] := \{ a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z} \}.$$

is a PID, so has unique factorization: every element is a product of finitely many irreducibles, uniquely up to reordering and units. Note that $\mathbb{Z}[i]^\times = \{ \pm 1, \pm i \}$, using the fact that the norm $N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$ defines a multiplicative function $N: \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$, so that $\mathbb{Z}[i]^\times = \{ z \in \mathbb{Z}[i] \mid N(z) = 1 \}$.

Suppose $p \equiv 1 \mod 4$. I’ll show $p$ is reducible in $\mathbb{Z}[i]$, i.e., $p = uv$ where $u, v$ are not units in $\mathbb{Z}[i]$. Given this, $p^2 = N(p) = N(u)N(v)$ in $\mathbb{Z}$, and since $N(u), N(v) > 1$ we must have $p = N(u) = N(v)$.

Writing $u = a + bi$ with $a, b \in \mathbb{Z}$ gives $p = N(u) = a^2 + b^2$.

So I suppose $p$ is irreducible in $\mathbb{Z}[i]$ and derive a contradiction. Since $p \equiv -1 \mod 4$ we know that $-1$ is a quadratic residue modulo $p$, so that there exists $a \in \mathbb{Z}$ such that $p \mid a^2 + 1$ in $\mathbb{Z}$. But $a^2 + 1 = (a + i)(a - i)$, so $p \mid (a + i)(a - i) \in \mathbb{Z}[i]$. If $p$ is irreducible then $p$ divides one of the factors, say $p \mid a + i$. But $p(c + di) = (pc) + (pd)i$, so $p \mid a + i$ implies $p \mid 1$, which is impossible. $\square$
Remark. That $\mathbb{Z}[i]$ is a PID, and that PIDs are UFDs, are standard facts proved in abstract algebra textbooks. (Reference.)

I return to the formula for $\sqrt{p^*}$. For odd primes $p$, define

$$\epsilon_q := \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_q^a, \quad \zeta_q = e^{2\pi i/p}.$$

**Lemma.** For an odd prime $p$, we have that $\epsilon_p^2 = p^*$, whence $p^{(p-3)/2}\epsilon_p = \pm \delta_p$.

**Proof.** Write $\zeta = \zeta_p$. We have

$$\epsilon_p^2 = \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \left(\frac{a}{p}\right) \zeta^a \zeta^b = \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \left(\frac{ab}{p}\right) \zeta^{a+b}.$$

We can reindex the inner sum using $b = ac$, since $x \mapsto ax$ defines a bijection $\mathbb{F}_p^\times \to \mathbb{F}_p^\times$. Thus

$$\epsilon_p^2 = \sum_{a=1}^{p-1} \sum_{c=1}^{p-1} \left(\frac{a^2 c}{p}\right) \zeta^{a+ac} = \sum_{c=1}^{p-1} \left(\frac{c}{p}\right) \sum_{a=1}^{p-1} (\zeta^{1+c})^a = \sum_{c=1}^{p-1} \left(\frac{c}{p}\right) \left(-1 + \sum_{a=0}^{p-1} (\zeta^{1+c})^a\right).$$

Since

$$\sum_{a=0}^{p-1} (\zeta^{1+c})^a = \begin{cases} p & \text{if } 1 + c \equiv 0 \pmod{p}, \text{ so } \zeta^{1+c} = 1, \\ 0 & \text{if } 1 + c \not\equiv 0 \pmod{p}, \text{ so } \zeta^{1+c} \text{ is a primitive } p\text{th root of unity}, \end{cases}$$

we deduce

$$\epsilon_p^2 = \sum_{c=1}^{p-1} \left(\frac{c}{p}\right) + p \left(\frac{-1}{p}\right).$$

Since exactly half the integers in $\{1, \ldots, p-1\}$ are quadratic residues (i.e., $(\mathbb{F}_p)^\times$ is a subgroup of index 2 in $\mathbb{F}_p^\times$), the first term is 0, so

$$\epsilon_p^2 = p \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}p = p^*$$

as desired. \qed

As a consequence of this, we have that

$$\sigma_k(\epsilon_p) = \left(\frac{k}{p}\right) \epsilon_p, \quad k \in (\mathbb{Z}/p)^\times.$$

**Remark.** It actually turns out that, if we make sure to set $\zeta_p := e^{2\pi i/p}$, that

$$\epsilon_p = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod{4}, \\ i\sqrt{p} & \text{if } p \equiv -1 \pmod{4}. \end{cases}$$

I.e., it is either positive real or positive imaginary. This is not obvious. See this paper: [https://math.ucsd.edu/~revans/Determination.pdf](https://math.ucsd.edu/~revans/Determination.pdf) for some proofs.
62. Quadratic Reciprocity

The discriminant formula \( \sigma_k(\delta_p) = (\frac{k}{p}) \delta_p \) gives a way to calculate the Legendre symbol.

**Proposition.** If \( k \nmid p \), then \((\frac{k}{p}) = (-1)^m\), where \( m \) counts size of the set
\[
\{ (i, j) \mid 1 \leq i < j \leq p - 1, \text{ remainder}(ki \div p) > \text{remainder}(kj \div p) \}.
\]

**Proof.** We have
\[
\sigma_k(\delta_p) = \prod_{1 \leq i < j \leq p} (\zeta^{ki} - \zeta^{kj}).
\]
We get a sign change for every \( i < j \) such that \( \text{remainder}(ki \div p) > \text{remainder}(kj \div p) \).

This gives another way to calculate \((\frac{-1}{p})\) for odd \( p \): for \( 1 \leq x \leq p - 1 \) we have \( \text{remainder}(-x \div p) = p - x \), so for all \( 1 \leq i < j \leq p - 1 \), we have \( \text{remainder}(-i \div p) > \text{remainder}(-j \div p) \). Therefore
\[
(\frac{-1}{p}) = (-1)^{(p-1)(p-2)/2} = (-1)^{(p-1)/2},
\]
since \((p-1)(p-2)/2\) is the number of such pairs and \( p - 2 \) is odd.

This also computes \((\frac{2}{p})\).

**Proposition.** For \( p \) odd we have that
\[
(\frac{2}{p}) = (-1)^{(p^2-1)/8}.
\]
That is, \( 2 \) is a quadratic residue modulo an odd prime \( p \) when \( p \equiv \pm1 \) mod \( 8 \), and is not when \( p \equiv \pm3 \) mod \( 8 \).

For instance, \( 2 \equiv 3^2 \mod 7 \), \( 2 \equiv 6^2 \mod 17 \), \( 2 \equiv 5^2 \mod 23 \), \( 2 \equiv 8^2 \mod 31 \), but 2 is not a square modulo 3, 5, 11, 13, 19, 29, . . .

**Proof.** Let \( d = (p - 1)/2 \), so \( p - 1 = 2d \). We can partion the set \( \{1, \ldots, p - 1\} = (\mathbb{Z}/p)^\times \) in two subsets in two ways.

**Lower/upper partition:**
\[
L = \{1, \ldots, d\}, \quad U = \{d + 1, \ldots, 2d\} = \{-d, \ldots, -1\}.
\]

**Even/odd partition:**
\[
E = \{2, \ldots, 2d\}, \quad O = \{1, \ldots, 2d - 1\} = \{-2d, \ldots, -2\}.
\]

The operation \( x \mapsto 2x \) produces bijections
\[
L \xrightarrow{\sim} E, \quad U \xrightarrow{\sim} O.
\]
Furthermore, both of these bijections are “order preserving”, in that they preserve the natural ordering of the exponents \( 1 < 2 < \cdots < 2d \) in each set. Now consider the set of pairs \( (i, j) \) with \( 1 \leq i < j \leq p - 1 \). There are three kinds of such pairs. The following chart describes the three kinds, as well as what the operation \( x \mapsto 2x \) does to them.

- \( “L/E” \) : \( (i \in L, j \in L) \), \( (d(d-1) = 2 \text{ elements}) \) \( \iff \) \( “E/E” \) : \( (i \in E, j \in E) \)
- \( “U/U” \) : \( (i \in U, j \in U) \), \( (d(d-1)/2 \text{ elements}) \) \( \iff \) \( “O/O” \) : \( (i \in O, j \in O) \)
- \( “L/U” \) : \( (i \in L, j \in U) \), \( (d^2 \text{ elements}) \) \( \iff \) \( “E/O” \) : \( (i \in E, j \in O) \)

Because \( L \xrightarrow{\sim} E \) and \( U \xrightarrow{\sim} O \) are order preserving, sign changes can only come from \( “L/U” \) pairs which are sent to \( “E/O” \) pairs which are “out of order”. So \((\frac{2}{p}) = (-1)^m\) where
\[
M = \text{number of } (i, j) \in E \times O \text{ such that } i > j.
\]
We count
\[ M = 1 + 2 + \cdots + d = \frac{(d+1)d}{2} = \frac{q^2 - 1}{8}. \]
so \( \left( \frac{2}{q} \right) = (-1)^{(q^2-1)/8} \) as desired.

Quadratic reciprocity was first noticed by Euler and Lagrange, but was only given a complete proof by Gauss (at the age of 19). Gauss eventually gave eight different proofs of this theorem. He called it the “golden theorem”. There apparently about 250 different published proofs of quadratic reciprocity. Many of these are just variations of each other, but it is a fact that some of these proofs are quite different from the one I’m going to give, which is based on one of Gauss’s ideas, expressed using Galois theory.

**Theorem (Quadratic reciprocity).** For odd primes \( p \) and \( q \), we have
\[
\left( \frac{p}{q} \right) = \left( \frac{q^*}{p} \right),
\]
where \( q^* = (-1)^{(q-1)/2}q \).

**Remark.** Since \( q^* = (-1)^{(q-1)/2}q \), the multiplicativity of the Legendre symbol gives:
\[
\left( \frac{pq}{p} \right) = \left( \frac{q^*}{p} \right) = \left( \frac{-1}{p} \right) \left( \frac{q}{p} \right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left( \frac{q}{p} \right).
\]
In other words, for odd primes \( p \) and \( q \) we have
\[ \left( \frac{pq}{p} \right) = \pm \left( \frac{q}{p} \right), \]
where the sign in front is \(-1\) if \( p \equiv q \equiv -1 \mod 4 \), and is \(+1\) otherwise.

**Remark.** The two special formulas:
\[
\left( \frac{-1}{p} \right) = (-1)^{(p-1)/2}, \quad \left( \frac{2}{p} \right) = (-1)^{(p^2-1)/8}, \quad (p \text{ odd}),
\]
which we proved earlier, are sometimes called the “supplementary cases” of quadratic reciprocity. Using these, quadratic reciprocity, multiplicativity \( \left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right) \), and that \( \left( \frac{n}{p} \right) = \left( \frac{b}{p} \right) \) if \( a \equiv b \mod p \), you can compute \( \left( \frac{a}{p} \right) \) very efficiently. To compute \( \left( \frac{2}{p} \right) \), first replace \( n \) with remainder \( (n \div p) \), then factor \( n = \pm q_1 \cdots q_k \) with \( q_i \) prime, then use quadratic reciprocity to compute \( \left( \frac{q_i}{p} \right) \) for each \( i \) when \( q_i \) is odd, with the supplementary cases to handle \( \left( \frac{2}{p} \right) \) and \( \left( \frac{-1}{p} \right) \).

The idea of the proof is to compare two formulas for the Legendre symbols \( \left( \frac{a}{q} \right) \) and \( \left( \frac{b}{p} \right) \) for odd primes \( p, q \):

1. We have
\[
\sigma_a(\epsilon_q) = \left( \frac{a}{q} \right) \epsilon_q, \quad \sigma_a \in \Aut(\mathbb{Q}(\zeta_q) : \mathbb{Q}) = (\mathbb{Z}/q)\times.
\]
Here \( \sigma_a \) is the automorphism given on roots of unity by \( \sigma_a(\zeta_q) = \zeta_q^a \), and \( \epsilon_q = \sum_{k=1}^{p-1} \left( \frac{k}{q} \right) \zeta_q^k \) so \( \epsilon_q^2 = q^* \).

2. We have
\[
\phi_p(\sqrt{b}) = \left( \frac{b}{p} \right) \sqrt{b}, \quad p \nmid b.
\]
Here \( \sqrt{b} \) is any chosen squareroot of \( b \in \mathbb{F}_p^\times \), which lives in some finite extension \( \mathbb{F}_p^r : \mathbb{F}_p \) (it is guaranteed to be in \( \mathbb{F}_{p^2} \)), while \( \phi_p \) is the mod \( p \) Frobenius.

\[\text{http://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html}\]
Consider the special cases \(a = p\) and \(b = q^*\), so these become:

\[
\sigma_p(\epsilon_q) = \left(\frac{p}{q}\right) \epsilon_q, \quad \phi_p(\sqrt{q^*}) = \left(\frac{q^*}{p}\right) \sqrt{q^*}.
\]

These are not directly comparable, because they are formulas which live in different fields: \(Q(\zeta_q)\) and \(F_{p^r}\). However, they are in some ways very similar:

- \(\sigma_p\) is a \(p\)th power function on the elements of the form \(\zeta_q^5 \in Q(\zeta_q)\), while \(\phi_p\) is the \(p\)th power map on every element of \(F_{p^r}\) (which are all roots of unity or 0).
- \(\epsilon_q\) is a squareroot of \(q^*\) in \(Q(\zeta_q)\), while \(\sqrt{q^*}\) is a squareroot of \(q^*\) in \(F_{p^r}\).

The idea of the proof can be easily summarized: the second identity is equal to the first identity reduced modulo \(p\). The only problem with this idea is that it doesn’t make sense as stated: you can’t reduce elements of fields of characteristic 0 modulo \(p\). But with a little work I will make it make sense.

Here is what I will do: I will produce a diagram of rings and ring homomorphisms of the form

\[
\begin{array}{ccc}
Q(\zeta_q) & \xleftarrow{\sigma_p} & Z[\zeta_q] \xrightarrow{\pi} F_{p^r} \\
| \sigma_p & | \sigma_p & | \phi_p \\
Q(\zeta_q) & \xleftarrow{\sigma_p} & Z[\zeta_q] \xrightarrow{\pi} F_{p^r}
\end{array}
\]

Here \(Z[\zeta_q]\) is a subring of \(Q(\zeta_q)\) which contains the element \(\epsilon_q\). It will turn out that all elements \(\sigma \in \text{Aut}(Q(\zeta_q) : Q)\) restrict to automorphisms \(\sigma : Z[\zeta_q] \to Z[\zeta_q]\). In particular, the formula

\[
\sigma_p(\epsilon_q) = \left(\frac{p}{q}\right) \epsilon_q
\]

makes sense in \(Z[\zeta_q]\). I’ll also build a ring homomorphism \(\pi : Z[\zeta_q] \to F_{p^r}\) such that

\[
\pi(\epsilon_q) = \sqrt{q^*}, \quad \phi_p \pi = \pi \sigma_p.
\]

Given this, we get an identity

\[
\pi(\sigma_p(\epsilon_q)) = \phi_p(\pi(\epsilon_q)) = \phi_p(\sqrt{q^*})
\]

in \(F_{p^r}\), and thus

\[
\left(\frac{p}{q}\right) \sqrt{q^*} = \left(\frac{q^*}{p}\right) \sqrt{q^*},
\]

which gives us \(\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)\) (because \(q^* \neq 0\) since \(p\) and \(q\) are distinct primes).

**Example.** Taking \(q = 3\) and \(p = 5\), we can construct

\[
Q(\omega) \xrightarrow{\pi} Z[\omega] \xrightarrow{\pi} F_{5^2}.
\]

We can write \(F_{5^2} = F_5(a)\) where \(a^2 = -a - 1\), since \(X^2 + X + 1 \in F_5[X]\) is irreducible. Note that \(a^3 = 1\), whence \(a^5 = a^2 = -a - 1\). Then \(\pi\) is given explicitly by \(\pi(m + n \omega) = m + na\). You can check directly that \(\pi \sigma_5 \pi = \phi_5 \pi\), since

\[
\pi \sigma_5(m + n \omega) = \pi(m + n \omega^5) = \pi(m + n(-1 - \omega)) = m + n(-1 - a),
\]

while

\[
\sigma_5 \pi(m + n \omega) = \sigma_5(m + na) = (m + na)^5 = m + na^5 = m + n(-1 - a).
\]

Therefore

\[
\pi(\sqrt{-3}) = \pi(\epsilon_3) = \pi(\omega - \omega^2) = a - a^2 = 1 - 2a,
\]

and you can check directly that \((1 - 2a)^2 = -3\) in \(F_{5^2}\). We see that \(-3\) is thus not a quadratic residue mod 5 (because its squareroot is in \(F_{5^2} \setminus F_5\)), which is compatible with the fact that 5 is
not a quadratic residue mod 3 (since \( \sigma_5(\epsilon_3) = \sigma_5(\omega - \omega^2)\omega^5 - \omega^{10} = -\epsilon_3 \), so \([5]\) is not a square of an element in \((\mathbb{Z}/3)^\times\).

I’ll write \( \zeta = \zeta_q \). Let
\[
\mathbb{Z}[\zeta] = \{ \sum_{k=0}^{n} c_k \zeta^k \mid c_k \in \mathbb{Z}, \ k \geq 0 \} \subset \mathbb{Q}(\zeta)
\]
the set of expressions in \( \mathbb{Q}(\zeta) \) which can be written as integer combinations of powers of \( \zeta \). It is obviously a subring of \( \mathbb{Q}(\zeta) \), and \( \epsilon_q \in \mathbb{Z}[\zeta] \). Furthermore, if \( \sigma_a \in \text{Aut}(\mathbb{Q}(\zeta) : \mathbb{Q}) \), we have
\[
\sigma_a(\sum c_k \zeta^k) = \sum c_k \zeta^{ak} \in \mathbb{Z}[\zeta],
\]
so \( \sigma_a \) restricts to a homomorphism \( \mathbb{Z}[\zeta] \to \mathbb{Z}[\zeta] \), which is actually an isomorphism because \( (\sigma_a)^{-1} = \sigma_b \) for some \( b \).

**Lemma.** Every element \( u \in \mathbb{Z}[\zeta] \) has a unique expression of the form
\[
u = \sum_{k=0}^{q-2} c_k \zeta^k, \quad c_k \in \mathbb{Z}.
\]

**Proof.** We prove existence of such an expression by induction on \( n \geq q - 2 \), where \( u = \sum_{k=0}^{n} c_k \zeta^k \).

If \( n = q - 2 \) there is nothing to prove. If \( n > q - 2 \), we have an identity \( \zeta^n = \zeta^{n-1} + \cdots + \zeta^{n-(q-1)} \), obtained from \( \zeta^{n-(q-2)} \Phi_q(\zeta) = 0 \). Using this, we see that \( u \) can be expressed as \( u = \sum_{k=0}^{n-1} c_k' \zeta^k \) for some \( c_k' \in \mathbb{Z} \).

Uniqueness is a consequence of the fact that \( 1, \zeta, \ldots, \zeta^{q-2} \) is a \( \mathbb{Q} \)-basis of \( \mathbb{Q}(\zeta) \).

\[\square\]

**Proposition.** There is an isomorphism of rings
\[
\mathbb{Z}[X]/(\Phi_q) \cong \mathbb{Z}[\zeta]
\]
which sends \( X \mapsto \zeta \).

**Proof.** Clearly, there is a unique homomorphism \( \mathbb{Z}[X] \to \mathbb{Z}[\zeta] \) sending \( X \mapsto \zeta \), which is surjective since \( \zeta \) generates the ring \( \mathbb{Z}[\zeta] \). Furthermore since \( \Phi_q(\zeta) = 0 \) this homomorphism factors through a unique homomorphism
\[
\mu : \mathbb{Z}[X]/(\Phi_q(X)) \to \mathbb{Z}[\zeta]
\]
which is also surjective. Because \( \Phi_q(X) \) is a monic polynomial of degree \( q - 1 \), we see that \( \mathbb{Z}[X]/(\Phi_q(X)) \) can be written as \( \sum_{i=0}^{q-2} a_i X^i \) with \( a_i \in \mathbb{Z} \). Since \( \mathbb{Z}[\zeta] \subset \mathbb{Q}(\zeta) \), we know that every element of \( \mathbb{Z}[\zeta] \) can be written uniquely as \( \sum_{i=0}^{q-2} a_i \zeta^i \) with \( a_i \in \mathbb{Q} \). Combining these statements, we see that \( \mu \) must be injective, since \( 0 = \mu(\sum_{i=0}^{q-2} a_i X^i) = \sum_{i=0}^{q-2} a_i \zeta^i \) implies \( a_i = 0 \). Thus \( \mu \) is an isomorphism as desired.

\[\square\]

Recall that \( \mathbb{F}_p^\times \) is cyclic of order \( p - 1 \). Thus \( \mathbb{F}_p^\times \) contains a primitive \( q \)th root of unity iff \( p^r \equiv 1 \mod p \). Given \( q \) not divisible by \( p \) there is always such an \( r \), e.g., let \( r = \text{order of } p \) in the group \( (\mathbb{Z}/q)^\times \).

**Proposition.** Consider a primitive \( q \)th root of unity \( \overline{\zeta} \in \mathbb{F}_p^\times \). There exists a unique ring homomorphism
\[
\pi : \mathbb{Z}[\zeta] \to \mathbb{F}_p^\times
\]
sending \( \zeta_q \mapsto \overline{\zeta} \).

**Corollary.** For \( \pi : \mathbb{Z}[\zeta] \to \mathbb{F}_p^\times \) as above, we have \( \pi \sigma_p = \phi_p \pi \).

**Proof.** Both \( \pi \sigma_p \) and \( \phi_p \pi \) are ring homomorphisms \( \mathbb{Z}[\zeta] \to \mathbb{F}_p^\times \). We have \( \pi \sigma_p(\zeta_q) = \pi(\overline{\zeta}^p) = \overline{\zeta}^p \) and \( \phi_p \pi(\zeta_q) = \phi_p(\overline{\zeta}) = \overline{\zeta}^p \). So by the uniqueness part of the previous proposition, \( \pi \sigma_p = \phi_p \pi \).

\[\square\]
63. Algebraic closures

An algebraic closure of a field \( F \) is a field extension \( L : F \) such that (i) it is an algebraic extension, and (ii) \( L \) algebraically closed, i.e., every polynomial in \( L[X] \) has a root in \( L \) (and hence splits over \( L \)).

**Proposition.** \( L : F \) is an algebraic closure iff (a) every element of \( L \) is a root of some \( f \in F[X] \), and (b) every \( f \in F[X] \) splits over \( L \).

**Proof.** Condition (a) is clearly equivalent to (i). Also it is clear that (ii) implies (b). It remains to show that (a) and (b) imply (ii).

It suffices to show that every irreducible \( f \in \text{Irred} L \) splits over \( L \). Since \( f = \sum c_k X^k \) has only finitely many non-zero coefficients \( c_0, \ldots, c_n \in L \), and \( L : F \) is algebraic, we have \( f \in K[X] \) where \( K = F(c_0, \ldots, c_n) \subseteq L \). By (a) each \( c_k \) is algebraic over \( F \), so \( [K : F] < \infty \).

Since \( f \) is irreducible over \( L \) it is also irreducible over the subfield \( K \), so we can construct an abstract simple extension \( K(\alpha) : K \) with \( f(\alpha) = 0 \). Since \( [K(\alpha) : F] = [K(\alpha) : K][K : F] < \infty \), there is a minimal polynomial \( g = f_{\alpha/F} \in \text{Irred}(F) \), and we must have \( f \mid g \in K[X] \).

By (b) \( g \) splits over \( L \), and therefore so does its factor \( f \). \( \square \)

To produce an algebraic closure of \( F \), it suffices to produce any extension \( C : F \) where \( C \) is algebraically closed. Then the subset \( F^{\text{alg}} \subseteq C \) of elements which are algebraic over \( F \) is an algebraic closure of \( F \).

**Example.** \( \mathbb{Q}^{\text{alg}} \subseteq \mathbb{C} \) is the algebraic closure of \( \mathbb{Q} \). It is also the algebraic closure of any number field, i.e., of any \( K \) which is finite over \( \mathbb{Q} \).

**Example (Algebraic closure \( \overline{\mathbb{F}}_p \) of \( \mathbb{F}_p \)).** Fix a prime \( p \). Define a sequence of fields

\[
K_0 \subseteq K_1 \subseteq K_2 \subseteq K_3 \subseteq \cdots
\]

so that

- \( K_0 = \mathbb{F}_p \), and
- \( K_n \) is defined to be the splitting field of \( X^{p^n} - X \) over \( K_{n-1} \).

Each extension \( K_n : K_{n-1} \) is a finite extension, so each \( K_n \) is a finite field. On the other hand, since \( X^{p^n} - X \) splits over \( K_n \), we see that \( K_n \) contains a splitting field of \( X^{p^n} - X \), i.e., a subfield isomorphic to \( \mathbb{F}_{p^n} \).

(It turns out that \( K_n \approx \mathbb{F}_{p^m} \) where \( m = \text{lcm}(1, \ldots, n) \). So \( K_0 = K_1 = \mathbb{F}_p, K_2 = \mathbb{F}_{p^2}, K_3 = \mathbb{F}_{p^3}, K_4 = \mathbb{F}_{p^6}, K_5 = K_6 = \mathbb{F}_{p^{12}}, \ldots \))

We define \( \overline{\mathbb{F}}_p \) to be the formal union of the above sequence of fields: \( \overline{\mathbb{F}}_p := \bigcup_n K_n \). This is still a field: any finite list of elements \( \alpha_1, \ldots, \alpha_k \in \overline{\mathbb{F}}_p \) are contained in \( K_n \) for some sufficiently large \( n \), so their sums and products are defined in \( K_n \) and hence in \( \overline{\mathbb{F}}_p \), and the field axioms can be verified for these operations.

To see that \( \overline{\mathbb{F}}_p : \mathbb{F}_p \) is an algebraic closure, note (a) that it is an algebraic extension, since each \( K_n : \mathbb{F}_p \) is algebraic, so every element of \( \overline{\mathbb{F}}_p \) is algebraic over \( \mathbb{F}_p \). To see that \( \overline{\mathbb{F}}_p \) is algebraically closed, it suffices to show (b) that every \( f \in \mathbb{F}_p[X] \) splits over it. But such an \( f \) has a splitting field which is a finite extension of \( \mathbb{F}_p \), and so is isomorphic to some \( \mathbb{F}_{p^n} \), which is isomorphic to a subfield of \( K_n \). Since \( \overline{\mathbb{F}}_p \) contains a subfield isomorphic to \( \mathbb{F}_{p^n} \), the claim follows.

It is a theorem that every field has an algebraic closure. In the case of \( \mathbb{F}_p \), we could explicitly write down a countable list of polynomials \( \{X^{p^n} - X\}_{n \geq 1} \) such that every algebraic element over \( \mathbb{F}_p \) is a root of one of the polynomials in our list. In the general case we don’t have such a list, and the proof of the theorem requires the axiom of choice, in the form of Zorn’s lemma. (The proof given here is one of the ones described in Milne, Fields and Galois Theory, [https://www.jmilne.org/math/CourseNotes/ft.html](https://www.jmilne.org/math/CourseNotes/ft.html))
Theorem (Zorn’s lemma). Let \((S, \subseteq)\) be a partially ordered set, such that

1. \(S\) is non-empty, and
2. for every non-empty chain \(C \subseteq S\) there is an upper bound \(u \in S\) for \(C\).

Then \(S\) has a maximal element \(m \in S\).

A partially ordered set is \((S, \subseteq)\), where \(\subseteq\) is a relation satisfying: (a) \(x \leq x\), (b) \(x \leq y\) and \(y \leq x\) imply \(x = y\), and (c) \(x \leq y\) and \(y \leq z\) imply \(x \leq z\). A chain is a subset \(C \subseteq S\) such that for all \(x, y \in C\), either \(x \leq y\) or \(y \leq x\). An upper bound for a subset \(C \subseteq S\) is \(u \in S\) such that \(c \leq u\) for all \(c \in C\). A maximal element of \(S\) is \(m \in S\) such that \(m \leq x\) implies \(m = x\).

Lemma. Let \(R\) be a commutative ring. If \(1 \neq 0\) in \(R\), then there exists an ideal \(M \subseteq R\) such that \(R/M\) is a field.

Proof. Let \(S\) be the collection of all proper ideals of \(R\). It is important to note that an ideal \(I \subseteq R\) is proper (i.e., \(I \neq R\)) iff \(1 \notin I\). The set \(S\) has an ordering by subset inclusion \(\subseteq\).

I’ll use Zorn’s lemma to show that \(S\) has at least one maximal element (called a maximal ideal of \(R\)), then I’ll show that for any such maximal ideal, \(R/M\) is a field.

Zorn’s Lemma (1). The set \(S\) is non-empty, since \((0) \in S\) (because of the hypothesis that \(1 \neq 0\) in \(R\)).

Zorn’s Lemma (2). Let \(C \subseteq S\) be a non-empty chain in \(S\), and let \(U = \bigcup_{I \in C} I\). It is easy to see that \(U\) is an ideal: if \(x_1, x_2 \in U\) and \(a_1, a_2 \in R\), then \(x_1 \in I_1, x_2 \in I_2\) for some \(I_1, I_2 \in C\). Since \(C\) is a chain, either \(I_1 \subseteq I_2\) or \(I_2 \subseteq I_1\). Thus \(a_1x_1 + a_2x_2 \in I_k \subseteq U\), where \(I_k\) is the larger of \(I_1, I_2\).

We know each \(I \in C\) is a proper ideal in \(R\), so \(1 \notin I\) for all \(I \in C\). Therefore \(1 \notin U = \bigcup_{I \in C} I\), so \(U\) is a proper ideal of \(R\). Thus \(U \in S\), so \(U\) is an upper bound for the chain \(C\) in \(S\).

Thus Zorn’s lemma applies, and tells us there exists a maximal ideal \(M \in S\).

I claim that \(R/M\) is a field. Since it is a commutative ring and clearly \(0 \neq 1\) in \(R/M\) (since \(1 \notin M\)) I just need to produce multiplicative inverses of non-zero elements. Let \(\overline{a} \in R/M\) which is not \(0\). This is represented by an element \(c \in R \setminus M\). Let \(N = (M, c)\) the ideal generated by \(M \cup \{c\}\) in \(R\). Maximality of \(M\) in \(S\) and the fact that \(M \subseteq N\) implies that \(N = R\). Therefore \(1 \in N = (M, c)\), so there exist \(m_1, \ldots, m_k \in M, a_1, \ldots, a_k, b \in R\) such that

\[1 = a_1m_1 + \cdots + a_km_k + bc.\]

Modulo \(M\) this becomes the identity \(1 = b\overline{a}\) in \(R/M\). Thus \(b\) is a multiplicative inverse of \(\overline{a}\).

Using this, we can adjoin roots from a set of polynomials simultaneously. The polynomials don’t even need to be irreducible.

Example. Let \(f_1, \ldots, f_k \in F[X]\) be a set of polynomials of positive degree.

Let \(P := F[X_1, \ldots, X_k]\), and consider the ideal \(I = (f_1(X_1), \ldots, f_k(X_k))\). Note that \(1 \notin I\) for degree reasons. Let \(R := P/I\) be the quotient ring, and note that \(1 \neq 0\) in \(R\).

The ring \(R\) is constructed to have the property that each \(f_i\) “has a root” in \(R\), namely \([X_i] \in R\), the image of \(X_i\) under the projection \(P \to P/I = R\). Also there is an obvious homomorphism\( F \to R\). However, \(R\) might not be a field. The above lemma tells us that there is an ideal \(M \subset R\) such that \(K := R/M\) is a field. Then we have a field extension \(F \to K\), such that each \(f_i\) has a root \(\alpha_i \in K\), namely as the image of \(X_i\).

Exercise. Consider \(f_1 = X^2 + 1, f_2 = X^2 + 4 \in \mathbb{Q}[X]\). Then \(R = \mathbb{Q}[X_1, X_2]/(X_1^2 + 1, X_2^2 + 4)\). Find all ideals \(M \subset R\) such that \(R/M\) is a field. (Hint: find all possible ring homomorphisms \(R \to \mathbb{C}\).)

Lemma. Let \(F\) be a field. Then there exists a field extension \(F \to K\) such that every \(f \in \text{Irred}(F)\) has a root in \(K\).

Proof. Write \(C = \text{Irred}(F)\). Form the infinitely generated polynomial ring

\[P := F[X_f, f \in C].\]
Elements of $P$ are polynomial expressions in finitely many of the variables $X_f$. (Polynomials are always finite expressions. In this ring, we have possibly infinitely many variables to choose from, but only finitely many can appear in any element.)

Let $I \subseteq F$ be the ideal generated by $\{f(X_f)\}_{f \in C}$. (Each $f$ gets a polynomial $f(X_f)$ in its own personal variable $X_f$!) Let $R := P/I$ be the quotient ring. Note that $1 \notin I$ for degree reasons, and that there is an obvious homomorphism $F \to R$.

Note: every $f \in C$ “has a root” in $R$ by construction, namely the element $[X_f]$ (image of $X_f \in P$). The only problem is that $R$ is not necessarily a field. Apply the above lemma to find $M \subseteq R$ so that $K := R/M$ is a field. There is an evident homomorphism $F \to K$, and every $f \in C$ has a root in $K$, namely $\alpha_f := [X_f]$. □

Proposition. Every field $F$ has an algebraic closure.

Proof. Form a sequence $F = K_0 \to K_1 \to K_2 \to \cdots$, where each $K_{n-1} \to K_n$ is a field extension such that every $f \in \text{Irred}(K_{n-1})$ has a root in $K_n$; such exists by the previous lemma. Let $L = \bigcup_{n=1}^\infty K_n$. It is easy to show that every $f \in F[X]$ splits over $L$: if $f$ factors as $f = g_1 \cdots g_r$ over $K_n$ with $g_i$ irreducible over $K_n$, then for each $i$ either $g_i$ is linear, or $g_i$ factors non-trivially over $K_{n+1}$.

The subfield $\Omega \subseteq L$ of elements which are algebraic over $F$ is the desired algebraic closure. (Actually, you can show that $L : F$ is algebraic, so $\Omega = L$.)

64. Non-finite Galois Extensions

Recall:

- $K : F$ is an algebraic extension if every $\alpha \in K$ is the root of some non-zero $f \in F[X]$.
- $K : F$ is a normal extension if it is algebraic and if every $f \in \text{Irred}(F)$ which has a root in $K$ splits over $K$.
- $K : F$ is a separable extension if it is an algebraic extension and if every $f \in \text{Irred}(F)$ which has a root in $K$ is separable.

These definitions apply to infinite extensions. We can create interesting examples of infinite extensions of $F$ by starting with some large extension $C : F$, and taking composites of infinite families of finite extensions of $F$ in $C$.

In fact, suppose $\{K_i\}$ is a family of subfields of $C$ which all contain $F$, and is such that for every pair $K_i, K_j$ in the family, there exists a $K_k$ such that $K_i \cup K_j \subseteq K_k$. Then the union of subsets $\Omega := \bigcup_i K_i \subseteq C$ is itself a subfield of $C$. (This is just because the composite field $K_i K_j \subseteq \Omega$ for every pair of subfields, so sums and products of arbitrary elements of the union are in the union.)

If each $K_i : F$ in the family is algebraic/normal/separable, then so is $\Omega : F$.

Say $\Omega : F$ is a Galois extension if it is normal and separable (but not necessarily finite). Thus if $\Omega$ is a union of a family of subfields as above which are each Galois extensions of $F$, then so is $\Omega : F$. Its Galois group is the automorphism group $G = \text{Aut}(\Omega : F)$.

Examples of Galois extensions over $\mathbb{Q}$ include:

- the algebraic closure $\mathbb{Q}^{\text{alg}} : \mathbb{Q}$,
- the maximal radical extension $\mathbb{Q}^{\text{rad}} : \mathbb{Q}$ (the union of all finite radical Galois extensions over $\mathbb{Q}$),
- the maximal 2-radical extension $\mathbb{Q}^{2-\text{rad}} : \mathbb{Q}$ (the union of all 2-radical Galois extensions over $\mathbb{Q}$, which is precisely the set of constructable numbers),
- the maximal abelian extension $\mathbb{Q}^{\text{ab}} : \mathbb{Q}$ (the union of all finite Galois extensions $L : \mathbb{Q}$ with abelian Galois group),
• the maximal cyclotomic extension $\mathbb{Q}^{cyc}$: $\mathbb{Q}$ (the union of all $\mathbb{Q}(\zeta_n)$; by the Kronecker-Weber theorem this is equal to $\mathbb{Q}^{ab}$).

**Example** (Maximal quadratic extension of $\mathbb{Q}$). Let $\Omega := \mathbb{Q}(\sqrt{c}, \ c \in \mathbb{Q})$, the field obtained by adjoining square roots of all rational numbers. We have $\Omega = \bigcup \mathbb{Q}(\sqrt{S})$, where $S \subset \mathbb{Q}$ ranges over the finite subsets of $\mathbb{Q}$. Therefore $\Omega : \mathbb{Q}$ is an infinite Galois extension, since each $\mathbb{Q}(\sqrt{S}) : \mathbb{Q}$ is a Galois extension, being a splitting field of $\prod_{c \in S}(X^2 - c)$.

Every rational number $c$ can be written $c = \pm p_1 \cdots p_k a^2$, where $a \in \mathbb{Q}$ and $p_1, \ldots, p_k$ are distinct prime integers. Thus we can also write

$$\Omega = \mathbb{Q}(\sqrt{P}), \quad P = \{-1\} \cup \{ p \in \mathbb{Z}_{>0} \mid p \text{ prime} \}.$$ 

Recall that if $S \subseteq P$ is a finite subset of size $k$, then $[\mathbb{Q}(\sqrt{S}) : \mathbb{Q}] = 2^k$. (This is a consequence of Exercise 6.14 in Stewart.)

Now I'll describe the Galois group $G = \text{Aut}(\Omega : \mathbb{Q})$, by constructing an isomorphism $\phi : G \cong \prod_{p \in P} \{\pm 1\}$,

where the right-hand side is a group by componentwise multiplication: $(a_p)(b_p) = (a_pb_p)$.

For each $p \in P$ define a function $\phi_p : G \to \{\pm 1\}$ by the formula

$$\sigma(\sqrt{p}) = \phi_p(\sigma)\sqrt{p}.$$ 

(It doesn’t matter which square root you use, as long as you use the same one on both sides.) Since $\sigma(\sqrt{p}) = \sigma(\phi_p(\sqrt{p})) = \phi_p(\sigma)\sqrt{p}$, we see that $\phi_p$ is a group homomorphism. They fit together to give a homomorphism $\phi : G \to \prod_{p \in P}\{\pm 1\}$, by $\phi(\sigma) := (\phi_p(\sigma)) \in \prod_{p \in P}\{\pm 1\}$.

The homomorphism $\phi$ is clearly injective, since $\Omega$ is generated by $\sqrt{P}$.

To show $\phi$ is surjective, note that the same idea produces injective homomorphisms $\phi_S := (\phi_s)_{s \in S} : \text{Aut}(\mathbb{Q}(\sqrt{S}) : \mathbb{Q}) \to \prod_{s \in S} \{\pm 1\}$, for each finite subset $S \subseteq P$. Furthermore, since $[\mathbb{Q}(\sqrt{S}) : \mathbb{Q}] = 2|S| = |\prod_{s \in S}\{\pm 1\}|$, it must also be surjective.

This isomorphism gives us the description of the entire subfield lattice of each finite extension $\mathbb{Q}(\sqrt{S}) : \mathbb{Q}$. For instance, for any $T \subseteq S$, we see that $H_T := \text{Aut}(\mathbb{Q}(\sqrt{S}) : \mathbb{Q}(\sqrt{T})) \cong \{ (a_s)_{s \in S} \mid a_s = 1 \text{ if } s \in T \}$.

In particular, if $A, B \subseteq S$ this tells us that $H_{A \cap B} = H_A H_B$, and therefore

$$\mathbb{Q}(\sqrt{A \cap B}) = \mathbb{Q}(\sqrt{A}) \cap \mathbb{Q}(\sqrt{B}).$$

Now to show that $\phi : G \to \prod_{p \in P}\{\pm 1\}$ is surjective, suppose given elements $a_p \in \{\pm 1\}$ for each $p \in P$. I want to produce $\sigma \in G$ such that $\sigma(\sqrt{p}) = a_p\sqrt{p}$. Define this by $\sigma(\alpha) = \sigma_S(\alpha)$ whenever $\alpha \in \mathbb{Q}(\sqrt{S})$. This is well-defined because $\Omega = \bigcup \mathbb{Q}(\sqrt{S})$, and because $\sigma_S$ and $\sigma_T$ agree on $\mathbb{Q}(\sqrt{S}) \cap \mathbb{Q}(\sqrt{T}) = \mathbb{Q}(\sqrt{S \cap T})$.

The following gives a general way to describe elements of an infinite Galois group in terms of finite Galois groups, an instance of which appeared in the previous example.

**Lemma.** Let $\Omega : F$ be a Galois extension, and let $\{L_i\}_{i \in I}$ be a collection of intermediate fields such that

1. each $L_i : F$ is finite Galois,
2. $\Omega = \bigcup_i L_i$, and
3. for any pair $L_i, L_j$ in the family, the intersection $L_i \cap L_j$ is also in the family.
Then there is a bijection between $G$ and the set
\[ G' = \{ (g_i) \in \prod_{i \in I} \text{Aut}(L_i : F) \mid L_i \subseteq L_j \text{ implies } g_j|L_i = g_i \}, \]
defined by $g \mapsto (g|L_i)$. This bijection is an isomorphism of groups, where $G'$ is given a group structure by componentwise multiplication: $(g_i)(h_i) = (g_i h_i)$.

**Proof.** Because each $L_i : F$ is normal, each $g \in G$ satisfies $g(L_i) = L_i$, so $g|L_i \in \text{Aut}(L_i : F)$.

Because $\Omega = \bigcup_i L_i$, any $g \in G$ is uniquely determined by its restrictions to all $L_i$, so $G \to G'$ is injective.

Conversely, given $(g_i) \in G'$, define $g \in G$ by $g(\alpha) = g_i(\alpha)$ if $\alpha \in L_i$. This is well-defined, since if $\alpha \in L_i \cap L_j$, then we know that $g_i|L_i \cap L_j = g_j|L_i \cap L_j$ so $g_i(\alpha) = g_j(\alpha)$.

$\square$

**Example (Algebraic closure of $\mathbb{F}_p$).** Let $\Omega : F = \mathbb{F}_p : \mathbb{F}_p$. Consider the collection $\{ \mathbb{F}_{p^n} \}$ of all finite subfields. We know that $\Omega = \bigcup \mathbb{F}_{p^n}$, and that the collection is closed under intersection.

For each $n$ we have an isomorphism
\[ \mathbb{Z}/n \rightarrow \text{Aut}(\mathbb{F}_{p^n} : \mathbb{F}_p), \quad k \mapsto \phi^k. \]

Furthermore, whenever $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ (i.e., when $m \mid n$), these isomorphisms are compatible with the obvious projections:
\[
\begin{array}{ccc}
\mathbb{Z}/n & \cong & \text{Aut}(\mathbb{F}_{p^n} : \mathbb{F}_p) \\
[x]_n & \mapsto & \phi^k \\
\mathbb{Z}/m & \rightarrow & \text{Aut}(\mathbb{F}_{p^m} : \mathbb{F}_p)
\end{array}
\]

So $G = \text{Aut}(\mathbb{F}_p : \mathbb{F}_p)$ is isomorphic to the group $\widehat{\mathbb{Z}}$, defined as the set of tuples
\[ \{ (a_n) \in \prod_{n \in \mathbb{Z}_{>0}} \mathbb{Z}/n \mid a_n \equiv a_m \mod m \text{ whenever } m \mid n \}, \]

with group law defined by componentwise addition. This is called the group of **profinite integers**. For instance, $G$ contains an element of infinite order, namely the Frobenius $\phi(x) = x^p$ on $\Omega$, which corresponds to the tuple $(a_n) \in \widehat{\mathbb{Z}}$ with $a_n = 1$ for all $n$.

There exist elements of $G$ which are not in $\langle \phi \rangle$. For instance, there exists $\sigma \in G$ such that $\sigma|\mathbb{F}_{p^k} = \phi$, but $\sigma|\mathbb{F}_{p^{2k}} \text{id}$ whenever $m$ is odd. This corresponds to the unique tuple $(a_n) \in \widehat{\mathbb{Z}}$, such that, for $n = 2^k m$ with $m$ odd, $a_n \in \mathbb{Z}/n$ satisfies $a_n \equiv 1 \mod 2^k$ and $a_m \equiv 0 \mod m$ (using the isomorphism $\mathbb{Z}/n \cong \mathbb{Z}/2^k \times \mathbb{Z}/m$.)

**Example (Cyclotomic extension of $\mathbb{Q}$).** There is an isomorphism of groups
\[ \text{Aut}(\mathbb{Q}^{\text{cyc}} : \mathbb{Q}) \cong \widehat{\mathbb{Z}}^\times, \]

where the right-hand side is the set of tuples
\[ \{ (a_n) \in \prod_{n \in \mathbb{Z}_{>0}} (\mathbb{Z}/n)^\times \mid a_n \equiv a_m \mod m \text{ whenever } m \mid n \}, \]

with group law defined by componentwise multiplication. This is called the group of **profinite units**. The isomorphism sends $\sigma \in G = \text{Aut}(\mathbb{Q}^{\text{cyc}} : \mathbb{Q})$ to the tuple $(a_n)$, with the property that $\sigma|\mathbb{Q}(\zeta_n) = \sigma_{a_n}$. That is, $\sigma(\zeta_n) = \zeta_{a_n}^n$ for all $n$.

An infinite extension $\Omega : F$ can in principle have $F$-homomorphisms $\Omega \to \Omega$ which are not isomorphisms. But this not happen if the extension is normal.
Lemma. Let $\Omega : F$ be a normal extension (not necessarily finite). Then every $F$-homomorphism $\phi : \Omega \rightarrow \Omega$ is an isomorphism.

Proof. We know that $\phi$ is injective, so we just have to show it is surjective. Consider $a \in \Omega$. Since $\Omega : F$ is algebraic, there is a minimal polynomial $f = f_{a/F} \in \text{Irred}(F)$, which splits over $\Omega$ since the extension is normal. An $F$-homomorphism $\phi$ must send the set of roots $R = \{ \beta \in \Omega \mid f(\beta) = 0 \}$ of $f$ to itself. Since $\phi$ is injective and $R$ is finite, $\phi$ must induce a bijection $R \rightarrow R$. Therefore $\phi$ is in the image of $\phi$ since $a \in R$.

Consider an intermediate field $L$ of $\Omega : F$ such that $L : F$ is finite Galois. Because $L : F$ is normal, any $\phi \in G$ must satisfy $\phi(L) = L$. Thus we get a group homomorphism $G \rightarrow \text{Aut}(L : F)$, $\phi \mapsto \phi|L$

defined by restricting an automorphism of $\Omega$ to the subfield $L$.

The following result is crucial: it relies on Zorn’s lemma.

Lemma. Let $\Omega : F$ be a normal extension (not necessarily finite), and $K$ any intermediate field (not necessarily finite). Then for any $F$-homomorphism $\phi : K \rightarrow \Omega$, there exists an isomorphism $\overline{\phi} : \Omega \rightarrow \Omega$ such that $\overline{\phi}|K = \phi$.

Proof. First observe that by the previous lemma, it suffices to construct a homomorphism $\overline{\phi}$ such that $\overline{\phi}|K = \phi$, since it will necessarily be an isomorphism.

To construct a homomorphism, we use Zorn’s lemma. Let $S$ be the collection of pairs $(L, \psi)$, where $L$ is an intermediate field containing $K$, and $\psi : L \rightarrow \Omega$ is a homomorphism such that $\psi|K = \phi$. The set $S$ has a partial order defined by

$$(L, \psi) \leq (L', \psi') \iff L \subseteq L', \psi|L = \psi.$$  

The set $S$ is non-empty, since $(K, \phi) \in S$. If $C \subseteq S$ is a chain, define $L_C := \bigcup_{(L, \psi) \in C} L$ and let $\psi_U : L_C \rightarrow \Omega$ be the unique function such that $\psi_U|L = \psi$ for each $(L, \psi) \in C$. Then $L_C$ is a subfield and $\psi_U$ is a homomorphism extending $\psi$. Thus $(L_U, \psi_U) \in S$ is an upper bound of $C$.

Zorn’s lemma applies to give a maximal element $(L_M, \psi_M)$ of $S$. To finish the proof, I need to show that $L_M = \Omega$.

I suppose $L_M \neq \Omega$ and derive a contradiction. Then there exists $\alpha \in \Omega \setminus L_M$. I claim there exists a homomorphism $\psi : L_M(\alpha) \rightarrow \Omega$ extending $\psi_M$, by the same argument we used for finite extensions. That is, such an extension corresponds to a choice of root $\beta \in \Omega$ of $f' = \psi_M(f)$ where $f = f_{\alpha/L_M}$, so it suffices to show that $f'$ has a root in $\Omega$. Since $\Omega : F$ is normal, there is a minimal polynomial $g = f_{a/F}$ and $g$ splits over $\Omega$, and thus $f \mid g$ in $L_M[X]$ and thus $f' \mid \phi(g) = g \in \Omega[X]$, so $f'$ splits over $\Omega$.

The argument of the previous paragraph contradicts the maximality of $(L_M, \psi_M)$ is $S$. Thus we must have $L_M = \Omega$, so $\psi_M : \Omega \rightarrow \Omega$ is the desired extension of $\psi$. □

In particular we have, for each $L \in \mathcal{F}$, a surjective homomorphism $g \mapsto g|L : G \rightarrow \text{Aut}(L : F)$.

We note the following consequence.

Corollary. Let $\Omega : F$ be a Galois extension (not necessarily finite), and $L$ an intermediate field of $\Omega : F$ such that $L : F$ is normal. Then restriction $g \mapsto g|L$ defines an isomorphism of groups $G/G_L \sim \rightarrow \text{Aut}(L : F)$, where $G_L := \text{Aut}(\Omega : L) \leq G = \text{Aut}(\Omega : F)$.

Proof. By the previous lemma, any $\phi : L \rightarrow L \subseteq \Omega$ extends to an automorphism of $\Omega$, which exactly means that the restriction map $G \rightarrow \text{Aut}(L : F)$ (which is defined because $L : F$ is normal) is surjective. The claim follows by the isomorphism theorem for groups, since the kernel of the restriction map is exactly $G_L$. □
65. Galois correspondence for general Galois extensions

The Galois correspondence will relate intermediate field of a Galois extension $\Omega : F$ with certain subgroups of $G = \text{Aut}(\Omega : F)$, called closed subgroups.

Let $\Omega : F$ be a (possibly infinite) Galois extension, and let $G = \text{Aut}(\Omega : F)$ be its automorphism group. Let $\mathcal{F} = \{L\}$ be the collection of all intermediate fields $L$ such that $[L : F] < \infty$ and $L : F$ is normal. (I.e., such that $L$ is a finite Galois extension.) Note that if $g \in G$, then $g|L$ is an element of $\text{Aut}(L : F)$, since $L : F$ is a normal extension.

Given a subset $S \subseteq G$, define the closure of $S$ to be

$$\overline{S} := \{ g \in G \mid \forall L \in \mathcal{F}, \exists s \in S, g|L = s|L \}.$$ 

That is, $g \in \overline{S}$ if for every finite Galois intermediate extension $L : F$, $g$ acts on $L$ exactly the same as some element of $S$ (which need not be unique, and may be different for different $L$).

Say that a subset $S \subseteq G$ is closed if $S = \overline{S}$.

**Proposition.** For subsets $S, T$ of $G$ we have

1. $S \subseteq \overline{S}$,
2. if $S \subseteq T$ then $\overline{S} \subseteq \overline{T}$, and
3. $\overline{\overline{S}} = \overline{S}$.

As a consequence, $\overline{S}$ is a closed set, and is the smallest closed set containing $S$.

**Proof.** (1) and (2) are immediate from the definition of closure.

To prove (3), note that $\overline{\overline{S}} \subseteq \overline{S}$ is immediate from (1) and (2), so we just have to prove: $g \in \overline{S}$ implies $g \in \overline{\overline{S}}$.

Suppose $g \in \overline{S}$, and suppose $L \in \mathcal{F}$. Then there exists $s \in S$ such that $g|L = s|L$. But since $s \in \overline{S}$, there must exist $t \in S$ such that $s|L = t|L$. Thus $g|L = t|L$ for some $t \in S$. This proves that $g \in \overline{S}$, as desired.

For the final claim, note that (3) implies that $\overline{S}$ is closed. Whenever $S \subseteq T$ with $T$ closed, we have $S \subseteq \overline{S} \subseteq \overline{T} = T$ (using (1), (2), and (3)), so $\overline{S}$ is a closed set containing $S$, but contained in every closed set containing $S$. \qed

A subgroup $H \leq G$ is closed if it is closed as a subset.

**Example.** If $\Omega : F$ is a finite extension, then every subset of $G$ is closed, since $g \in \overline{S}$ in particular implies there exists $s \in S$ such that $g|\Omega = s|\Omega$, i.e., that $g = s$, so $g \in S$.

**Example.** Not every subgroup of $G$ is closed. For instance, consider $\Omega : F = F_p : \mathbb{F}_p$. Then the cyclic subgroup $\langle \phi \rangle \leq G$ generated by the Frobenius map $\phi : \mathbb{F}_p \to \mathbb{F}_p$ is not a closed subgroup. In fact, we know that $\langle \phi \rangle = G$, since each $\text{Aut}(\mathbb{F}_{p^n}, \mathbb{F}_p)$ is generated as a group by $\phi|_{\mathbb{F}_{p^n}}$, but $\langle \phi \rangle \neq G$.

**Lemma.** Let $K$ be any intermediate field of $\Omega : F$. Then $G_K = \text{Aut}(\Omega : K)$ is a closed subgroup of $G$.

**Proof.** We use the following observation: $\Omega = \bigcup_{L \in \mathcal{F}} L$, and thus

$$K = \bigcup_{L \in \mathcal{F}} L \cap K.$$ 

I need to show that $g \in G_K$ implies $g \in G_K$, i.e., that $g|K = \text{id}_K$. By the above remark it suffices to show $g|L \cap K = \text{id}_{L \cap K}$ for all $L \in \mathcal{F}$. Since $g \in G_K$, we know that for all $L \in \mathcal{F}$ there exists $h \in G_K$ such that $g|L = h|L$, and therefore $g|L \cap K = h|L \cap K = \text{id}_{L \cap K}$ since $h \in G_K$. \qed
Theorem (Galois correspondence for infinite extensions). There is a bijective correspondence
\[
\{ \text{closed subgroups } H \leq G \} \longleftrightarrow \{ \text{intermediate fields } K \text{ of } \Omega : F \},
\]
given by \( H \mapsto \Omega^H \) and \( K \mapsto G_K := \text{Aut}(\Omega : K) \).

Proof. Using the lemma, we see that both functions \( H \mapsto \Omega^H \) and \( K \mapsto G_K \) are well-defined. We thus need to show that \( H = G_{\Omega^H} \) and \( K = \Omega^{G_K} \).

(1). Consider an intermediate field \( K \). We clearly have \( K \subseteq \Omega^{G_K} \). To show equality, suppose that instead there is \( \alpha \in \Omega^{G_K} \setminus K \). Then \( d := [K(\alpha) : K] \geq 2 \). Because \( \Omega : K \) is normal and separable, we know that there are exactly \( d \) distinct \( K \)-homomorphisms \( \psi : K(\alpha) \to \Omega \) (corresponding to roots of the minimal polynomial \( f_{\alpha/K} \in \text{Irred}(K) \), which has degree \( d \)).

Since \( d \geq 2 \) there exists at least one such \( \psi \) with \( \psi(\alpha) \neq \alpha \). We proved earlier that any \( F \)-homomorphism \( \psi \) extends to an element \( g \in G \), which is necessarily in \( G_K \) since \( g|K = \psi|K = \text{id}_K \). But since \( g(\alpha) \neq \alpha \) we have \( \alpha \notin \Omega^{G_K} \), contradicting our hypothesis on \( \alpha \).

(2). Consider a subgroup \( H \leq G \). Let \( K := \Omega^H \). Then \( G_K = \text{Aut}(\Omega : K) \) is a closed subgroup, and we clearly have \( H \leq G_K \). Since \( H \) is closed so \( H = \overline{H} \), to show \( G_K = H \) it suffices to show that \( g \in G_K \) implies \( g \in \overline{H} \), i.e., that for any \( L \in \mathcal{F} \) there exists \( h \in H \) such that \( g|L = h|L \).

Note that restriction defines an isomorphism \( G/G_L \cong \text{Aut}(L : F) \), which has degree \( d \) a subgroup, whose fixed field is exactly \( \Omega^{G_L} = L \cap \Omega \), and by the Galois correspondence for finite Galois extensions we know that \( \text{Aut}(L : L \cap K) = H \cap G_L \). For \( g \in G_K \) we have that \( g|L \in \text{Aut}(L : L \cap K) \), so \( g|L \) corresponds to an element of \( H \cap G_L \). That is, \( g = h \alpha \) for some \( h \in H \) and \( \alpha \in G_L \), and therefore \( g|L = h|L \) as desired.

\[ \square \]

Remark. The proof actually shows that the operation which takes a subgroup \( H \leq G \) to \( G_{\Omega^H} \) is equal to the closure operation \( H \mapsto \overline{H} \).

Proposition. Let \( K \) be an intermediate field of the Galois extension \( \Omega : F \), and let \( G_K = \text{Aut}(\Omega : F) \leq G \) be its corresponding closed subgroup. Then \( K : F \) is normal iff \( G_K \) is normal in \( G \), and if so then restriction defines an isomorphism of groups \( G/G_K \cong \text{Aut}(K : F) \).

Proof. If \( K : F \) is normal, then any \( g \in G \) satisfies \( g(K) \subseteq K \), by the usual proof: any \( \alpha \in K \) is the root of some \( f \in \text{Irred}(F) \) which splits over \( K \), and \( g \) permutes the roots of \( f \). Thus \( g \) restricts to an \( F \)-homomorphism \( K \to K \), which must be an isomorphism because \( K : F \) is normal (as proved earlier).

Now if \( \sigma \in G_K \) and \( g \in G \), we check easily that \( g\sigma g^{-1} \in G_K \), since \( g^{-1}(K) = K \). So \( G_K \) is normal.

Conversely suppose \( G_K \) is normal, and consider any \( \alpha \in K \). We see that \( g(\alpha) \) is fixed by \( G_K \), since \( G_K g(\alpha) = gG_K g^{-1}(\alpha) = gG_K(\alpha) = g(\alpha) \). Thus \( g(\alpha) \in K \) by the Galois correspondence. Since the Galois group \( G \) permutes all roots of \( f = f_{\alpha/F} \in \text{Irred}(F) \), we conclude that \( f \) splits over \( K \).\[ \square \]

66. The Galois group as a topological group

This statement of the Galois correspondence is not entirely satisfactory, since it uses the notion of a closed subgroup of \( G \), which itself is defined in terms of the finite subextensions of \( \Omega : F \). However, it turns out that the datum of “closed subsets” exactly determine a topology on \( G \), and makes \( G \) into a topological group.

We say that a subset \( U \subseteq G \) is open if its complement \( G \setminus U \) is closed.

Lemma. Let \( U \subseteq G \) be a subset. The following are equivalent.

(1) \( U \) is open.
(2) For all \( a \in U \) there exists \( L \in \mathcal{F} \) such that \( aG_L \subseteq U \).

\[ \text{open subset} \]
(3) \[ U = \bigcup_{a \in G, L \in F} aG_L. \]

(4) For all \( g \in U \) there exist \( a \in G, L \in F \) such that \( g \in aG_L \subseteq U \).

**Proof.** (1) \( \iff \) (2). This is immediate from the definition of closed subset. The set \( U \) is open (i.e., \( G \setminus U \) is closed) by definition iff \( a \notin \overline{G \setminus U} \) for all \( a \in U \), i.e., iff for all \( a \in U \) there exists \( L \in F \) such that \( aL \notin (G \setminus U)L \). The collection of elements \( g \) of \( G \) such that \( aL = gL \) is exactly the set \( aG_L \), so this condition says that \( aG_L \cap (G \setminus U) = \emptyset \), or equivalently that \( aG_L \subseteq U \).

(2) \( \iff \) (3) is true tautologically, as is (3) \( \iff \) (4). \( \square \)

**Example.** An open subgroup \( H \leq G \) necessarily contains \( eG_L = G_L \) for some \( L \in F \). The isomorphism \( G/G_L \approx \text{Aut}(L:F) \) and the Galois correspondence for finite extensions, applied to the subgroup \( H G_L/G_L \leq G/G_L \), implies that \( H = G_K \) for a subfield \( K \subseteq L \).

Conversely, any \( G_K \) for a finite extension \( K : F \) is an open subgroup of \( G \).

These open \( G_K \) always have finite index in \( G \). However, it is not the case that finite index subgroups of \( G \) are always open. See Milne, *Fields and Galois Theory*.

We call the \( aG_L \) (as \( a \in G \) and \( L \in F \)) the **basic open sets**. A consequence is any subset which is a union of basic open sets is open.

A **topology** on a set \( X \) is a collection \( \mathcal{O} \) of subsets of \( X \) (called **open subsets**), with the properties that

1. \( \emptyset, X \) are open subsets,
2. If \( \{U_i\} \) is a collection of open subsets, so is \( \bigcup U_i \),
3. If \( U, V \) are open subsets, so is \( U \cap V \).

**Example.** \( \mathbb{R}^n \) has a topology, where the open subsets are exactly the unions of subsets of the form \( B_\varepsilon(x) = \{y \in \mathbb{R}^n \mid |x - y| < \varepsilon\} \).

**Proposition.**

1. \( \emptyset \) and \( G \) are open subsets of \( G \).
2. If \( \{U_i\} \) is a collection of open subsets, so is \( \bigcup U_i \).
3. If \( U, V \) are open subsets, so is \( U \cap V \).

In other words, the open subsets of \( G \) define a topology on \( G \), called the **Krull topology**.

**Proof.** (1) and (2) are straightforward. To prove (3), suppose \( g \in U \cap V \). Then there exist \( a, b \in G \) and \( L, M \in F \) such that \( g \in aG_L \subseteq U \) and \( g \in bG_M \subseteq V \). Since \( gG_L = aG_L \) and \( gG_M = bG_M \) (basic property of cosets), we have that \( gG_L \subseteq U \) and \( gG_M \subseteq V \). Let \( LM \in F \) be the composite extension, which is also finite Galois, so that \( G_LM = G_L \cap G_M \). Then \( gG_L \subseteq U \cap V \). \( \square \)

A function \( f : X \to Y \) between two topological spaces is **continuous** if \( f^{-1}(U) \subseteq X \) is open whenever \( U \subseteq Y \) is open.

**Proposition.** **With respect to the Krull topology, multiplication and inverse are continuous maps.**

**Proof.** To show that multiplication \( \mu : G \times G \to G \), we need the topology on \( G \times G \), which is the **product topology**: open subsets of \( G \times G \) are unions of subsets of the form \( a_1G_{L_1} \times a_2G_{L_2} \), with \( a_1, a_2 \in G \) and \( L_1, L_2 \in F \).

To show \( \mu \) is continuous, I need to show that for any \( bG_L \subseteq G \) with \( L \in F \), the preimage \( \mu^{-1}(bG_L) \) is open in \( G \times G \). That is, given \( (a_1, a_2) \in \mu^{-1}(bG_L) \), it suffices to find \( L_1, L_2 \in F \) such that \( aG_{L_1} \times aG_{L_2} \subseteq \mu^{-1}(bG_L) \). In fact, take \( L_1 = L_2 = L \), so \[ \mu(a_1G_L \times a_2G_L) = a_1G_La_2G_L = a_1a_2G_L \subseteq a_1a_2G_L = bG_L, \]
using that $G_L \leq G$ is normal so $G_L a_2 = a_2 G_L$, and that $a_1 a_2 \in b G_L$.

The proof that inverse is continuous is similar.  \hfill \Box

\textsc{Department of Mathematics, University of Illinois, Urbana, IL}

\textit{E-mail address:} rezk@illinois.edu