By the way, have we discussed:

**Example** Consider \( \mathbb{Z}[\sqrt{5}] = \{a+b\sqrt{5} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C} \).

This is a subring of \( \mathbb{C} \). Note that

\[(1+\sqrt{5})(1-\sqrt{5}) = 1 - (\sqrt{5})^2 = 6 = 2 \cdot 3.\]

If \( a+b\sqrt{5} \in \mathbb{Z}[\sqrt{5}] \), then

\[|a+b\sqrt{5}|^2 \text{ (its norm squared as a complex number) satisfies}\]

\[|a+b\sqrt{5}|^2 = (a+b\sqrt{5})(a-b\sqrt{5}) = a^2 + 5b^2.\]

If \( z = a+b\sqrt{5} \in \mathbb{Z}[\sqrt{5}] \) and \( z = w_1w_2 \), \( w_1, w_2 \in \mathbb{Z}[\sqrt{5}] \), then \( |z|^2 = |w_1|^2 |w_2|^2 \). Now

\[|1+\sqrt{5}|^2 = |1-\sqrt{5}|^2 = 6, \quad 121^2 = 4, \quad 131^2 = 9.\]

For each of these possible choices of \( z \), since \( |z|^2 < 10 \), we find that \( z = w_1w_2 \) implies that either (a) one of \( w_1, w_2 \) is a unit [satisfies \( |w_i|^2 = 1 \)], or

(b) both \( w_1, w_2 \in \mathbb{Z} \).

It is immediate that \( 1+\sqrt{5}, 1-\sqrt{5}, 2, 3 \) are irreducible in \( \mathbb{Z}[\sqrt{5}] \). So it is not a UFD.
Remark: We've used again and again:

Prop: A ring $R$ is a domain iff it satisfies the cancellation law: if $ra = rb$ and $r \neq 0$ then $a = b$.

Proof. If $R$ is a domain, $ra = rb$ if and only if $r(a-b) = 0$; since $r \neq 0$, this implies $a-b = 0$, i.e., $a = b$.

Conversely, if $R$ satisfies the cancellation law, suppose $r \in R$ is a nonzero element that satisfies $ra = 0$ for some $a \in R$. Since $r \neq 0$, we conclude that $a = 0$. So $R$ has no nonzero divisors, i.e., it is a domain. $\square$

Def: If $F$ is a subfield of a field $E$, that is, a subring that contains 1 and is itself a field, we say that $E$ is a field extension of $F$; we sometimes write “$E/F$ is a field extension.”

Lemma: Let $E/F$ be a field extension, let $d \in E$, and let $p(x) \in F[x]$ be a monic irreducible polynomial having $\alpha$ as a root. Then

1) $\deg(p) \leq \deg(f)$ for every $f \in F[x]$ having $\alpha$ as a root.

2) $P$ is the only monic polynomial in $F[x]$ of degree $\deg(p)$ having $\alpha$ as a root.
Note Recall that if \( f(x) = \sum_{i=0}^{n} a_i x^i \) and \( a_n \neq 0 \), we say \( f \) is \textit{monic} if \( a_n = 1 \).

Proof of Lemma. Let

\[
I = \{ f \in \mathbb{F}[x] \mid f(0) = 0 \}.
\]

It is easily seen to be an ideal of \( \mathbb{F}[x] \). Since \( \mathbb{F}[x] \) is a PIDs, we have \( I = (p) \) for some \( q \in \mathbb{F}[x] \), and \( p = q \cdot f \) for some \( f \in \mathbb{F}[x] \). If \( \deg(q) < \deg(p) \) then \( \deg(f) \geq 1 \) and \( p \) is not irreducible; so \( \deg(q) \geq \deg(p) \). (1) is then immediate. Since \( \deg(q) \geq \deg(p) \) and \( p \in I \), we must have \( \deg(q) = \deg(p) \) and \( p = q \cdot f \) for some \( f \in \mathbb{F}[x] = \mathbb{F} \setminus \{0\} \). If now \( q \in I \) satisfies \( \deg(q) = \deg(p) \) then \( q = p \cdot c \) for some \( c \in \mathbb{F}[x] \) and \( q \) is monic iff \( c = 1 \), thus proving (2).

\[\square\]

Def The dimension of \( E \) as a vector space over \( F \) is called the degree of \( E \) over \( F \) and written \([E:F]\). An extension \( E/F \) is \textit{finite} if \( E \) is a finite-dimensional \( F \)-vector space.
Theorem: Let $p \in F[x]$ be an irreducible polynomial of degree $d$. Then $E = F[x]/(p(x))$ is a field extension of degree $d$, with basis $\{1, \theta, \theta^2, \ldots, \theta^{d-1}\}$ over $F$ where $\theta$ is a root of $p$.

Proof. Let $E = F[x]/(p)$, as we saw previously, this is an extension field of $F$, and $\theta = x + (p)$ is a root of $p$ in $F$.

Suppose $\{1, \theta, \theta^2, \ldots, \theta^{d-1}\}$ are not linearly independent over $F$, say $c_0, c_1, \ldots, c_{d-1} \in F$ with $\sum_{i=0}^{d-1} c_i \theta^i = 0$. Then $\theta$ is a root of $f(y) = \sum_{i=0}^{d-1} c_i y^i$, a contradiction by the previous lemma since $p$ is irreducible.

but $\deg(f) < \deg(p)$.

Now, given $e = f(x) + (p) \in E = F[x]/(p)$, use the division algorithm to write $f = p \cdot q + r$ with $r = 0$ or $\deg(r) < \deg(p)$.

Then $e = f + (p) = r + (p) \in \text{span} \{1 + (p), x + (p), \ldots, x^{d-1} + (p)\}$, as desired.

So $\{1, \theta, \theta^2, \ldots, \theta^{d-1}\}$ are a linearly independent set spanning $E$. \qed
Def $E/F$ a field extension, $x_1,\ldots,x_n \in E$.

The field obtained by adjoining $x_1,\ldots,x_n$ to $F$, written $F(x_1,\ldots,x_n)$, is the intersection of all subfields of $E$ containing $F \cup \{x_1,\ldots,x_n\}$.

An extension $E/F$ is simple if $E = F(\alpha)$ for some $\alpha \in E$.

**Exercise**

$F(x_1,\ldots,x_n) = \left\{ \frac{f(x_1,\ldots,x_n)}{g(x_1,\ldots,x_n)} \mid f, g \in F[x_1,\ldots,x_n], \text{ } g(x_1,\ldots,x_n) \neq 0 \right\}$.

Note $F[x_1,\ldots,x_n]$ means the sub ring of $E$ generated by $F$ and $\{x_1,\ldots,x_n\}$.

Def $E/F$ a field extension. An element $\alpha \in E$ is algebraic over $F$ if $p(\alpha) = 0$ for some (monic) $p \in F[x]$; otherwise $\alpha$ is transcendental over $F$. An extension $E/F$ is algebraic if every element of $E$ is algebraic over $F$.

Remark The set of all elements of $C$, algebraic over $\mathbb{Q}$, is a subfield of $C$ that is algebraic over $\mathbb{Q}$ but not finite over $\mathbb{Q}$.
Theorem If an extension $E/F$ is finite then it is algebraic.

Proof. Suppose $[E:F] = n$ and $\alpha \in E$. Then $1, \alpha, \alpha^2, \ldots, \alpha^n$ form a linearly dependent set over $F$, i.e. there are $c_0, \ldots, c_n \in F$ not all zero such that $p(\alpha) = 0$ where

$$p(x) = \sum_{i=0}^{n} c_i x^i.$$  

\[\square\]

---

Theorem $E/F$ a field extension, $\alpha \in E$ algebraic over $F$. Then

1) there is a monic irreducible $p(x) \in F[x]$ having $\alpha$ as a root.

2) $F[x]/(p(x)) \cong F(\alpha)$; indeed, the homomorphism

$$F[x] \xrightarrow{\cong} F(\alpha)$$

$p(x) \mapsto p(\alpha)$

factors through an isomorphism

$$\cong: F[x]/(p(x)) \rightarrow F(\alpha).$$

3) $p(x)$ is the unique monic polynomial of least degree in $F[x]$ having $\alpha$ as a root.

4) $[F(\alpha):F] = \deg(p)$.

Proof (1) Since $\alpha$ is algebraic over $F$, there is $f \in F[x]$ with $f(\alpha) = 0$. Factorizing $f = f_1 \cdots f_k$ into irreducibles, at least one of $f_i(\alpha), \ldots, f_k(\alpha)$ must be zero, say $f_i$. Dividing $f_i$ by its leading coefficient makes it monic.
(2) Define $F[x] \overset{\hat{a}}{\longrightarrow} E$ as in the statement of the theorem. Then $\text{Im} \hat{a} = F[x]/\ker \hat{a}$ is a subring of $E$, hence a domain. So $\ker \hat{a}$ is prime. Since $F[x]$ is a PID, this implies $\ker \hat{a} = (p)$ for some irreducible $p \in F[x]$ (which we may assume monic if we choose). By an earlier result, $\text{Im}(\hat{a})$ is then a subfield of $E$ containing $\alpha = \hat{a}(x)$. It's clear from our earlier-stated exercise that $\text{Im}(\hat{a}) \subseteq F(\alpha)$, so in fact the induced homomorphism

$$\hat{a} : F[x]/(p) \longrightarrow F(\alpha) \subseteq E$$

is an isomorphism. (3) and (4) were proven before.

The polynomial $p$ in the theorem is the irreducible polynomial of $\alpha$ over $F$.

**Def.** A splitting field of $f \in F[x]$ is a field extension $E/F$ such that

1) $f$ splits over $E$

2) for any field $K$ such that $F \subseteq K \subseteq E$, $f$ does not split over $K$.

**Theorem.** If $F$ is a field, every $f \in F[x]$ has a splitting field.

**Proof.** Given $f \in F[x]$, Kronecker's Theorem shows that there is $E/F$ such that $f$ splits over $E$. Then, letting $u_1, \ldots, u_n$ be the roots of $f$ in $E$, $F(u_1, \ldots, u_n)$ is a splitting field of $f$. $\square$
Example. You did an exercise to prove that
\[ p(x) = x^4 - 10x^2 + 1 \]
is irreducible over \( \mathbb{Q} \).

Hence, by an earlier theorem,
\[ \mathbb{Q}[x]/(p) \]
is a simple field extension of degree 4 over \( \mathbb{Q} \).

Let's find a root of \( p \) in \( \mathbb{C} \): first let
\[ q(y) = y^2 - 10y + 1 \]. By the quadratic formula we get
\[ y = \frac{5 \pm \sqrt{24}}{2} \]  
\[ = 5 \pm 2\sqrt{6} \].

Now \( p(x) = q(x^2) \), so, for example,
\[ \sqrt{5+2\sqrt{6}} \]
is a root of \( p \). You may check that
\[ (\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6} \]. So \( \alpha = \sqrt{2} + \sqrt{3} \) is a root of \( p \).

Thus, by our earlier theorem,
\[ \mathbb{Q}[x]/(p) \cong \mathbb{Q}(\alpha) \subseteq \mathbb{C}, \text{ via} \]

\[ \mathbb{Q}[x] \]
\[ \begin{array}{c}
\alpha \mapsto \\
\end{array} \]
\[ \mathbb{Q}(\alpha) \]
\[ f(x) \mapsto \tilde{f}(\alpha) = f(\alpha). \]
Lemma. If \( FSBE \) are fields with \( B/F, E/B \) finite, then \( E/F \) is finite and
\[ [E:F] = [E:B][B:F]. \]

Proof. Choose bases \( b_1, \ldots, b_m \) of \( B \) over \( F \) and \( e_1, \ldots, e_n \) of \( E \) over \( B \). We claim that
\[ S = \{ e_i b_j \mid 1 \leq i \leq n, 1 \leq j \leq m \} \]
is a basis of \( E \) over \( F \).

**S is linearly independent.** Suppose \( \sum c_{ij} e_i b_j = 0 \), \( c_{ij} \in F \).

Let \( a_i = \sum_j c_{ij} b_j \). Then each \( a_i \in B \), so linear independence of \( e_1, \ldots, e_n \) over \( B \) implies that each \( a_i = 0 \). But then linear independence of the \( b_j \) over \( F \) implies that, for each \( i \), all \( c_{ij} = 0 \) (\( j = 1, \ldots, m \)) must be zero.

**S spans \( E \) over \( F \).** Given \( e \in E \), write
\[ e = \sum_{i=1}^n a_i e_i \]
with each \( a_i \in B \). Then, for each \( a_i \), write \( a_i = \sum_j c_{ij} b_j \) for some \( c_{ij} \in F \). Then
\[ e = \sum_{i,j} c_{ij} e_i b_j, \]
as desired. \( \square \)
Theorem: Let $\sigma: F \to F'$ be an isomorphism of fields, $f \in F[x]$, $E$ a splitting field of $f$ over $F$ and $E'$ a splitting field of $f^*$ (the image of $f$ in $F'[x]$) over $F'$. Then

1. there is an isomorphism $E \xrightarrow{\sigma} E'$ making
   
   $\begin{array}{cc}
   E & \xrightarrow{\sigma} & E' \\
   F & \xrightarrow{\sigma} & F'
   \end{array}$

   commute.

2. If $f$ is separable, there are exactly $[E:F]$ distinct such isomorphisms $\sigma: E \to E'$.

Proof. By induction on $[E:F]$. If $[E:F]=1$, then $f$ is a product of linear factors in $F[x]$, so $f^*$ is a product of linear factors in $F'[x]$ and $E'=F'$; (1) and (2) are then both clear.

So, suppose (1) and (2) hold for all field extensions of degree less than $n$ ($n>1$). Write $f=pq$ where $p$ is irreducible in $F[x]$ and $q \in F[x]$. If $\deg(p)=1$, then $E$ is a splitting field of $q$ over $F$ and we may replace $f$ by $q$. If $\deg(f)=1$, then we reduce to the above paragraph. So we may assume $\deg(p)>1$; choose a root $\beta$ of $p$ in $E$. Since $f$ is separable, so is $p$, so $p^*$ has $d=\deg(p)$ distinct roots in $E'$, say
Def Let $F \subset \mathbb{C}$ factor into irreducibles over $F[x]$ as
$$f(x) = p_1(x) p_2(x) \cdots p_t(x).$$
Then $F$ is separable if each $p_i(x)$ has no repeated roots.

Note Suppose $F$ has characteristic zero and $p \in F[x]$ is irreducible. Then $p'(x)$ is not the zero polynomial, so $(p, p') = 1$ and thus $p$ has no repeated roots. We conclude that every irreducible polynomial over a field of characteristic zero is separable, hence so is every polynomial.

Def If every polynomial in $F[x]$ is separable, we say $F$ is a perfect field.

Def Let $E/F$ be a field extension. Then $\alpha \in E$
- is a separable element if $\alpha$ is transcendental over $F$ or its irreducible polynomial is separable.
The extension $E/F$ is separable if every element of $E$ is separable over $F.$
Lemma  Let \( \sigma : F \rightarrow F' \) be an isomorphism of fields, \( E/F \) and \( E'/F' \) extensions, and given \( f \in F[x] \), let \( f^* \) denote its image in \( F'[x] \). Suppose that \( p \in F[x] \) is irreducible and that \( \beta \in E, p' \in E'/ \) are roots of \( p, p^* \) respectively. Then there is a unique isomorphism
\[
\begin{array}{c}
F(\beta) \xrightarrow{\sigma} F'(\beta') \\
\end{array}
\]
such that \( \sigma(\beta) = \beta' \) and
\[
\begin{array}{c}
F \xrightarrow{\sigma} F' \\
\downarrow \quad \downarrow \sigma \\
F(\beta) \xrightarrow{\sigma} F'(\beta') \\
\end{array}
\text{commutes.}
\]

Proof. Since there are canonical isomorphisms
\[
F(\beta) \xrightarrow{\cong} F[x]/(p) \quad \text{and} \quad F'(\beta') \xrightarrow{\cong} F'[x]/(p^*)
\]
compatible with the inclusions of \( F \) and \( F' \), respectively, and taking \( x+ (p) \) to \( \beta \) and \( x+ (p^*) \) to \( \beta' \), respectively, it suffices to observe that the image of \( (p) \) in \( F'[x] \) is \( (p^*) \), we get isomorphisms
\[
F(\beta) \xrightarrow{\cong} F[x]/(p) \xrightarrow{\cong} F'[x]/(p^*) \xrightarrow{\cong} F'(\beta')
\]
giving the desired identification. \( \square \)
\(\beta', \beta_2', \ldots, \beta_d'.\) For each \(i',\) there is a unique isomorphism \(F(\beta) \xrightarrow{\sigma_i} F'(\beta'_i)\) restricting to \(c_1 \sigma_i\) on \(F\), by the lemma. Now \(E\) is a splitting field of \(f\) over \(F(\beta)\) and \(E'\) is a splitting field of \(f'\) over \(F'(\beta'_i)\) for each \(i;\) by inductive hypothesis, the fact that

\[ [E:F(\beta)] = [E':F'(\beta'_i)] = \frac{[E:F]}{d} \]

for every \(i,\) this implies that there are exactly \(\frac{[E:F]}{d}\) extensions of \(\sigma_i\) to isomorphisms \(E \xrightarrow{\sigma} E'.\) Hence there are

\[ \frac{[E:F]}{d} \cdot d = [E:F] \]

extensions of \(\sigma\) to isomorphisms \(E \xrightarrow{\sigma} E',\) as desired.

Cor. If \(f \in F[x]\), then any two splittings fields of \(f\) over \(F\) are isomorphic by an isomorphism fixing each element of \(F.\)

Cor. Any two fields of order \(q = p^n\) \((p\ prime, n > 1)\) are isomorphic.

If. Our proof of existence observed that, if \(F\) is a field of order \(q,\) then \(a^q = a\) for every \(a \in F;\) the multiplicative group \(F^\times\) of \(F\) has order \(q - 1,\) so \(a \cdot a \cdots a = a^{q-1} = 1\) for every \(a \neq 0\) in \(F.\)
So, since we also showed that $\overline{\mathbb{F}}_q = \mathbb{F}_q^9 - \mathbb{F}_q$ is separable, $F$ is a splitting field of $\overline{\mathbb{F}}_q$ over the prime field $\mathbb{F}_p \mathbb{Z}$.

We often write $\mathbb{F}_q$ for a field with $q = p^n$ elements, since (up to isomorphism) there can be no ambiguity about which one we mean.

**Remark** Suppose the multiplicative group of units $G = \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ is not cyclic of order $q-1$.

Write $|G| = p_1^{e_1} \cdots p_k^{e_k}$ where $p_1, \ldots, p_k$ are distinct primes. It follows from the structure theorem for finitely generated abelian groups that

$$G \cong G_1 \times G_2 \times \cdots \times G_k$$

where $G_i$ is a $p_i$-group. It follows also from a lemma we proved that if each $G_i$ were cyclic, $G_i \cong \mathbb{Z}/p_i^{e_i} \mathbb{Z}$, then $G$ would be cyclic.

So some $G_i$ is not cyclic, and every element of $\mathbb{F}_q^*$ has order at most $p_i^{e_i-1}$. Then every element of $G$ has order dividing $r = (q-1)/p_i$, and then

$$\psi(x) = (x^r - 1)x$$

has the property that $\psi(a) = 0$ for all $a \in \mathbb{F}_q$, a contradiction since $r < q-1$. So $\mathbb{F}_q^*$ is a cyclic group.