Chapter 1

Introduction

Techniques of abstract algebra have been applied to problems in number theory for a long time, notably in the effort to prove Fermat’s last theorem. As an introductory example, we will sketch a problem for which an algebraic approach works very well. If \( p \) is an odd prime and \( p \equiv 1 \pmod{4} \), we will prove that \( p \) is the sum of two squares, that is, \( p \) can expressed as \( x^2 + y^2 \) where \( x \) and \( y \) are integers. Since \( p - 1 \) is even, it follows that \(-1\) is a quadratic residue (that is, a square) mod \( p \). To see this, pair each of the numbers \( 2, 3, \ldots, p-2 \) with its inverse mod \( p \), and pair 1 with \( p-1 \equiv -1 \pmod{p} \). The product of the numbers 1 through \( p - 1 \) is, mod \( p \),

\[
1 \times 2 \times \cdots \times \frac{p-1}{2} \times -1 \times -2 \times \cdots \times -\frac{p-1}{2}
\]

and therefore

\[
\left(\frac{p-1}{2}\right)! \equiv -1 \pmod{p}.
\]

If \(-1 \equiv x^2 \pmod{p}\), then \( p \) divides \( x^2 + 1 \). Now we enter the ring \( \mathbb{Z}[i] \) of Gaussian integers and factor \( x^2 + 1 \) as \((x + i)(x - i)\). Since \( p \) can divide neither factor, it follows that \( p \) is not prime in \( \mathbb{Z}[i] \). Since the Gaussian integers form a unique factorization domain, \( p \) is not irreducible, and we can write \( p = \alpha\beta \) where neither \( \alpha \) nor \( \beta \) is a unit.

Define the norm of \( \gamma = a + bi \) as \( N(\gamma) = a^2 + b^2 \). Then \( N(\gamma) = 1 \) iff \( \gamma \) is 1, -1, i or -i, equivalently, iff \( \gamma \) is a unit. Thus

\[
p^2 = N(p) = N(\alpha)N(\beta) \text{ with } N(\alpha) > 1 \text{ and } N(\beta) > 1,
\]

so \( N(\alpha) = N(\beta) = p \). If \( \alpha = x + iy \), then \( p = x^2 + y^2 \).

Conversely, if \( p \) is an odd prime and \( p = x^2 + y^2 \), then \( p \) is congruent to 1 mod 4. [If \( x \) is even, then \( x^2 \equiv 0 \pmod{4} \), and if \( x \) is odd, then \( x^2 \equiv 1 \pmod{4} \). We cannot have \( x \) and \( y \) both even or both odd, since \( p \) is odd.]

It is natural to conjecture that we can identify those primes that can be represented as \( x^2 + |m|y^2 \), where \( m \) is a negative integer, by working in the ring \( \mathbb{Z}[\sqrt{m}] \). But the above argument depends critically on unique factorization, which does not hold in general. A
standard example is $2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$. Difficulties of this sort led Kummer to invent “ideal numbers”, which became ideals at the hands of Dedekind. We will see that although a ring of algebraic integers need not be a UFD, unique factorization of ideals will always hold.

1.1 Integral Extensions

If $E/F$ is a field extension and $\alpha \in E$, then $\alpha$ is algebraic over $F$ iff $\alpha$ is a root of a nonconstant polynomial with coefficients in $F$. We can assume if we like that the polynomial is monic, and this turns out to be crucial in generalizing the idea to ring extensions.

1.1.1 Definitions and Comments

All rings are assumed commutative. Let $A$ be a subring of the ring $R$, and let $x \in R$. We say that $x$ is integral over $A$ if $x$ is a root of a monic polynomial $f$ with coefficients in $A$. The equation $f(X) = 0$ is called an equation of integral dependence for $x$ over $A$. If $x$ is a real or complex number that is integral over $\mathbb{Z}$, then $x$ is called an algebraic integer. Thus for every integer $d$, $\sqrt{d}$ is an algebraic integer, as is any $n^{th}$ root of unity. (The monic polynomials are, respectively, $X^2 - d$ and $X^n - 1$.) The next results gives several conditions equivalent to integrality.

1.1.2 Theorem

Let $A$ be a subring of $R$, and let $x \in R$. The following conditions are equivalent:

(i) The element $x$ is integral over $A$;

(ii) The $A$-module $A[x]$ is finitely generated;

(iii) The element $x$ belongs to a subring $B$ of $R$ such that $A \subseteq B$ and $B$ is a finitely generated $A$-module;

(iv) There is a subring $B$ of $R$ such that $B$ is a finitely generated $A$-module and $x$ stabilizes $B$, that is, $xB \subseteq B$. (If $R$ is a field, the assumption that $B$ is a subring can be dropped, as long as $B \neq 0$);

(v) There is a faithful $A[x]$-module $B$ that is finitely generated as an $A$-module. (Recall that a faithful module is one whose annihilator is 0.)

Proof.

(i) implies (ii): If $x$ is a root of a monic polynomial of degree $n$ over $A$, then $x^n$ and all higher powers of $x$ can be expressed as linear combinations of lower powers of $x$. Thus $1, x, x^2, \ldots, x^{n-1}$ generate $A[x]$ over $A$.


(iii) implies (i): If $\beta_1, \ldots, \beta_n$ generate $B$ over $A$, then $x\beta_i$ is a linear combination of the $\beta_j$, say $x\beta_i = \sum_{j=1}^{n} c_{ij} \beta_j$. Thus if $\beta$ is a column vector whose components are the $\beta_i$, $I$ is an $n$ by $n$ identity matrix, and $C = [c_{ij}]$, then

$$(xI - C)\beta = 0,$$
1.1. INTEGRAL EXTENSIONS

and if we premultiply by the adjoint matrix of $xI - C$ (as in Cramer’s rule), we get

$$[\det(xI - C)]I\beta = 0$$

hence $\det(xI - C)b = 0$ for every $b \in B$. Since $B$ is a ring, we may set $b = 1$ and conclude

that $x$ is a root of the monic polynomial $\det(XI - C)$ in $A[X]$.

If we replace (iii) by (iv), the same proofs work. If $R$ is a field, then in (iv)$\Rightarrow$(i), $x$ is
an eigenvalue of $C$, so $\det(xI - C) = 0$.

If we replace (iii) by (v), the proofs go through as before. [Since $B$ is an $A[x]$-module,
in (v)$\Rightarrow$(i) we have $x\beta_i \in B$. When we obtain $[\det(xI - C)]b = 0$ for every $b \in B$, the hypoethesis that $B$ is faithful yields $\det(xI - C) = 0$.]

We are going to prove a transitivity property for integral extensions, and the following result will be helpful.

1.1.3 Lemma

Let $A$ be a subring of $R$, with $x_1, \ldots, x_n \in R$. If $x_1$ is integral over $A$, $x_2$ is integral over $A[x_1]$, \ldots, and $x_n$ is integral over $A[x_1, \ldots, x_{n-1}]$, then $A[x_1, \ldots, x_n]$ is a finitely generated $A$-module.

Proof. The $n = 1$ case follows from (1.1.2), condition (ii). Going from $n - 1$ to $n$ amounts to proving that if $A, B$ and $C$ are rings, with $C$ a finitely generated $B$-module and $B$ a finitely generated $A$-module, then $C$ is a finitely generated $A$-module. This follows by a brief computation:

$$C = \sum_{j=1}^{s} By_j, \quad B = \sum_{k=1}^{r} Ax_k, \quad \text{so } C = \sum_{j=1}^{r} \sum_{k=1}^{s} Ay_j x_k. \quad \clubsuit$$

1.1.4 Transitivity of Integral Extensions

Let $A$, $B$ and $C$ be subrings of $R$. If $C$ is integral over $B$, that is, every element of $C$ is integral over $B$, and $B$ is integral over $A$, then $C$ is integral over $A$.

Proof. Let $x \in C$, with $x^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0 = 0$, $b_i \in B$. Then $x$ is integral over $A[b_0, \ldots, b_{n-1}]$. Each $b_i$ is integral over $A$, hence over $A[b_0, \ldots, b_{i-1}]$. By (1.1.3), $A[b_0, \ldots, b_{i-1}, x]$ is a finitely generated $A$-module. It follows from condition (iii) of (1.1.2) that $x$ is integral over $A$. \clubsuit

1.1.5 Definitions and Comments

If $A$ is a subring of $R$, the integral closure of $A$ in $R$ is the set $A_c$ of elements of $R$ that
are integral over $A$. Note that $A \subseteq A_c$ because each $a \in A$ is a root of $X - a$. We say that
$A$ is integrally closed in $R$ if $A_c = A$. If we simply say that $A$ is integrally closed without
reference to $R$, we assume that $A$ is an integral domain with fraction field $K$, and $A$ is
integrally closed in $K$.

If $x$ and $y$ are integral over $A$, then just as in the proof of (1.1.4), it follows from
(1.1.3) that $A[x, y]$ is a finitely generated $A$-module. Since $x + y, x - y$ and $xy$ belong to
this module, they are integral over \(A\) by (1.1.2), condition (iii). The important conclusion is that
\[
A_c \text{ is a subring of } R \text{ containing } A.
\]

If we take the integral closure of the integral closure, we get nothing new.

1.1.6 Proposition

The integral closure \(A_c\) of \(A\) in \(R\) is integrally closed in \(R\).

Proof. By definition, \(A_c\) is integral over \(A\). If \(x\) is integral over \(A_c\), then as in the proof of (1.1.4), \(x\) is integral over \(A\), and therefore \(x \in A_c\). ♣

We can identify a large class of integrally closed rings.

1.1.7 Proposition

If \(A\) is a UFD, then \(A\) is integrally closed.

Proof. If \(x\) belongs to the fraction field \(K\), then we can write \(x = a/b\) where \(a, b \in A\), with \(a\) and \(b\) relatively prime. If \(x\) is integral over \(A_c\), then there is an equation of the form
\[
\left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + a_1\left(\frac{a}{b}\right) + a_0 = 0
\]

with all \(a_i\) belonging to \(A\). Multiplying by \(b^n\), we have \(a^n + bc = 0\), with \(c \in A\). Thus \(b\) divides \(a^n\), which cannot happen for relatively prime \(a\) and \(b\) unless \(b\) has no prime factors at all, in other words, \(b\) is a unit. But then \(x = ab^{-1} \in A\). ♣

Problems For Section 1.1

Let \(A\) be a subring of the integral domain \(B\), with \(B\) integral over \(A\). In Problems 1-3, we are going to show that \(A\) is a field if and only if \(B\) is a field.

1. Assume that \(B\) is a field, and let \(a\) be a nonzero element of \(A\). Then since \(a^{-1} \in B\), there is an equation of the form
\[
(a^{-1})^n + c_{n-1}(a^{-1})^{n-1} + \cdots + c_1a^{-1} + c_0 = 0
\]

with all \(c_i\) belonging to \(A\). Show that \(a^{-1} \in A\), proving that \(A\) is a field.

2. Now assume that \(A\) is a field, and let \(b\) be a nonzero element of \(B\). By condition (ii) of (1.1.2), \(A[b]\) is a finite-dimensional vector space over \(A\). Let \(f\) be the \(A\)-linear transformation on this vector space given by multiplication by \(b\), in other words, \(f(z) = bz\), \(z \in A[b]\). Show that \(f\) is injective.

3. Show that \(f\) is surjective as well, and conclude that \(B\) is a field.

In Problems 4-6, let \(A\) be a subring of \(B\), with \(B\) integral over \(A\). Let \(Q\) be a prime ideal of \(B\) and let \(P = Q \cap A\).

4. Show that \(P\) is a prime ideal of \(A\), and that \(A/P\) can be regarded as a subring of \(B/Q\).

5. Show that \(B/Q\) is integral over \(A/P\).

6. Show that \(P\) is a maximal ideal of \(A\) if and only if \(Q\) is a maximal ideal of \(B\).
1.2 Localization

Let $S$ be a subset of the ring $R$, and assume that $S$ is multiplicative, in other words, $0 \not\in S$, $1 \in S$, and if $a$ and $b$ belong to $S$, so does $ab$. In the case of interest to us, $S$ will be the complement of a prime ideal. We would like to divide elements of $R$ by elements of $S$ to form the localized ring $S^{-1}R$, also called the ring of fractions of $R$ by $S$. There is no difficulty when $R$ is an integral domain, because in this case all division takes place in the fraction field of $R$. Although we will not need the general construction for arbitrary rings $R$, we will give a sketch. For full details, see TBGY, Section 2.8.

1.2.1 Construction of the Localized Ring

If $S$ is a multiplicative subset of the ring $R$, we define an equivalence relation on $R \times S$ by $(a, b) \sim (c, d)$ iff for some $s \in S$ we have $s(ad - bc) = 0$. If $a \in R$ and $b \in S$, we define the fraction $a/b$ as the equivalence class of $(a, b)$. We make the set of fractions into a ring in a natural way. The sum of $a/b$ and $c/d$ is defined as $(ad + bc)/bd$, and the product of $a/b$ and $c/d$ is defined as $ac/bd$. The additive identity is $0/1$, which coincides with $0/s$ for every $s \in S$. The additive inverse of $a/b$ is $-a/b = (-a)/b$. The multiplicative identity is $1/1$, which coincides with $s/s$ for every $s \in S$. To summarize:

$S^{-1}R$ is a ring. If $R$ is an integral domain, so is $S^{-1}R$. If $R$ is an integral domain and $S = R \setminus \{0\}$, then $S^{-1}R$ is a field, the fraction field of $R$.

There is a natural ring homomorphism $h : R \to S^{-1}R$ given by $h(a) = a/1$. If $S$ has no zero-divisors, then $h$ is a monomorphism, so $R$ can be embedded in $S^{-1}R$. In particular, a ring $R$ can be embedded in its full ring of fractions $S^{-1}R$, where $S$ consists of all non-divisors of $0$ in $R$. An integral domain can be embedded in its fraction field.

Our goal is to study the relation between prime ideals of $R$ and prime ideals of $S^{-1}R$.

1.2.2 Lemma

If $X$ is any subset of $R$, define $S^{-1}X = \{x/s : x \in X, s \in S\}$. If $I$ is an ideal of $R$, then $S^{-1}I$ is an ideal of $S^{-1}R$. If $J$ is another ideal of $R$, then

(i) $S^{-1}(I + J) = S^{-1}I + S^{-1}J$;
(ii) $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$;
(iii) $S^{-1}(I \cap J) = (S^{-1}I) \cap (S^{-1}J)$;
(iv) $S^{-1}I$ is a proper ideal iff $S \cap I = \emptyset$.

Proof. The definitions of addition and multiplication in $S^{-1}R$ imply that $S^{-1}R$ is an ideal, and that in (i), (ii) and (iii), the left side is contained in the right side. The reverse inclusions in (i) and (ii) follow from

\[
\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}
\]

To prove (iii), let $a/s = b/t$, where $a \in I$, $b \in J$, $s, t \in S$. There exists $u \in S$ such that $u(at - bs) = 0$. Then $a/s = uat/ust = ubs/ust \in S^{-1}(I \cap J)$.

Finally, if $s \in S \cap I$, then $1/1 = s/s \in S^{-1}I$, so $S^{-1}I = S^{-1}R$. Conversely, if $S^{-1}I = S^{-1}R$, then $1/1 = a/s$ for some $a \in I$, $s \in S$. There exists $t \in S$ such that $t(s - a) = 0$, so $at = st \in S \cap I$. \hfill \blacktriangle
Ideals in $S^{-1}R$ must be of a special form.

1.2.3 Lemma

Let $h$ be the natural homomorphism from $R$ to $S^{-1}R$ [see (1.2.1)]. If $J$ is an ideal of $S^{-1}R$ and $I = h^{-1}(J)$, then $I$ is an ideal of $R$ and $S^{-1}I = J$.

Proof. $I$ is an ideal by the basic properties of preimages of sets. Let $a/s \in S^{-1}I$, with $a \in I$ and $s \in S$. Then $a/1 = h(a) \in J$, so $a/s = (a/1)(1/s) \in J$. Conversely, let $a/s \in J$, with $a \in R$, $s \in S$. Then $h(a) = a/1 = (a/s)(s/1) \in J$, so $a \in I$ and $a/s \in S^{-1}I$. ♣

Prime ideals yield sharper results.

1.2.4 Lemma

If $I$ is any ideal of $R$, then $I \subseteq h^{-1}(S^{-1}I)$. There will be equality if $I$ is prime and disjoint from $S$.

Proof. If $a \in I$, then $h(a) = a/1 \in S^{-1}I$. Thus assume that $I$ is prime and disjoint from $S$, and let $a \in h^{-1}(S^{-1}I)$. Then $h(a) = a/1 \in S^{-1}I$, so $a/1 = b/s$ for some $b \in I, s \in S$. There exists $t \in S$ such that $t(au - b) = 0$. Thus $ast = bt \in I$, with $st \notin I$ because $S \cap I = \emptyset$. Since $I$ is prime, we have $a \in I$. ♣

1.2.5 Lemma

If $I$ is a prime ideal of $R$ disjoint from $S$, then $S^{-1}I$ is a prime ideal of $S^{-1}R$.

Proof. By part (iv) of (1.2.2), $S^{-1}I$ is a proper ideal. Let $(a/s)(b/t) = ab/st \in S^{-1}I$, with $a, b \in R, s, t \in S$. Then $ab/st = c/u$ for some $c \in I, u \in S$. There exists $v \in S$ such that $v(abu - cst) = 0$. Thus $abv = cstv \in I$, and $uv \notin I$ because $S \cap I = \emptyset$. Since $I$ is prime, $ab \in I$, hence $a \in I$ or $b \in I$. Therefore either $a/s$ or $b/t$ belongs to $S^{-1}I$. ♣

The sequence of lemmas can be assembled to give a precise conclusion.

1.2.6 Theorem

There is a one-to-one correspondence between prime ideals $P$ of $R$ that are disjoint from $S$ and prime ideals $Q$ of $S^{-1}R$, given by

$$P \to S^{-1}P \text{ and } Q \to h^{-1}(Q).$$

Proof. By (1.2.3), $S^{-1}(h^{-1}(Q)) = Q$, and by (1.2.4), $h^{-1}(S^{-1}P) = P$. By (1.2.5), $S^{-1}P$ is a prime ideal, and $h^{-1}(Q)$ is a prime ideal by the basic properties of preimages of sets. If $h^{-1}(Q)$ meets $S$, then by (1.2.2) part (iv), $Q = S^{-1}(h^{-1}(Q)) = S^{-1}R$, a contradiction. Thus the maps $P \to S^{-1}P$ and $Q \to h^{-1}(Q)$ are inverses of each other, and the result follows. ♣
1.2. Definitions and Comments

If $P$ is a prime ideal of $R$, then $S = R \setminus P$ is a multiplicative set. In this case, we write $R_P$ for $S^{-1}R$, and call it the localization of $R$ at $P$. We are going to show that $R_P$ is a local ring, that is, a ring with a unique maximal ideal. First, we give some conditions equivalent to the definition of a local ring.

1.2.8 Proposition

For a ring $R$, the following conditions are equivalent.

(i) $R$ is a local ring;
(ii) There is a proper ideal $I$ of $R$ that contains all nonunits of $R$;
(iii) The set of nonunits of $R$ is an ideal.

Proof. (i) implies (ii): If $a$ is a nonunit, then $(a)$ is a proper ideal, hence is contained in the unique maximal ideal $I$.

(ii) implies (iii): If $a$ and $b$ are nonunits, so are $a + b$ and $ra$. If not, then $I$ contains a unit, so $I = R$, contradicting the hypothesis.

(iii) implies (i): If $I$ is the ideal of nonunits, then $I$ is maximal, because any larger ideal $J$ would have to contain a unit, so $J = R$. If $H$ is any proper ideal, then $H$ cannot contain a unit, so $H \subseteq I$. Therefore $I$ is the unique maximal ideal. ♣

1.2.9 Theorem

$R_P$ is a local ring.

Proof. Let $Q$ be a maximal ideal of $R_P$. Then $Q$ is prime, so by (1.2.6), $Q = S^{-1}I$ for some prime ideal $I$ of $R$ that is disjoint from $S = R \setminus P$. In other words, $I \subseteq P$. Consequently, $Q = S^{-1}I \subseteq S^{-1}P$. If $S^{-1}P = R_P = S^{-1}R$, then by (1.2.2) part (iv), $P$ is not disjoint from $S = R \setminus P$, which is impossible. Therefore $S^{-1}P$ is a proper ideal containing every maximal ideal, so it must be the unique maximal ideal. ♣

1.2.10 Remark

It is convenient to write the ideal $S^{-1}I$ as $IR_P$. There is no ambiguity, because the product of an element of $I$ and an arbitrary element of $R$ belongs to $I$.

1.2.11 Localization of Modules

If $M$ is an $R$-module and $S$ a multiplicative subset of $R$, we can essentially repeat the construction of (1.2.1) to form the localization of $M$ by $S$, and thereby divide elements of $M$ by elements of $S$. If $x, y \in M$ and $s, t \in S$, we call $(x, s)$ and $(y, t)$ equivalent if for some $u \in S$, we have $u(tx - sy) = 0$. The equivalence class of $(x, s)$ is denoted by $x/s$, and addition is defined by

$$
\frac{x}{s} + \frac{y}{t} = \frac{tx + sy}{st}.
$$
CHAPTER 1. INTRODUCTION

If $a/s \in S^{-1}R$ and $x/t \in S^{-1}M$, we define

$$\frac{ax}{st}.$$ 

In this way, $S^{-1}M$ becomes an $S^{-1}R$-module. Exactly as in (1.2.2), if $M$ and $N$ are submodules of an $R$-module $L$, then

$$S^{-1}(M + N) = S^{-1}M + S^{-1}N \text{ and } S^{-1}(M \cap N) = (S^{-1}M) \cap (S^{-1}N).$$

Problems For Section 1.2

1. Let $M$ be a maximal ideal of $R$, and assume that for every $x \in M$, $1 + x$ is a unit. Show that $R$ is a local ring (with maximal ideal $M$).

2. Show that if $p$ is prime and $n$ is a positive integer, then $\mathbb{Z}/p^n\mathbb{Z}$ is a local ring with maximal ideal $(p)$.

3. For any field $k$, let $R$ be the ring of rational functions $f/g$ with $f, g \in k[X_1, \ldots, X_n]$ and $g(a) \neq 0$, where $a$ is a fixed point of $k^n$. Show that $R$ is a local ring, and identify the unique maximal ideal.

Let $S$ be a multiplicative subset of the ring $R$. We are going to construct a mapping from $R$-modules to $S^{-1}R$-modules, and another mapping from $R$-module homomorphisms to $S^{-1}R$-module homomorphisms, as follows. If $M$ is an $R$-module, we map $M$ to $S^{-1}M$. If $f : M \rightarrow N$ is an $R$-module homomorphism, we define $S^{-1}f : S^{-1}M \rightarrow S^{-1}N$ by

$$\frac{x}{s} \rightarrow \frac{f(x)}{s}.$$ 

Since $f$ is a homomorphism, so is $S^{-1}f$. In Problems 4-6, we study these mappings.

4. Let $f : M \rightarrow N$ and $g : N \rightarrow L$ be $R$-module homomorphisms. Show that $S^{-1}(g \circ f) = (S^{-1}g) \circ (S^{-1}f)$. Also, if $1_M$ is the identity mapping on $M$, show that $S^{-1}1_M = 1_{S^{-1}M}$. Thus we have a functor $S^{-1}$, called the localization functor, from the category of $R$-modules to the category of $S^{-1}R$-modules.

5. If

$$M \xrightarrow{f} N \xrightarrow{g} L$$

is an exact sequence of $R$-modules, show that

$$S^{-1}M \xrightarrow{S^{-1}f} S^{-1}N \xrightarrow{S^{-1}g} S^{-1}L$$

is exact. Thus $S^{-1}$ is an exact functor.

6. If $M$ is an $R$-module and $S$ is a multiplicative subset of $R$, denote $S^{-1}M$ by $M_S$. If $N$ is a submodule of $M$, show that $(M/N)_S \cong M_S/N_S$. 