Chapter 9

Rings and Ideals

In this chapter we introduce some abstract algebra in order to shed some light on several ad-hoc constructions that we have employed previously.

In general, a ring is a set on which two compositions called addition and multiplication are defined in such a way that certain axioms hold. In particular, R should be a group with respect to addition and a monoid with respect to multiplication; moreover, distributivity $a(b+c) = ab + bc$ should hold.

Here, all our rings will be commutative ($ab = ba$) domains ($ab = 0$ implies $a = 0$ or $b = 0$; the ring $\mathbb{Z}/6\mathbb{Z}$ is not a domain because $[2][3] = [0]$) and will have a multiplicative unit 1 (the ring $2\mathbb{Z}$ of even numbers does not have a unit; sometimes such objects are called rngs).

9.1 Euclidean Rings

A domain R is called a Euclidean ring if there exists a function $\nu : R \longrightarrow \mathbb{N}$ such that

E1 $\nu(r) = 0$ if and only if $r = 0$;

E2 for all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that $a = bq + r$ and $\nu(r) < \nu(b)$.

For example, $R = \mathbb{Z}$ is a Euclidean ring with respect to the absoulute value $\nu = |\cdot|$.

Lemma 9.1. *If R is Euclidean with respect to ν, then $\nu(b) = 1$ implies that $b \in R^\times$.*

Proof. Assume that $\nu(b) = 1$; then $1 = bq + r$ with $\nu(r) < \nu(b) = 1$. Thus $\nu(r) = 0$, hence $r = 0$ by [E1], and we have proved that $b \mid 1$, i.e, $b \in R^\times$. □

Let us now give a few important examples of Euclidean rings.

Proposition 9.2. *The ring $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ of Gaussian integers is Euclidean with respect to the norm function $N(x + iy) = x^2 + y^2$.*

Proof. Let us first show that the norm function is multiplicative. This means that $N[(a+bi)(c+di)] = N(a+bi) \cdot N(c+di)$, and is easily checked by computation.

Now assume that we are given elements $a = r + si$ and $b + t + ui$ in $\mathbb{Z}[i]$; then we need to find $q, r \in \mathbb{Z}[i]$ with $a = bq + r$ and $N(r) < N(b)$. Since N is multiplicative, this is equivalent to the statement that for every $p = \frac{a}{b} \in \mathbb{Q}(i) = \{x + yi : x, y \in \mathbb{Q}\}$ there is an element $q \in \mathbb{Z}[i]$ with $N(p - q) < 1$.

Now write $p - q = x + yi$ for $x, y \in \mathbb{Q}$, and let $q = c + di$ with $c, d \in \mathbb{Z}$ and $|x - c| \leq \frac{1}{2}$, $|y - d| \leq \frac{1}{2}$. Then $N(p - q) \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1$. □

This result can be generalized somewhat: the rings $\mathbb{Z}[\sqrt{m}\,]$ are Euclidean with respect to $\nu(a + b\sqrt{m}\,) = |a^2 - mb^2|$ for $m = -2, 2, 3$. In fact, there are more values of m for which these rings are Euclidean, but the proofs soon become very technical.

Proposition 9.3. *Let K be a field. Then the ring $K[X]$ of polynomials in one variable X with coefficients from K is Euclidean with respect to $\nu(f) = 2^{\deg f}$.*

Proof. Assume that $a, b \in R$ are nonzero polynomials. Then we have to find $q, r \in R$ with $a = bq + r$ and $\deg r < \deg b$. We do this by induction and long division.

First observe that the claim is trivial if $\deg a < \deg b$; thus we may assume that $\deg a \geq \deg b$. Then the claim is trivial if $\deg a = 0$, since this implies $\deg b = 0$, hence b is a nonzero constant, hence a unit, and we can write $a = bq + 0$ with $q = ab^{-1}$.

Now assume that the claim is true for all polynomials a with $\deg a < m$, and write $a = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_0$ and $b = a_n x^n + b_{n-1}x^{n-1} + \ldots + b_0$ with $m \geq n$. Then a and $b \cdot q_1$ with $q_1 = \frac{a_m}{b_n} X^{m-n}$ are polynomials of degree m with the same leading coefficient a_m, hence $r_1 = a - bq_1$ is a polynomial with degree $\deg r_1 < m$. By induction assumption, there exist polynomials q, r with $r_1 = bq + r$ and $\deg r < \deg b$. But now $a = bq_1 + r_1 = b(q_1 + q) + r$, and this proves the theorem. □

9.2 Ideals

Our goal is to show that Euclidean rings are UFDs. This will have concrete applications; apart from showing again that e.g. $\mathbb{Z}$ has unique factorization, the fact that $\mathbb{Z}[i]$ is a UFD implies that every prime $p \equiv 1 \bmod 4$ is the sum of two integral squares. Even Lagrange's 4-squares theorem (every positive integer is the sum of 4 integral squares) can be proved by showing that the division algebra of quaternions $A = Q(i, j, k)$ with $i^2 = j^2 = k^2 = -1$ and $ij = -ji$, $ij = k$ contains a (left) Euclidean subring.

The proof that Euclidean rings are UFDs becomes simpler upon introducing another type of rings: principal ideal rings (PIDs). Thus what we actually will prove are the inclusions

Euclidean Rings ⊂ Principal Ideal Rings ⊂ Unique Factorization Rings.

Let R be a ring. A subring I of R is called an ideal if $IR \subseteq I$, i.e., if $ir \in I$ for all $i \in I$ and all $r \in R$.

Let me give you a few examples:

- In any ring, the set $(a) = \{ar : r \in R\}$ is an ideal for any $a \in R$. Such ideals are called principal ideals. In particular, $R = (1)$ and (0) are ideals.

- For $a, b \in R$, the set $(a, b) = \{ar + bs : r, s \in R\}$ is an ideal.

  In $\mathbb{Z}$, the ideal $I = (3, 5)$ contains $2 = 5 - 3$, 3, hence $1 = 3 - 2 = 3 - (5 - 3) = 2 \cdot 3 - 5$. But if $1 \in I$, then $m = 1 \cdot m \in I$ for any $m \in \mathbb{Z}$, and we conclude that $I = (1) = \mathbb{Z}$.

  Similarly, the ideal $I = (6, 9)$ contains $3 = 9 - 6$, hence $3m \in I$ for any $m \in \mathbb{Z}$. On the other hand, if $r \in I$, then $r = 6a + 9b = 3(2a + 3b)$ is a multiple of 3. This shows that $I = (3) = 3\mathbb{Z}$.

- More generally, the set $(a_1, \ldots, a_n) = \{r_1 a_1 + \ldots + r_n a_n : r_i \in R\}$ forms an ideal. Ideals of thi form are called finitely generated. For any set of $a_i \in R$, $I = (a_1, a_2, \ldots)$ is defined to be the set of all **finite** R-linear combinations of the a_i; this is again an ideal.

- Every subring of $\mathbb{Z}$ is an ideal; im fact, the subrings of $\mathbb{Z}$ have the form $(m) = m\mathbb{Z}$ for some integer m, and these are all ideals: $a \in (m)$ implies $a = mb$ for some integer b; but then $ar = m(br) \in (m)$ for any integer r.

- The set I of ideals $\left(\begin{smallmatrix} a & 0 \\ c & d \end{smallmatrix}\right)$ with $a, c, d \in \mathbb{Z}$ forms a subring of the ring $M_2(\mathbb{Z})$ of 2×2-matrices with entries in $\mathbb{Z}$, but they do no not form an ideal because e.g. $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ is not in I.

- In the polynomial ring $\mathbb{C}[X, Y]$ in two variables, the ideal (X, Y) is not principal (!).

- Let $\mathcal{S} = \{(a_n) = (a_0, a_1, a_2, \ldots) : a_j \in \mathbb{Q}\}$ denote the set sequences in $\mathbb{Q}$. Then $\mathcal{S}$ is a ring if you add and multiply sequences in the familiar way: $(a_n) + (b_n) = (c_n)$ for $c_j = a_j + b_j$ $(j \in \mathbb{N})$ and similarly for subtraction and multiplication.

  The set $\mathcal{B}$ of bounded sequences is a subring of $\mathcal{S}$. It is not an ideal in $\mathcal{S}$ because bounded sequences times sequences are not bounded in general: $(1, 1, 1, \ldots) \cdot (1, 2, 3, \ldots) = (1, 2, 3, \ldots)$.

  The set $\mathcal{C}$ of Cauchy sequences is a subring of $\mathcal{B}$ because sums and products of Cauchy sequences are Cauchy again. Now $\mathcal{C}$ is clearly not an ideal in $\mathcal{S}$, but it is an ideal in $\mathcal{B}$ because the product of a Cauchy sequence and a bounded sequence is Cauchy again.

  The set $\mathcal{L}$ of converging sequences (sequences that have a limit within $\mathbb{Q}$) form a subring of $\mathcal{C}$ (this is because if $\lim a_n = a$ and $\lim b_n = b$ with $a, b \in \mathbb{Q}$, then $\lim(a_n + b_n) = a + b \in \mathbb{Q}$ and $\lim a_n b_n = ab \in \mathbb{Q}$), but not an ideal: in fact, if $(a_n) = (1, 1, 1, \ldots)$ and (b_n) is a Cauchy sequence that

does not converge in $\mathbb{Q}$ (for example, take a sequence of rational numbers "converging" to $\sqrt{2}$); then $(a_n)(b_n)$ does not converge.

Finally, let $\mathcal{N}$ denote the set of null sequences, i.e., sequences converging to 0. They form a subring of $\mathcal{L}$, and actually form an ideal in $\mathcal{L}$, in $\mathcal{C}$ and even in $\mathcal{B}$.

A domain in which every ideal is principal is called a principal ideal domain. Checking whether a given ideal is principal or not is often a nontrivial task. For example, is the ideal $\mathcal{N}$ principal in $\mathcal{L}$?

In order to become familiar with ideals, let us prove

Lemma 9.4. *Let R be a ring. Then $(b) \supseteq (a)$ if and only if $b \mid a$ (to contain is to divide).*

Proof. If $(b) \supseteq (a)$, then $a \in (b)$ and hence $a = bc$ for some $c \in R$. Thus $b \mid a$. The converse is also clear. □

Lemma 9.5. *Let R be a ring. Then $(a) = R$ if and only of $a \in R^\times$.*

Proof. From $(a) = (1)$ we deduce that $1 \in (a)$, hence there is some $r \in R$ with $ar = 1$. But then $a \in R^\times$. □

Lemma 9.6. *Let R be a ring. Then $(a) \subseteq (a, b)$ for any $b \in R$.*

This is trivial.

Lemma 9.7. *Let R be a ring. If $(a) \subseteq I$ and $(b) \subseteq I$, then $(a, b) \subseteq I$.*

Proof. This is clear by the definition of an ideal: from $a, b \in I$ we get $ar + bs \in I$ for all $r, s \in I$. □

The next result connects ideals to the notion of a greatest common divisor:

Proposition 9.8. *Let R be a PID. Then elements have a gcd. Moreover, $d = \gcd(a, b)$ for $a, b, d \in R$ if and only if $(a, b) = (d)$.*

Proof. Let $a, b \in R$. We have to show that there is some $d \in R$ satisfying the axioms of a gcd. Since R is a PID, we can write $(a, b) = (d)$ (such a d will not be unique). There are two things to show:

1. $d \mid a$, $d \mid b$: In fact, $a \in (a, b) = (d)$ implies $a = dr$ for some $r \in R$, hence $d \mid a$; similarly we find $d \mid b$.
2. $e \mid a$, $e \mid b \Longrightarrow e \mid d$: since $d \in (a, b)$ there exist $r, s \in R$ with $d = ar + bs$. Now the assumptions imply that e divides the right hand side, hence $e \mid d$

□

We have seen examples of this before when we showed that $(3, 5) = (1)$ and $(6, 9) = (3)$.

9.3 Principal Ideal Domains

Now we claim

Theorem 9.9. *Every Euclidean domain is a PID.*

Proof. Let I be an ideal in the Euclidean ring R. If $I = (0)$ we are done; thus assume that I is not the zero ideal. Let $a \in I$ be a nonzero element with minimal $f(a)$, where f is the Euclidean function. We claim that $I = (a)$.

In fact, let $b \in I$ and write $b = aq + r$ with $f(r) < f(a)$; since $a \in I$ and I is an ideal we know that $aq \in I$, hence $r = b - aq \in I$. By the definition of a we must have $r = 0$, and this shows that every element of I is a multiple of a, i.e., $I = (a)$. □

This provides us with many (but not all) PIDs. In our proof of unique factorization in $\mathbb{Z}$, the main problem was showing that irreducibles are prime. In PIDs, we get this for free:

Proposition 9.10. *In any PID irreducible elements are prime.*

Proof. Let $p \in R$ be irreducible, and assume that $p \mid ab$. If $p \mid a$ we are done, so assume that $p \nmid a$. We claim that $(a, p) = (1) = R$. In fact, write $(d) = (a, p)$. Then $d \mid p$, hence $p = dr$ for $d, r \in R$. Since p is irreducible, d or r must be a unit. If d is a unit, then $(a, p) = (1)$ as claimed, and if r is a unit, then $(d) = (p)$, hence $(a, p) = (p)$ and finally $p \mid a$: contradiction.

Thus $(a, p) = (1)$, hence there exist $r, s \in R$ with $ar + ps = 1$. But then $b = abr + aps$, and since $p \mid ab$, p divides the right hand side and therefore b. □

Next we have to show that every nonzero nonunit in a PID has a factorization into irreducibles. This is not at all obvious: consider e.g. the domain $D = \mathbb{Z}[\sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \ldots]$ containing $\mathbb{Z}$ and all roots $2^{1/2^n}$ for $n \geq 1$. Then 2 is not a unit, and it is not irreducible because $2 = \sqrt{2} \cdot \sqrt{2}$. But $\sqrt{2} = \sqrt[4]{2} \cdot \sqrt[4]{2}$ shows that $\sqrt{2}$ is also reducible, and this process can be continued indefinitely: although 2 is a nonunit, it is not a product of irreducibles because none of its factors is irreducible. In PIDs, this does not happen:

Proposition 9.11. *Let R be a PID. Then every $a \in R \setminus \{0\}$ has a factorization into a unit times irreducible elements.*

Proof. If a is a unit, we are done. If a is a nonunit then we claim that a has an irreducible factor. This is clear if a is irreducible; if not then it has a nontrivial factorization $a = a_1 b_1$. If a_1 is irreducible, we are done; if not, then there is a nontrivial factorization $a_1 = a_2 b_2$ etc. In this way we get a sequence of elements $a_1, a_2, \ldots$ with $\ldots, a_3 \mid a_2, a_2 \mid a_1, a_1 \mid a$. Consider the ideal $I = (a, a_1, a_2, \ldots)$. Since R is a PID, there is a $c \in R$ with $I = (c)$. Since I is the union of the ideals (a), (a_1), (a_2), $\ldots$, c must be an element of one of these, say $c \in (a_m)$. But then $(c) \subseteq (a_m)$ and $(a_m) \subseteq I = (c)$ imply that $I = (a_m)$. Now $a_{m+1} \mid a_m$, as well as $a_m \mid a_{m+1}$ because $a_{m+1} \in I = (a_m)$: this implies that a_m and a_{m+1} differ by a unit, hence $a_m = a_{m+1} b_{m+1}$ is not a nontrivial factorization.

Thus we have shown that every nonzero nonunit a is divisible by an irreducible element. We now claim that a has a factorization into irreducibles. In fact, write $a = a_1 b_1$ with a_1 irreducible. If b_1 is irreducible, we are done; if not, write $b_1 = a_2 b_2$ with a_2 irreducible and continue. By the same argument as above this process must terminate, and after finitely many steps we have a factorization of a into irreducibles. □

Now we are ready to prove

Theorem 9.12. *Every PID is a UFD.*

Proof. We have already shown the following two facts:

1. Every element $\neq 0$ has a factorization into irreducible elements;
2. Irreducibles are primes.

Now assume that $a = p_1 \cdots p_r = q_1 \cdots q_s$ are factorizations into irreducibles. Since p_1 is prime and divides the right hand side, it must divide one of the factors, say $p_1 \mid q_1$. Since q_1 is irreducible, we must have $q_1 = p_1 u_1$ for some unit u_1; replacing q_2 by $q_2 u_1$ and cancelling p_1 shows that $p_2 \cdots p_r = q_2 \cdots q_s$. Now do induction on the number of irreducible factors just as in $\mathbb{Z}$. □

9.4 Residue Classes modulo Ideals

Ideals have played a role in our proof that Euclidean domains have unique factorization. The main purpose of ideals, however, is that they can be used to generalize the notion of residue classes modulo elements.

In fact, let R be a ring (as always commutative and with a multiplicative unit 1) and I an ideal in R. Then we say that $a \equiv b \bmod I$ if $a - b \in I$. If $I = (m)$ is principal, this is the usual definition: we have $a \equiv b \bmod (m) \iff a - b \in (m) \iff a - b = mr$ for some $r \in R \iff m \mid a - b \iff a \equiv b \bmod m$.

The residue class $a \bmod I$ is denoted by $[r]$ or $r + I$. Thus $r + I = \{a \in R : a \equiv r \bmod I\} = \{r + i : i \in I\}$. The set of residue classes modulo I is denoted by R/I. Note that $\mathbb{Z}/m\mathbb{Z}$ is equal to R/I for $R = \mathbb{Z}$ and $I = m\mathbb{Z} = (m)$.

Proposition 9.13. *The set R/I of residue classes modulo I forms a ring.*

We define the norm of an ideal I by $N(I) = \#R/I$. Note that the norm of an ideal might be infinite; for example, $\mathbb{Z}/(0)$ has infinitely many elements (distinct integers determine distinct residue classes modulo (0); similarly, $\mathbb{Z}[X]/(X)$ is infinite). Since R/I is a ring, we can form its unit group $(R/I)^\times$. We now define Euler's phi function for ideals in R by $\Phi(I) = \#(R/I)^\times$.

In the case $R = \mathbb{Z}$ we have proved that $\phi(p^n) = (p-1)p^{n-1}$ for positive primes (or $\phi(p) = (|p|-1)|p|^{n-1}$ for arbitrary primes). We did this by counting all the elements in $\mathbb{Z}/p^n\mathbb{Z}$ (there were p^n of them) and subtracting the number classes represented by multiples of p (there are p^{n-1} of them).

After this excursion into the depths of abstract algebra we now return to number theory: in the next two chapters we will study the arithmetic of two UFDs, namely the ring $\mathbb{Z}[i]$ of Gaussian integers and the ring $\mathbb{F}_p[X]$ of polynomials with coefficients in the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Exercises

9.1 Let R be the ring of continuous functions $\mathbb{R} \longrightarrow \mathbb{R}$, where addition and multiplication are defined pointwise.

1. Determine the unit group $R^\times$;
2. does R contain irreducible elements?
3. for $a \in \mathbb{R}$ let $I_a = \{f \in R : f(a) = 0\}$; is I_a an ideal?
4. find an ideal in R that is not principal.

9.2 Prove that the ideal (X, Y) in $\mathbb{C}[X, Y]$ is not principal.