2 Background on rings and fields

Keywords: Field of fractions, rational function, ideal, generators of an ideal, kernel, coset, prime ideal, maximal ideal, quotient ring, principal ideal, PID, UFD, first isomorphism theorem for rings, characteristic, prime field, Frobenius.

This chapter is a reminder and reference on rings and fields. You're supposed to know most or all of this chapter already, and this chapter is not detailed enough to learn the material if you haven't seen it before. We use the material in this chapter throughout the rest of the notes. If you're not yet familiar with the material in this chapter but still want to follow the module then you'll have to work very hard to catch up. A good place to learn this material is chapter 3 in *Concrete Abstract Algebra* by Niels Lauritzen.

2.1 Fields of fractions

Exercise (2.1) Let A be an integral domain. Put

$$B = \{(a,b) \in A \times A \mid b \neq 0\}$$

and let $\sim$ be the binary relation on B defined by $(a,b) \sim (c,d)$ if and only if $ad = bc$.

(a) Prove that $\sim$ is an equivalence relation. We denote the equivalence class of (a,b) by a/b.

(b) Prove that the following are well-defined operations on $A/\sim$:

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{a\,c}{b\,d}, \qquad \frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}.$$

Prove that this makes $A/\sim$ into a field. It is called the **field of fractions** of A and sometimes written $\operatorname{Frac} A$.

(c) What goes wrong in the above if A is a ring which is not an integral domain?

If K is a field, the field of fractions $\operatorname{Frac} K[X]$ of the polynomial ring is written $K(X)$. An element of $K(X)$ is called a **rational function**, in analogy with the observation that $\operatorname{Frac} \mathbb{Z} = \mathbb{Q}$.

2.2 Ideals and factorisation

A nonzero subset I of a ring A is said to be an **ideal** if

$$x - y \in I \quad \text{for all} \quad x, y \in I; \tag{26}$$

$$ax \in I \quad \text{for all} \quad a \in A, \quad x \in I. \tag{27}$$

Note that (26) means precisely that $I \subset A$ is an additive subgroup.

Exercise (2.2) Let A be a ring.

(a) If $x_1, \ldots, x_n \in A$ then $I := \{\sum_{k=1}^{n} a_k\, x_k \mid a_1, \ldots, a_n \in A\}$ is an ideal in A.

(b) Suppose that J is an ideal containing $x_1, \ldots, x_n$. Prove that $I \subset J$. Thus, I is the smallest ideal containing $\{x_1, \ldots, x_n\}$. We call it the ideal **generated by $x_1, \ldots, x_n$**. It is written $(x_1, \ldots, x_n)$ or $x_1A + \cdots + x_nA$.

The **kernel** of a ring homomorphism $f\colon A \to B$ is defined to be $\ker(f) := \{a \in A \mid f(a) = 0\}$. Then $\ker(f)$ is an ideal in A.

Let A be a ring and $I \subset A$ an ideal. For $a \in A$ we write $a + I := \{a + x \mid x \in I\}$ (this is called a **coset**) and $A/I := \{a + I \mid x \in I\}$. We have $a + I = b + I$ if and only if $a - b \in I$. We put a ring structure on the set A/I by $(a + I) + (b + I) := (a + b) + I$ and $(a + I)(b + I) := (ab) + I$. One should prove that this is well-defined, that is, if $a_1 + I = a_2 + I$ then $a_1b + I = a_1b + I$, and likewise for addition. One should also prove that this makes A/I into a ring. This is the unique ring structure on the set A/I such that the natural map $A \to A/I$, $a \mapsto a + I$ is a ring homomorphism. Its kernel is precisely I. This proves:

Proposition 28. *Let I be an ideal in a ring A. Then there exists a ring B and a surjective ring homomorphism $A \to B$ whose kernel is I.* □

We call A/I the **quotient ring** of A by I.

Definition 29. Let I be an ideal in a ring A such that $I \neq A$. We call I a **prime ideal** if $ab \in I$ implies $a \in I$ or $b \in I$. We call it a **maximal ideal** if for every ideal J such that $I \subset J \subset A$ we have $I = J$ or $J = A$.

Proposition 30. *Let I be an ideal in A.*

(a) *Then, I is a prime ideal if and only if A/I is an integral domain.*

(b) *Also, I is a maximal ideal if and only if A/I is a field.* □

Definition 31. Let A be a ring. A **principal ideal** in A is an ideal of the form aA with $a \in A$, that is, an ideal generated by a single element a. A **principal ideal domain** or PID is an integral domain all of whose ideals are principal.

Proposition 32. *The ring $\mathbb{Z}$ is a PID. If K is a field then $K[X]$ is a PID.* □

Exercise (2.3) Prove the second half of proposition 32, namely, that $K[X]$ is a PID for any field K. Hint: if $I \subset K[X]$ is a nonzero ideal, let $f \in I$ be a nonzero of minimal degree. Use theorem 2 (division with remainder) to prove that $I = (f)$.

Proposition 33. *Let A be a PID. Then for all nonzero $a \in A$, the following are equivalent.*

(1) *The ideal (a) is a maximal ideal in A.*

(2) *The ideal (a) is a prime ideal in A.*

(3) *a is irreducible.*

Proof. The implications (1) $\Rightarrow$ (2) $\Rightarrow$ (3) are clear. Proof of (3) $\Rightarrow$ (1). Consider an ideal I such that $(a) \subset I \subset A$, say, $I = (b)$. Then $a \in I$, that is,

$a = bc$ for some $c \in A$. By irreducibility of a, one among b, c is a unit in A. If b is a unit then $I = A$. If c is a unit then $(a) = I$. □

Definition 34. Let A be an integral domain. We say that A is a **unique factorisation domain** or UFD if the following holds. Every nonzero element of A can be written $a_1 \cdots a_n$ where a_i is an irreducible element of A, for all i. Moreover, if $b_1 \cdots b_m$ is another such factorisation, then $m = n$ and there exists $\pi \in S_n$ such that for all i, we have an equality of ideals $(a_i) = (b_{\pi(i)})$.

Proposition 35. *Every PID is a UFD. In particular, so are $\mathbb{Z}$ and $K[X]$ for K a field.* □

2.3 Prime fields

Theorem 36 (First isomorphism theorem for rings)**.** *Let $f\colon A \to B$ be a ring homomorphism with kernel I and image C. Then C is a subring of B, and there exists an isomorphism $A/I \to C$ defined by $a + I \mapsto f(a)$.* □

Let A be a ring. Then there is a unique ring homomorphism $\theta\colon \mathbb{Z} \to A$. Indeed, we must have $\theta(1) = 1$ and therefore, if $n \in \mathbb{Z}_{\geq 0}$ then $\theta(n) = 1 + \cdots + 1$ (n terms) and $\theta(-n) = -\theta(n)$. Conversely, it should be clear that this defines a homomorphism θ.

The kernel of θ is an ideal in $\mathbb{Z}$, and therefore of the form $n\mathbb{Z}$ for a unique $n \in \mathbb{Z}_{\geq 0}$; see proposition 32. We call n the **characteristic** of A.

Proposition 37. *Let A be a ring. Then A contains a smallest subring. It is isomorphic to $\mathbb{Z}/n$ where n is the characteristic of A.*

Proof. First one proves that the image of $f_A\colon \mathbb{Z} \to A$ is the smallest subring of A. By theorem 36, the first isomorphism theorem for rings, the image of f_A is isomorphic to $\mathbb{Z}/\ker(f_A) = \mathbb{Z}/n\mathbb{Z}$. □

Definition 38. Let K be a field. It is clear that there exists a smallest subfield of K. It is called the **prime subfield** of K. A **prime field** is a field equal to its own prime subfield.

Proposition 39.

(a) *The fields $\mathbb{Q}$ and $\mathbb{Z}/p$ (for p a prime number) are prime fields. They are the only prime fields up to isomorphism.*

(b) *Let K be a field of characteristic n and prime subfield K_0. Then either $n = 0$ or n is a prime number. If $n = 0$ then $K_0 \cong \mathbb{Q}$. If $n = p$ is a prime number then $K_0 \cong \mathbb{Z}/p$.* □

2.4 Exercises

(2.4) Let R be a ring. Prove that R is an integral domain if and only if it can be embedded into a field. (We say that R can be embedded into a field if it is isomorphic to a subring of a field).

(2.5) Suppose that $f = X^{n-1} + X^{n-2} + \cdots + 1 \in \mathbb{Q}[X]$ is irreducible, with $n \geq 1$. Prove that n is a prime number.

(2.6) Let A be a ring of characteristic p (a prime number).

(a) Prove that the binomial coefficient $\binom{p}{k}$ is divisible by p if $0 < k < p$.

(b) Prove that $F\colon A \to A$ defined by $F(a) = a^p$ is a ring homomorphism. It is called the **Frobenius ring homomorphism**. Hint: use the binomial theorem.

(c) Give examples showing that F need not be surjective or injective.

(d) Prove $(a_1 + \cdots + a_n)^p = a_1^p + \cdots + a_n^p$ for all $a_i \in A$.

(e) Prove Fermat's theorem that $p \mid n^p - n$ for all integers n.

(2.7) Let $\mathbb{F}_q$ be a finite field of q elements. Prove the following identity in $\mathbb{F}_q[X]$:

$$\prod_{\alpha \in \mathbb{F}_q} (X - \alpha) = X^q - X.$$

[You may use results about finite groups, and that $K[X]$ is a unique factorisation domain for all fields K.]

(2.8) Prove that the polynomial ring $K[X]$ over any field K has infinitely many irreducible polynomials. Hint: Imitate Euclid's proof that there are infinitely many prime numbers.

(2.9) Let $f\colon \mathbb{R} \to \mathbb{R}$ be a ring homomorphism. Prove that f is the identity. (You may use that $f(1) = 1$ but not that f is continuous). This result is quite curious, since there are uncountably many homomorphisms $\mathbb{C} \to \mathbb{C}$.