Chapter 1

Basics Properties of Rings

Definition 1.1. A ring (with 1) is a set R along with elements $0, 1 \in R$ and maps $+ : R \times R \to R$, $\times : R \times R \to R$ (write $a + b$ for addition and abbreviate $a \times b$ by ab) such that

(1) $(R, +)$ is an abelian group with 0 as identity

(2) $(R, \times)$ is a semigroup with identity 1 (i.e. $\forall a, b \in R, (ab)c = a(bc)$)

(3) $\forall a, b, c, a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

Example.

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ with the obvious choices for $0, 1, +, \times$ are rings
- $\mathbb{R}[x]$ (the polynomials with real coefficients) is a ring

Observe that $\mathbb{R}$ is a group under $+$. So $\forall a \in \mathbb{R}, \exists$ inverse $b \in \mathbb{R}$ such that $a + b = 0$. We will call this inverse $-a$: $(-a) + a = 0$. Further, we define $x - y = x + (-y)$ as subtraction. In general we cannot do division in rings!

Note. Some people do not demand $1 \in R$ and do not demand $1r = r = r1$. For these people, I define a "ring with 1". Other people demand $0 \neq 1$ as an extra axiom. This barely makes any difference as $0 = 1 \implies R = \{0\}$.

Example. $M_n(R)$ along with usual $+, \times$ and $0 = 0_n$ is a ring. The identity element is $1 = I_n$ (Note that $(AB)C = A(BC)$ but $AB \neq BA$ in general.

Definition 1.2. A ring R is commutative if $ab = ba \ \forall a, b \in R$.

Example. Residue Class Rings. Take $m \geq 1$ to be an integer and define an equivalence relation on $\mathbb{Z}$ by

$$a \sim b \Leftrightarrow m \text{ divides } a - b \Leftrightarrow a \equiv b \bmod m.$$

Let $\mathbb{Z}/m\mathbb{Z}$ denote the set of equivalence classes:

$$\mathbb{Z}/m\mathbb{Z} = \{0, 1, \ldots, m - 1\} = \{[0]_m, [1]_m, \ldots, [m - 1]_m\}.$$

It turns out that $\mathbb{Z}/m\mathbb{Z}$ is a ring under the operations

$$[a] + [b] = [a + b] \qquad\qquad [a] \times [b] = [ab]$$

E.g. $\mathbb{Z}/5\mathbb{Z}$ is a ring.

Note. Our intuition is bases on rings like $\mathbb{Z}, \mathbb{Q}, \dots$ which are all well-behaved rings. In general rings are not so well-behaved!

Example.

- Let $R = M_2(\mathbb{R})$ and $a = b = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Then $a \neq 0, b \neq 0$, but $ab = 0$.
- Let $R = \mathbb{Z}/6\mathbb{Z}, = [2], b = [3]$. Then $a \neq 0, b \neq 0$, but $ab = [0]$.
- Polynomials can have too many roots, e.g. consider $x^2 - 1$ in the ring $\mathbb{Z}/8\mathbb{Z}$: $x = [1], [3], [5], [7]$ are all roots of the polynomial.
- Cancellation can also fail, i.e. $ra = rb \nRightarrow a = b$. E.g. let $r = [2], a = [2], b = [0]$ in $\mathbb{Z}/4\mathbb{Z}$.

All this happens because we cannot divide.

Definition 1.3. A ring R is called a division ring if $R/\{0\}$ is a group under multiplication with 1 as the identity ($1 \neq 0$). In other words, $\forall a \neq 0, \exists b$ such that $ab = ba = 1$.

Example.

- $\mathbb{Z}$ is not a division ring (as 2 does not have an inverse under $\times$)
- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are all division rings under the usual operations of addition and multiplication.

A commutative division ring is called a field. For example, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are fields.

Fields are great: the whole theory of vector spaces works over a general field.

Example. The ring of polynomials in $\mathbb{R}$, $\mathbb{R}[x]$, is not a field, as $\frac{1}{x}$ is not a polynomial.

Definition 1.4. If R is a ring and $S \subseteq R$ is a subset, we say S is a subring if $0, 1 \in S$ and $t + s, st \in S\ \forall s, t \in S$ and furthermore if S becomes a ring itself with this $0, 1, +, \times$, i.e. S satisfies the axioms.

Lemma 1.5. *If R is a ring and $S \subseteq R$ is a subset of R such that $0, 1 \in S$ and $s + t, st, s - t \in S\ \forall s, t \in S$ then S is a subring of R.*

Proof. We need to check the three axioms: $(S, +)$ is a group, because $s, t \in S \implies s - t \in S$. So inverses exist. Also it is obviously abelian and the other axioms are obvious, e.g. say $r, s \in S$. Need $r(s + t) = rs + rt$: but this is true in R, so it must be true in S. $\square$

Example.

- $\mathbb{Z}$ is a subring of $\mathbb{Q}$
- $\mathbb{Q}$ is a subring of $\mathbb{R}$
- $\mathbb{R}$ is a subring of $\mathbb{C}$.
- Let $d \in \mathbb{Z}$ be an integer that is not a square. Define $\mathbb{Z}[\sqrt{d}]$ to be the following subset of $\mathbb{C}$:

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} | a, b \in \mathbb{Z}\}.$$

Lemma 1.6. $\mathbb{Z}[\sqrt{d}]$ *is a ring.*

Proof. It is a subset of $\mathbb{C}$ so let's use Lemma 1.5: We need to check that if $a + b\sqrt{d} = r \in \mathbb{Z}[\sqrt{d}]$ and $a' + b'\sqrt{d} = r' \in \mathbb{Z}[\sqrt{d}]$, then $r \pm r', rr' \in \mathbb{Z}[\sqrt{d}]$. $r \pm r' \in \mathbb{Z}[\sqrt{d}]$ is easy to check and

$$rr' = (a + b\sqrt{d})(a' + b'\sqrt{d}) = (aa' \underset{\in\mathbb{Z}}{+} bb'd) + (ab' \underset{\in\mathbb{Z}}{+} ba)\sqrt{d}.$$

$\square$

A slightly less obvious fact about $\mathbb{Z}[\sqrt{d}]$: if $a + d\sqrt{d} = a' + d'\sqrt{d}$, then $a = a', b = b'$ (where $a, a', b, b' \in \mathbb{Z}$). For $a + d\sqrt{d} = a' + d'\sqrt{d}$,

$$\begin{aligned} a - a' = & b'\sqrt{d} - d\sqrt{d} \\ = & \ (b' - b)\sqrt{d}. \end{aligned}$$

If $b \neq b'$, then $\sqrt{d} = \frac{a-a'}{b-b'} \in \mathbb{Q}$, but $\sqrt{d} \notin \mathbb{Q}$. Hence $b = b' \implies a - a' = 0 \implies a = a'$.

Example. $\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} | a, b \in \mathbb{Q}\}$ (for $\sqrt{d} \notin \mathbb{Z}$) is a ring (by the same proof as before: subring of $\mathbb{C}$).

Lemma 1.7. $\mathbb{Q}[\sqrt{d}]$ *is a field.*

Proof. $\mathbb{Q}[\sqrt{d}]$ is clearly commutative, so all I need to do is to check that if $0 \neq r \in \mathbb{Q}[\sqrt{d}]$, then $\frac{1}{r} \in \mathbb{Q}[\sqrt{d}]$. So assume $0 \neq r = a + b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$. Then $a^2 - b^2 d \neq 0$ for if $a^2 - b^2 d = 0$, then $a^2 = b^2 d$ and either $b = 0$ or $d = \left(\frac{a}{b}\right)^2$. But d is not square by assumption, hence

$$b = 0 \implies a^2 = 0 \implies a = 0 \implies r = 0$$

contradiction. So $\mathbb{Q} \ni t = a^2 - b^2 d \neq 0$ and from above we see that $\frac{1}{r} = \frac{a}{t} - \frac{b}{t}\sqrt{d}$. $\square$

Example. The set of all functions $f : [0, 1] \to \mathbb{R}$ is naturally a ring. the role of 0 is played by the function sending any $x \in [0, 1]$ to 0 and 1 is the function sending any $x \in [0, 1]$ to 1. Define $f + g$ by $(f + g)(x) = f(x) + g(x)$ and fg by $(fg)(x) = f(x)g(x)$.

Exercise. This defines a ring.

Proposition 1.8. *Let R be a ring and say $r, s, r_i, s_i \in R$.*

(a) $r0 = 0r = 0\ \forall r, s \in R$

(b) if $-r$ denotes the inverse of r under addition, then

$$(-r)s = r(-s) = -(rs) \quad (-r)(-s) = rs\ \forall r, s \in R$$

(c) $\left(\sum_{i=1}^{n} r_i\right)\left(\sum_{j=1}^{n} s_j\right) = \sum_{i,j=1}^{n} r_i s_j$

(d) if $r \in R$ and $rs = s\ \forall s \in R$, then $r = 1$.

(e) if R is a ring and $0 = 1$ in R then $R = \{0\}$ has one element (conversely, $\{0\}$ is a ring).

Proof.

(a) standard exercise in group theory: $0 + 0 = 0$, hence $r(0+0) = r(0) \implies r0 + r0 = r0 \implies r0 = 0$. Similarly for $0r = 0$.

(b) to check $(-r)s = -(rs)$ is need to check that $(-r)s + rs = 0$. Then by distributivity, it suffices to prove that$(-r + r)s = 0$. But $-r + r = 0$ and $0s = 0$ by (a). Hence $r(-s) = -rs$. Now

$$(-r)(-s) = -(r(-s)) = -(-rs) = rs$$

since R is an additive group.

(c) tedious induction on $m + n$ using distributivity.

(d) set $s = 1$.

(e) if $r \in R$, then $r = r1 = r0 = 0$ by (a). Conversely, check that $\{0\}$ satisfies all the axioms.

$\square$

Convention: By definition $0, 1 \in R$ and define $2 \in R$ to be $1 + 1$. Similarly for $3, 4, ..., 73, ...$ Further, define $-1 \in R$ to be the additive inverse of 1 such that $1 + (-1) = 0$ and similarly $-n$ to be the additive inverse of n. We obtain a map $\mathbb{Z} \to R$ which may or may not be an injection, e.g. $73 = 0$ in $\mathbb{Z}/73\mathbb{Z}$ and $73 = 1$ in $\mathbb{Z}/72\mathbb{Z}$.

Definition 1.9. If R is a ring and if $0 \neq a \in R$, then we say a is a left-divisor of zero if $\exists b \neq 0$ in R such that $ab = 0$ (similarly for right-divisor of zero. Note that if R is commutative, these notions coincide and we say that a is a zero divisor). If $a \in R$ and $\exists b \in R$ such that $ab = ba = 1$, then we say a is a unit (for R commutative, we only need $ab = 1$ for a to be a unit). Write R^* for the set of units in R.

Remark. R^* is a group, as associativity and identity are ring axioms and inverses exists by definition of a unit.

Example.

- 2 is a zero divisor in $\mathbb{Z}/6\mathbb{Z}$ as $2 \times 3 = 0$ in this ring but $2 \neq 0, 3 \neq 0$.
- 5 is a unit in $\mathbb{Z}/6\mathbb{Z}$ since $5 \times 5 = 1$ in this ring.
- The matrix $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ is a left and ring zero divisor in $M_2(\mathbb{R})$ as
$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = 0$$
(note that if $a \in R$ and $a^n = 0$ for some $n \geq 1$ then a is nilpotent).
- the units in $M_2(\mathbb{R})$ are the invertible matrices (i.e. $GL_2(\mathbb{R})$) .
- $R = \mathbb{Z}$ has no zero divisors as $ab = 0 \implies a = 0$ or $b = 0$.
- The units in $\mathbb{Z}$ are $\mathbb{Z}^* = \{\pm 1\}$.
- If R is a field (or even a divison ring), then $R^* = R \setminus \{0\}$.

Definition 1.10. A ring R is an integral domain if

(1) R is commutative

(2) $0 \neq 1$

(3) R has no zero divisors (i.e. if $ab = 0$, then $a = 0$ or $b = 0$).

Example.

- $\mathbb{Z}$ is an integral domain
- any field is an integral domain
- the zero ring $\{0\}$ is not an integral domain (which is a wise convention).
- any subring of a an integral domain is again an integral domain $\implies$ any subring of $\mathbb{C}$, e.g. $\mathbb{Z}[\sqrt{d}], \mathbb{Q}[\sqrt{d}]$ etc., is an integral domain.

Lemma 1.11. *Let m be a positive integer and let R be the ring $\mathbb{Z}/m\mathbb{Z}$. Then R is an integral domain iff m is prime.*

Proof. Note first that if $m = 1$ is not prime, then $\mathbb{Z}/1\mathbb{Z} = \{0\}$ is not an integral domain. If $m = p$ is prime, then I need to check that $\mathbb{Z}/p\mathbb{Z}$ is an integral domain: clearly, we have that $\mathbb{Z}/p\mathbb{Z}$ is commutative and $0 \neq 1$. Now say that $a, b \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$: lift a to $A \in \mathbb{Z}$ and b to $B \in \mathbb{Z}$. Since $a, b \neq 0$ we have that $p \nmid A, p \nmid B$, hence $p \nmid AB$. So $AB \neq 0 \bmod p \implies ab \neq 0$. So $\mathbb{Z}/p\mathbb{Z}$ is an integral domain if p is prime. To show the converse, assume that m is not prime, i.e. $m = ab$ with $1 < a < b < m$. Then $a, b \neq 0$ and $ab = 0$ in $\mathbb{Z}/m\mathbb{Z}$. So $\mathbb{Z}/m\mathbb{Z}$ is not an integral domain. □

Lemma 1.12.

(i) if R is a ring and $a \in R^*$ with $ar = as$, then $r = s$

(ii) if R is an integral domain and if $a \neq 0$ and $ar = as$, then $r = s$.

Proof. For the first part, choose $b \in R$ such that $ba = 1$. Then

$$ar = as \implies bar = bas \implies 1r = 1s \implies r = s.$$

For the second part, let $a \neq 0$ and $ar = as$. Then $a(r - s) = 0$. But R is an integral domain and $a \neq 0$. So

$$r - s = 0 \implies r = s.$$

□

Note. (ii) is not a special case of (i), for example $2 \in \mathbb{Z}$ is non-zero but not a unit.

Abstract Polynomial Rings

Let R be any commutative ring. Define the polynomial ring $R[x]$ of polynomials to be, formally, the set of all infinite sequences $(c_0, c_1, \ldots, c_n, \ldots)$ with $c_i \in R\ \forall i$ but all but finitely many c_i equal to zero. Informally, we think of $(c_0, c_1, \ldots, c_n, 0, 0 \ldots)$ as being $c_0 + c_1 x + \ldots + x^n$. Define $0 = (0, 0, \ldots)$, $1 = (1, 0, 0, \ldots)$ and

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots)$$

and

$$(a_0, a_1, \ldots)(b_0, b_1, \ldots) = (c_0, c_1, \ldots)$$

with $c_n = \sum_{i=0}^{n} a_i b_{n-i}$.

Exercise. This defines a ring.

Notation. Call this ring $R[x]$ and write $f = (a_0, a_1, \ldots, a_d, 0, 0, \ldots) = a_0 + a_1 x + \ldots + a_d x^d$. If $a_d \neq 0$ then we say that d is the degree of f if $a_n = 0\ \forall n > d$.

Proposition 1.13. *If R is an integral domain then $R[x]$ is also an integral domain.*

Proof. Say $0 \neq a, b \in R[x]$. Write

$$a = a_0 + a_1 x + \ldots + a_d x^d$$

$$b = b_0 + b_1 x + \ldots + b_e x^e$$

with $a_d, b_e \neq 0$. Then $ab = \text{STUFF} + a_d b_e x^{d+e}$. Now, as R is an integral domain, $a_d b_e \neq 0 \implies ab \neq 0$. □

If R is a commutative ring, define $R[x_1, x_2] = (R[x_1])[x_2]$.

Corollary 1.14. *If R is an integral domain, then so is $R[x_1, \ldots, x_n]$.*

Proof. Do induction on n. $\square$

We say that a subfield of a ring R is a subring $S \subseteq R$ that is a a field. For example, R is a subring of $R[x]$ (the constant polynomials) but also a subfield of $\mathbb{R}[x]$.

Remark. If K is a subfield of the ring R, then R is naturally a vector space over K. For example, $\mathbb{C}$ is a vector space over $\mathbb{R}$.

Lemma 1.15. *A finite integral domain is a field.*

Proof. Say that $0 \neq a \in R$ with R being a finite integral domain. We need to find an inverse for a, i.e. b such that $ab = 1$. Consider the map $m_a : R \to R$ given by $m_a(r) = ar$ for $r \in R$. m_a is injective, for if $m_a(r) = m_a(s)$, then $ar = as \implies r = s$ by 1.12(ii). Hence m_a is injective. Also m_a is surjective since R is finite. Hence it is a bijetion, so we can choose b such that $m_a(b) = ab = 1$. $\square$

Trickier: a finite division ring is a field. This is known as the Artin-Wedderburn Theorem.

Corollary 1.16. *The ring $\mathbb{Z}/m\mathbb{Z}$ is a field iff m is prime.*

Proof. By 1.11 and 1.15 and the fact that a field is an integral domain. $\square$

Chapter 2

Homomorphisms, Ideals & Quotient Rings

Definition 2.1. Let R and S be rings. A map $\varphi : R \to S$ is a ring homomorphism if

- **(i)** $\varphi(0) = 0, \varphi(1) = 1$
- **(ii)** $\varphi(a + b) = \varphi(a) + \varphi(b)$
- **(ii)** $\varphi(a \times b) = \varphi(a) \times \varphi(b)$

Remark. From Group Theory, we know $\varphi(-x) = -\varphi(x)$ and so $\varphi(x - y) = \varphi(x) + -\varphi(y)$

Definition 2.2. $\varphi : R \to S$ is an isomorphism if $\exists$ a ring homomorphism $\psi : S \to R$ such that $\varphi \circ \psi$ and $\psi \circ \varphi$ are the identity map.
In practice, a ring homomorphism $\varphi : R \to S$ is an isomorphism iff φ is a bijection.

Special case: $R = S$. A ring homomorphism $\varphi : R \to R$ is called an endomorphism and an isomorphism $\varphi : R \to R$ is called an automorphism.

Example.

1. $\mathbb{Z} \to \frac{\mathbb{Z}}{n\mathbb{Z}}$ (where n is a positive integer) given by $t \to t \bmod n$ is a homomorphism: $[0]$ is the zero in $\frac{\mathbb{Z}}{n\mathbb{Z}}$, $[1]$ is the one in $\frac{\mathbb{Z}}{n\mathbb{Z}}$ and if $a, b \in \mathbb{Z}$, then
$$(ab) \bmod n = (a \bmod n)(b \bmod n)$$
(this is the definition of the product in $\frac{\mathbb{Z}}{n\mathbb{Z}}$). And similarly
$$(a + b) \bmod n = (a \bmod n) + (b \bmod n)$$
(this is the defintion of addition in $\frac{\mathbb{Z}}{n\mathbb{Z}}$). So this is a ring homomorphism.

2. $R = \mathbb{C}$ with $f : R \to R$ given by $f(z) = f(\overline{z})$ is a ring homomorphism: $\overline{0} = 0, \overline{1} = 1$ and

$$f(a+b) = \overline{a+b} = \overline{a} + \overline{b} = f(a) + f(b)$$

$$f(ab) = \overline{ab} = \overline{a}\overline{b} = f(a)f(b).$$

Notice that since f is bijective, this is in fact an isomorphism (and an automorphism). f is its own inverse, i.e. $f \circ f =$ identity.

3. $R = \mathbb{R}[x], S = \mathbb{R}$. Choose some $\lambda \in \mathbb{R}$. Define $\varphi : \mathbb{R}[x] \to \mathbb{R}$ by $\varphi(f) = f(\lambda)$, where $f(x) \in \mathbb{R}[x]$ (e.g. if $\lambda = 2$ and $f = x^2 + 1$, then $\varphi(f) = f(2) = 5$). φ is called the evaluation homomorphism. Note that the polynomial 1 is not the same as the polynomial x: $\varphi(x) = \lambda$, but $\varphi(1) = 1$. φ is easily checked to be a ring homomorphism.

4. The "Frobenius Homomorphism": Say R is a commutative ring and say $p = 0$ in R (e.g. $R = \frac{\mathbb{Z}}{p\mathbb{Z}}$ or $\frac{\mathbb{Z}}{p\mathbb{Z}[x]}$). Define $\varphi : R \to R$ by

$$\varphi(x) = x^p = \underbrace{(x \cdot x \cdot x \cdot \ldots \cdot x)}_{p \text{ times}}$$

(or $\varphi(r) = r^p$). This is also a ring homomorphism as $\varphi(0) = 0, \varphi(1) = 1$ and

$$\varphi(rs) = (rs)^p = r^p s^p = \varphi(r)\varphi(s)$$

$$\varphi(r+s) = (a+b)^p = a^p + pa^{p-1}b + \cdots + \begin{pmatrix} p \\ i \end{pmatrix} a^{p-i}b^i + \cdots + b^p.$$

But $p \mid \begin{pmatrix} p \\ i \end{pmatrix}$ if $1 \leq i \leq p-1$. Therefore $\begin{pmatrix} p \\ i \end{pmatrix} = 0$ in R and hence $(a+b)^p = a^p + b^p = \varphi(a) + \varphi(b)$.

5. $R = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Define $\varphi : R \to R$ by

$$\varphi(a + b\sqrt{2}) = a - b\sqrt{2}.$$

φ is a ring homomorphism because:
- $\varphi(0) = 0$
- $\varphi(1) = 1$
- $\varphi((a+b\sqrt{2})(c+d\sqrt{2})) = \varphi(ac+2bd+\sqrt{2}(bc+ad)) = ac+2bd-\sqrt{2}(bc+ad)$

$$\varphi(a+b\sqrt{2})\varphi(c+d\sqrt{2}) = (a-b\sqrt{2})(c-d\sqrt{2}) = ac+2bd-(bc+ad)\sqrt{2} \implies \varphi(xy) = \varphi(x)\varphi(y).$$

6. Inclusions: $\mathbb{Q} \hookrightarrow \mathbb{R}, \mathbb{R} \hookrightarrow \mathbb{C}, M_2(\mathbb{R}) \hookrightarrow M_2(\mathbb{C})$ are all ring homomorphisms.

Remark. Injective ring homomorphisms $R \to S$ are "the same as" subrings of S.

Lemma 2.3. *Let $\varphi : R \to S$ be a ring homomorphism and let T be the image of φ, i.e. $T = \{\varphi(r) | r \in R\}$. Then T is a subring of S.*

Proof. By Lemma 1.5, we need to check that Tcontains 0,1 and that T is closed under $+, -, \times$. Clearly $\varphi(0) = 0, \varphi(1) = 1$, so $0, 1 \in T$. Now say $a, b \in T$. Let $a = \varphi(r)$ and $b = \varphi(s)$. Then

$$\begin{aligned} a + b &= \varphi(r) + \varphi(s) = \varphi(r + s) \\ a - b &= \varphi(r) - \varphi(s) = \varphi(r - s) \\ ab &= \varphi(r)\varphi(s) = \varphi(rs). \end{aligned}$$

Hence T is a subring of S. □

In fact, any map $\varphi : X \to Y$ between sets factors as $X \xrightarrow{\pi} Z \xrightarrow{i} Y$ with π a surjection and i an injection ($Z \subseteq Y$ is image of φ). The above Lemma 2.3. shows that the same is true for rings: any ring homomorphism $\varphi : R \to S$ is $R \xrightarrow{\pi} T \xrightarrow{i} S$, π a surjection, i an injection and π, i are ring homomorphisms.

We have already seen an example of a surjective ring homomorphism: $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, n \geq 1$.

Question: Are there any more surjections $\varphi : \mathbb{Z} \to R$, where R is ring of a completely different type to $\mathbb{Z}/n\mathbb{Z}$?

Answer: We will answer this soon.

Here is a problem that we need to solve first: Say $\varphi : R \to S$ is a ring homomorphism. We have seen that $\mathrm{Im}(\varphi)$ is a subring of S. Is it also true that $\ker(\varphi) = \{r \in R : \varphi(r) = 0\}$ is a subring of R (for example the kernel of $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is the set of integers which are multiples of $m = \{\dots, -m, 0, m, \dots\}$)? No, as this is not a subring of $\mathbb{Z}$ in general (for example it is very likely that $1 \notin \ker(\varphi)$).

Definition 2.4. A subset $I \subseteq R$ (where R is a ring) is called a left ideal if

(1) I is a subgroup of R (under $+$)

(2) If $r \in R$ and $i \in I$, then $ri \in I$.

Similarily for right ideals. A subset $I \subseteq R$ (R a ring) is called a bi-ideal, or a 2-sided ideal, if I is a left and right ideal.

Remark. If R is a commutative ring, then all three of these notions coincide, and we will call I an ideal, i.e. if

(1) I is a subgroup of R under $+$

(2) $ri \in I$ for $\forall r \in R, i \in I$.

Notation. If I is an ideal of R, we write $I \trianglelefteq R$ or $I \triangleleft R$.

Example.

1. If R is a ring, then $\{0\}$ and R are both bi-ideals of R.
2. Let $R = \mathbb{R}[x]$ be the set of all polynomials with real coefficients. Let $I = x\mathbb{R}[x]$ be the polynomials with no constant term. If $f = a_1x + \cdots +, g = b_1x + \cdots + \in I$, then $f \pm g = (a_1 \pm b_1)x + \dots$ has no constant term and so $\in I$. Also, $0 \in I$, therefore I is a subgroup of $(R, +)$. Next, we need to check that if $f \in I$ and $g \in R$, then $fg \in I$ (i.e. R is a commutative ring). $f = a_1x + a_2x^2 + \dots, g = b_0 + b_1x + \dots$ ($b_0 \neq 0$ is okay), then $fg = a_1b_0x + O(x^2)$. Therefore, $fg \in I$, so $I \trianglelefteq R$, i.e. I is an ideal of R.

3. Say $m \geq 1$. Set $I = m\mathbb{Z} = \{mt : t \in \mathbb{Z}\} \subseteq R = \mathbb{Z}$ (m is an integer), I is the set of multiples of m.

   Remark. I is the kernel of the map from $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

   Claim. I is an ideal. For $0 = 0m \in I$. If $a, b \in I$, then $a = ms, b = mt$ for $s, t \in \mathbb{Z}$. Therefore $a \pm b = m(s \pm t) \in I$, hence I is a subgroup of $(\mathbb{Z}, +)$. Finally, if $r \in R = \mathbb{Z}$, and $i \in I$, then $i = mu$ for some $u \in \mathbb{Z}$ and so $ri = rmu = m(ru) \in I$. Therefore, I is an ideal of $R = \mathbb{Z}$ (note that R is a commutative ring).

   Remark. If $m = 0$, then $\{mr : r \in \mathbb{Z}\} = \{0\}$ is also an ideal, and everything in the above proof works, giving another proof that $\{0\} \trianglelefteq \mathbb{Z}$.

4. All ideals of $\mathbb{Z}$ are of the form $m\mathbb{Z} = \{mr : r \in \mathbb{Z}\}$ for $m = 0, 1, 2, \ldots$. For, say $I \subseteq \mathbb{Z}$ is an ideal, then if I contains a negative number $n < 0$, then (I is a subgroup) and $-n > 0$ and $-n \in I$. So either $I = \{0\}$ or I contains some positive integer. Let m be the smallest positive integer in I. Easy check

   $$I = \{\ldots, -2m, -m, 0, m, 2m, \ldots\} = m\mathbb{Z}.$$

   For, certainly $m\mathbb{Z} \subseteq I$ as $m \in I$ and I is a group, and if $t \in I$, with t not a multiple of m, then $\exists n$ such that

   $$mn < t < m(n+1)$$

   and $t - mn \in I$, but $0 < t - mn < m$, contradicting the definition of m being the smallest positive integer in I. So $I = m\mathbb{Z}$.

Ideals are hardly every subrings. In fact:

Lemma 2.5. *If I is a left-ideal of R, and $1 \in I$, then $I = R$.*

Proof. Say $r \in R$. Then

$$I \in I \implies r1 \in I \implies r \in I,$$

so $I = R$. □

Remark. This lemma (2.5) also holds for right ideals.

If R is a non-commutative ring, then we can define a new ring R_{opp} by $R_{opp} = R$ (as a set) and $0, 1$ as before, with the same rule of addition, but $a \times b$ in R_{opp} is defined to be $b \times a$ in R. So the left ideals of R_{opp} are the right ideals of R.

Definition 2.6. If $\varphi : R \to S$ is a ring homomorphism, define the kernel of φ to be

$$\varphi^{-1}(\{0\}) = \{r \in R : \varphi(r) = 0\}.$$

Proposition 2.7. *The kernel of a ring homomorphism φ is an ideal.*

Proof. φ is by definition a group homomorphism (with the group law $+$ and identity 0), so the kernel of φ is a subgroup by M2PM2. Now say that $r \in R$ and $i \in \ker\varphi$, i.e. $\varphi(i) = 0$. We want to show that ri and ir are in $\ker\varphi$. But

$$\varphi(ri) = \varphi(r)\varphi(i) = \varphi(r) \cdot 0 = 0 \implies ri \in \ker\varphi$$

by Proposition 1.8a. Similarly, $ir \in \ker\varphi$. Hence $\ker\varphi$ is a bi-ideal. □

Next, we will define the quotient ring R/I, where R is a ring and I is a bi-ideal of R. This is well-defined, for if $I \trianglelefteq R$ is a bi-ideal, then I is a subgroup of $(R, +)$, so we can define the quotient group R/I per group theory. Recall that an element of R/I is a subset $r + I$ of R,

$$r + I = \{r + i : r \in I\}.$$

We will now aim to put a ring structure on R/I such that a natural map $R \to R/I$ is a ring homomorphism with kernel I.

Question: Is every bi-ideal the kernel of a homomorphism?

Set up: Let R be a ring and $I \trianglelefteq R$ a bi-ideal of R. Our goal is to form the quotient ring R/I. So far we know that $(R, +)$ is a group and $I \subseteq R$ is a normal subgroup. Hence the quotient group R/I exists and has well-defined addition. Recall that the elements of R/I are I-cosets in R, i.e. subsets of R of the form $r + I = \{r + i : i \in I\}$.We will now make R/I a ring.

Define 0 of R/I to be $0 + I = I$.

Define 1 of R/I to be $1 + I$.

Define $+$ on R/I to be

$$(r + I) + (s + I) = (r + s + I)\,.$$

By group theory, we know that this is well-defined.

For multiplication, define

$$(r + I)(s + I) = rs + I.$$

We need to check that this is well-defined. More precisely, that $r' = r + i, i \in I$ and $s' = s + j, j \in I$. Then $r + I = r' + I$ and $s + I = s' + I$. So we need to check that

$$rs + I = r's' + I,$$

i.e. that is $r's' = rs + k$, for some $k \in I$. Well,

$$r's' = (r + i)(s + j) = rs + is + rj + ij.$$

Set $k = is + rj + ij$. We want to show that $k \in I$. Once we have checked that, we are done. But $i, j \in I$ and $r, s \in R$, so $is, rj \in I$ since I is a bi-ideal. Also, $i, j \in I \implies ij \in I$ since I is also a left-ideal. So $k \in K$ (as $(I, +)$ is a group).

So we have a well-defined product on R/I induced from the product on R. We now claim that R/I is a ring.

1. R/I is a group under addition, by group theory.
2. $$(1 + I)(r + I) = 1r + I = r + I = (r + I)(1 + I),$$

   so $1 + I$ works as the multiplicative identity. Moreover,

   $$((r + I)(s + I))\,(t+I) = (rs + I)\,(t+I) = rst+I = (r+I)\,((s + I)(t + I))\,.$$

Finally,

$$\begin{aligned}
(x+I)\left((y+I)+(z+I)\right) &= (x+I)(z+y+I) = x(y+z)+I \\
&= xy+xz+I \qquad \text{by distributivity in } R \\
&= (xy+I)(xz+I) \\
&= (x+I)(y+I)+(x+I)(z+I)
\end{aligned}$$

and similarly for the other distributivity law.

Therefore, R/I is a ring.

Definition 2.8. Let R be a ring and I be a bi-ideal of R. We say that R/I is the quotient ring.

Now, it is easy to check that the natural map $R \to R/I$ given by $r \mapsto r+I$ is a ring homomorphism: the image of 0 is 0, the image of 1 is 1 and if $r \mapsto r+I, s \mapsto s+I$, then $r+s \mapsto r+s+I$ and $rs \mapsto rs+I$. It is just as easy to show that the kernel of $R \to R/I$ is

$$= \{r : r+I = I\} = \{r : r \in I\} = I.$$

The First Isomorphism Theorem strengthens this. It says a surjective ring homomorphsim is determined by its kernel.

Theorem 2.9. *(First Isomorphism Theorem). Say that $\psi : R \to S$ is a homomorphism of rings. Say $I = \ker\psi$. This is an ideal of R by 2.7. Further let $T = Im\psi$. This is a subring of S by 2.3. Then there is a natural isomorphism of rings*

$$R/I \cong T$$

(and indeed ψ induces this natural isomorphism).

Proof. I is a bi-ideal and R/I is a well-defined ring. Our plan will be to define a map $\alpha : R/I \to T$. Say $r+I \in R/I$. Define

$$\alpha(r+I) = \psi(r).$$

Is this well-defined? Say $r' = r+i$. Then $r+I = r'+I$ (this is if and only if). Therefore we need to check $\psi(r) = \psi(r')$. But

$$\psi(r') = \psi(r) + \psi(i) = \psi(r) + 0 = \psi(r)$$

as $I = \ker\psi$. Hence α is well-defined. Now, for injectivity of α, say

$$\alpha(r+I) = \alpha(s+I) \quad r, s \in R.$$

Then by definition of α,

$$\psi(r) = \psi(s) \implies \psi(r-s) = 0$$

since ψ is a ring homomorphism. Therefore $r-s \in \ker\psi = I$. So set $r-s = i$. Then

$$r = s+i \implies r+I = s+I.$$

Hence α is injective. Next, surjectivity: say $t \in T$. We need to find $r \in R$ such that $\alpha(r + I) = t$. Well, $T = \mathrm{Im}(\psi)$, and so $\exists r \in R$ such that $\psi(r) = t$. Then

$$\alpha(r + I) = \psi(r) = t,$$

so α is surjective. Combining, α is bijective. Now, set $\beta : T \to R/I$ to be the inverse of α. We leave it as an exercise to show that β is a ring homomorphism. Then $\alpha + \beta$ and $\alpha \circ \beta$ are the identities. Therefore, α is an isomorphism. $\square$

We saw already that the image of a ring is a ring. However, it is not true that the image of an ideal is an ideal. For example, consider the map $\mathbb{Z} \to \mathbb{C}$ given by $x \mapsto x$. Then $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$, but not of $\mathbb{C}$.

However, the pre-image of an ideal is also an ideal. That is

Proposition 2.10. *Say $f : R \to S$ is a homomorphism of rings. Say $I \subseteq S$ is a left ideal (resp. right ideal, resp bi-ideal). Then*

$$f^{-1}(I) = \{r \in R : f(r) \in I\}$$

is a left ideal (resp. right ideal, resp. bi-ideal) of R.

Proof. Set $J = f^{-1}(I)$. If $\alpha, \beta \in J$, then $f(\alpha) \in I, f(\beta) \in I$. Therefore, $f(\alpha \pm \beta) \in I$. Hence J is closed under $\pm$ and $0 \in J$ and $f(0) = 0$. Therefore J is a subgroup of R (under addition). Now say $r \in R$ and $j \in J$. We need to show that $rj \in J$ (resp. $jr \in J$, resp $rj.jr \in J$). But

$$f(rj) = \underbrace{f(r)}_{\in S}\underbrace{f(j)}_{\in I} \implies f(r)f(j) \in I$$

(since I is a left ideal). Therefore $f(rj) \in I \implies rj \in J$ (for the case of a right ideal or a bi-ideal, the working is just the same). $\square$

Proposition 2.11. *If R is a commutative ring, then R is a field $\iff$ R has exactly two ideals (namely, $\{0\}$ and R).*

Say R is a commutative ring. What are all the ideals of R? We have seen that if $R = \mathbb{Z}$, then the ideals are $\{0\}$ and $n\mathbb{Z}, n \neq 0$. Another class of examples is given by Proposition 2.11. above.

Remark. $R = \{0\}$, the zero ring, is not a field, by definition.

Proof. **($\implies$)** Easy. Firstly note $\{0\} \neq R$ for a field, so there are at least 2 ideals. Now say that R is a field and $I \subseteq R$ is an ideal and $I \neq 0$. We want to show that $I = R$. Choose $0 \neq x \in I$. As R is a field, there exists $y \in R$ such that $yx = 1$. By definition of an ideal, $1 = xy \in I$. Now say that $r \in R$ is arbitrary, then $r = r1 \in I$.

($\impliedby$) We have two ideals, $R \neq \{0\}$ (as otherwise, $R = \{0\}$ has only one ideal). We need to show that if $0 \neq r \in R$, then r has an inverse. So choose $0 \neq r \in R$. Set $I = \{ar : a \in R\}$. It is easily shown that I is an ideal. Furthermore, $r = 1r \in I$, so $I \neq 0$, hence $I = R$, by assumption. Therefore $1 \in R \implies \exists a$ such that $ar = 1$. Hence r has an inverse. So R is a field. $\square$

Therefore the only ideals of $\mathbb{C}$ are 0 and $\mathbb{C}$ (and similarly for $\mathbb{R}$ and $\mathbb{Q}$).

Definition 2.12. Let R be a commutative ring. An ideal P of R is said to be prime, or a prime ideal, if $P \neq R$ and if $a, b \in R$ with $ab \in P$, then either $a \in P$ or $b \in P$. An ideal $M \subseteq R$ is maximal if $M \neq R$ and if J is an ideal with $M \subseteq J \subseteq R$, then either $J = R$ or $M = J$.

Proposition 2.13. *R a commutative ring and $I \subseteq R$ an ideal. Then R/I is a field if and only if I is maximal.*

Proof.

($\Longleftarrow$) Say I is a maximal ideal. We want to show that R/I is a field. By definition, $I \neq R$, therefore $R/I \neq \{0\}$. Now, need to show check that a non-zero element of R/I has an inverse. So choose $x + I \in R/I$ with $x + I$ not the zero element, i.e. $x + I \neq I$, i.e. $x \notin I$. We need to invert $x + I$ in R/I. Define a subset $J \subseteq R$ thus:

$$J = \{ax + i : a \in R, i \in I\}.$$

We claim that J is an ideal. We have that $0 \in J$, since $0 \in R$ and $0 \in I$. Further, if $ax + i_1$ and $bx + i_2$ are in J, $a, b \in R, i_1, i_2 \in I$, then

$$(ax + i_1) \pm (bx + i_2) = \underbrace{(a \pm b)}_{\in R}x + \underbrace{(i_1 + i_2)}_{\in I} \in J,$$

therefore J is a group under addition. Finally if $r \in R, a \in R, i \in I$, then

$$\underset{\in R}{r}\underset{\in J}{(ax + i)} = \underset{\in R}{(ra)}x + \underset{\in I}{ri} \in J.$$

Therefore J is an ideal.
Now, clearly $I \subseteq J$ (simply set $a = 0$). So $I \subseteq J \subseteq R$. But I is maximal. Therefore $J = I$ or $J = R$. But $J \neq I$, as $x \notin I$, but $x \in J$ ($a = 1, i = 0$). So $J = R$. Therefore $1 \in J$, and so we can write $1 = ax + i$ for some $a \in R, i \in I$.
We now claim that $a + I$ is an inverse to $x + I$. For

$$(a + I)(x + I) = (ax + I) = 1 - i + I = 1 + I = 1 \text{ of } R/I.$$

($\Longrightarrow$) Want R/I a field $\Longrightarrow$ I is maximal. Firstly, R/I a field $\Longrightarrow$ $I \neq R$. Now say $I \subseteq J \subseteq R$ and say $J \neq I$. We want $J = R$, then we are done. So let us choose $j \in J$ such that $j \notin I$. Then $j + I \neq I$ in R/I (i.e. $j + I \neq 0$). But R/I is a field. Hence $j + I$ has an inverse, say $k + I$. Therefore

$$(j + I)(k + I) = 1 + I \implies jk \in I + i \implies jk + i = 1$$

for some $i \in I$. Finally, $i \in I \implies i \in J$ and $j \in J \implies jk \in J$. Therefore $jk + i = 1 \in J$. Hence $J = R$.

□

Proposition 2.14. *R is a commutative ring, I is an ideal. Then I is prime iff R/I is an integral domain.*

Corollary 2.15. *Maximal ideals are prime in a commutative ring.*

Proof. M maximal $\overset{2.13}{\Longrightarrow}$ R/M is a field $\overset{obvious}{\Longrightarrow}$ R/M is an integral domain $\Longrightarrow$ M is prime. □

Proof. (of 2.14)
Case 1. $I = R$. Then I is not prime and R/I is not an integral domain. Now say

Case 2. $I \neq R$. Then I is not prime iff $\exists a, b \in R$ such that $ab \in I, a \notin I, b \notin I$.

$$\iff \exists a, b \in R \text{ st. } ab + I = 0 \in R/I$$

with $a + I \neq 0, b + I \neq 0$ in R/I. But

$$\iff \exists a + I, b + I \in R/I \text{ s.t. } a + I \neq 0, b + I \neq 0 \text{ and } (a + I)(b + I) = 0.$$

This is iff R/I is not an integral domain.

□

Remark. It is not hard to prove 2.15 directly (i.e. no quotients). We leave this an an exercise.

Corollary 2.16. *$\{0\}$ is a prime ideal of a commutative ring $R \iff R$ is an integral domain and $\{0\}$ is a maximal ideal of R iff R is a field.*

Corollary 2.17. *Prime ideals are not always maximal.*

Proof. There exists an integral domain that is not a field. for instance, $\mathbb{Z}$, and $\{0\}$ is prime, but not maximal. □

Corollary 2.18. *Maximal ideals of $\mathbb{Z}$ are those of the form $p\mathbb{Z}$, where p is prime. Prime ideals of $\mathbb{Z}$ are of the form $p\mathbb{Z}$, where p is prime, and $\{0\}$.*

Proof. $\mathbb{Z}$ is an integral domain, but not a field. Hence $\{0\}$ is prime, but not maximal. All other ideals of $\mathbb{Z}$ are $n\mathbb{Z}, n > 0$, where n is the smallest positive element of the ideal after definition 2.4, and $\mathbb{Z}/n\mathbb{Z}$ is a field $\overset{1.11}{\iff}$ it is an integral domain $\overset{1.16}{\iff}$ n is prime. □

Remark. We have seen that it is not true that prime $\Longrightarrow$ maximal. Is it true, however, that prime and non-zero $\Longrightarrow$ maximal? This would be consistent with everything we have seen so far. Yet, the answer is no. For example, consider the set $R = \mathbb{C}[x, y]$ with $I = \{rx : r \in R\}$. Clearly $I \neq 0$ as $x \in I$. To check that I is prime but not maximal, we need to check that R/I is an integral domain but not a field. Well, consider the map $\mathbb{C}[x, y] \to \mathbb{C}[y]$ given by $f(x, y) \mapsto f(0, y)$. It is easy to check that f is a surjective ring homomorphism with kernel being the multiples of x. By the First Isomorphism Theorem, $\frac{R}{I} \cong \mathbb{C}[y]$, which is an integral domain, but not a field (by Proposition 1.13).

Generators of Ideals

Definition. Let R be a commutative ring (out of sheer laziness) and $X \subseteq R$ a subset. I want to talk about the ideal generated by X. We say that the ideal generated by X in R is

$$\bigcap_{I \subseteq R \text{ an ideal}, X \subseteq I} I.$$

However, we will ignore this definition implicitly use

Lemma. *If Σ is a set and $\forall \sigma \in \Sigma$, $I\sigma$ is an ideal of R, then*

$$I = \bigcap_{\sigma \in \Sigma} I\sigma$$

is an ideal.

Proof. $0 \in I\sigma \ \forall \sigma \implies 0 \in \cap I\sigma$. Also,

$$i, j \in I\sigma \ \forall \sigma \implies i \pm j \in I\sigma \ \forall \sigma \implies i \pm j \in I$$

$$i \in I, r \in R \implies i \in I\sigma \ \forall \sigma \implies ri \in I\sigma \ \forall \sigma \implies ri \in I.$$

□

Therefore there is a better definition: In the case that X is finite,

Definition 2.19. Let R be a commutative ring and $X \subseteq R$ be a finite subset of R. Say $X = \{x_1, \ldots, x_n\}$. The ideal generated by X is the set

$$I = \{r_1 x_1 + \cdots + r_n x_n : r_i \in R\}.$$

Notation. We write $I = (x_1, \ldots, x_n)$.

Lemma 2.20. *I as defined above is an ideal and it is the smallest ideal of R containing X.*

Proof. $0 \in I$ (set $r_i = 0 \ \forall i$). Also I is closed under $\pm$:

$$(r_1 x_1 + \cdots + r_n x_n) \pm (s_1 x_1 + \cdots + s_n x_n) = (r_1 + s_1) x_1 \pm (r_2 + s_2) x_2 \pm \cdots \pm (r_n + s_n) x_n.$$

Finally, if $r_1 x_1 + \cdots + r_n x_n \in I$ and $a \in R$, then

$$a(r_1 x_1 + \cdots + r_n x_n) = (a r_1) x_1 + \cdots + (a r_n) x_n \in I.$$

Furthermore, if J is any ideal of R with $X \subseteq J$,

$$x_1, \ldots, x_n \in J \implies r_1 x_1, \ldots, r_n x_n \in J \implies r_1 x_1 + \cdots + r_n x_n \in J \implies I \subseteq J.$$

□

Remark. We just showed that the ideal $(x_1, \ldots, x_n)$ is the smallest ideal of R containing $\{x_1, \ldots, x_n\}$. Therefore

$$(x_1, \ldots, x_n) = \bigcap_{X \subseteq I \subseteq R} I.$$

Hence both definitions (hard and easy one) are the same!

If X is infinite, the ideal generated by X is

$$\{r_1x_1 + \cdots + r_nx_n : x_i \in X\}$$

where the sum is finite, and n is as big as you like. Check that this is an ideal.

Special case: $n = 1$ and $X_1 = \{x_1\} = \{x\}, x \in R$. Then $(x) = \{rx : r \in R\} = Rx$ is called a principle ideal.

Not every ideal is principal, for example, consider $I \subseteq \mathbb{C}[x, y]$ defined by $I = (x, y)$, i.e.

$$I = \{fx + gy : f, g \in \mathbb{C}[x, y]\}.$$

Check that I is the set of polynomials in x and y with no constant term. Further, I is the kernel of the map $\mathbb{C}[x, y] \to \mathbb{C}$ given by

$$f(x, y) \to f(0, 0).$$

We claim that I cannot be principal, as if $I = (f)$, then $x \in I$, then f divides x and

$$\implies f = \lambda, \lambda \neq 0 \text{ or } f = \lambda x, \lambda \neq 0$$

and $y \in I \implies f \neq \lambda x$. So $f = \lambda \neq 0$, but $\lambda \notin I$. Therefore (x, y) cannot be principal.

However, if $R = \mathbb{Z}$, and

$$I = (6, 8) = \{6m + 8n : n, m \in \mathbb{Z}\},$$

then $2 \in I$ as $8 - 6 = 2$, and therefore $2t \in I\ \forall t \in \mathbb{Z}$, as I is an ideal. On the other hand $6m + 8n$ is even for all n, m, and so $I = 2\mathbb{Z} = (2)$. Therefore, $(6, 8)$ is a principal ideal.

If fact, we have seen that every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z} = (n)$ for some $n \in \mathbb{Z}$. Hence every ideal is principal.

Question: Let $a, b \in \mathbb{Z}$, not both 0. Let $I = (a, b)$ be an ideal of $\mathbb{Z}$. I must be (d) for some d. What is d?

Definition 2.21. Let R be a commutative ring. We say that an ideal I is finitely generated if

$$I = (x_1, \ldots, x_n),\ x_i \in R.$$

We say that I is principal if $I = (x)$ for some $x \in R$. Further, we say that R is Noetherian if all ideals of R are finitely generated. Finally, we say that R is a principal ideal domain (PID) if

1. R is an integral domain
2. all ideals of R are principal.

We think of these definitions in the following way:

- R noetherian $\iff$ R is "finite dimensional". Therefore R not Noetherian $\implies$ R pathological (much too big).
- R a PID $\implies$ R is $\leq$ "one-dimensional"

Here are some things we cannot prove yet:

- $\mathbb{C}[x]$ is a PID
- $\mathbb{C}[x_1, \ldots, x_n]$ is not a PID if $n > 1$. But it is Noetherian
- $\mathbb{C}[x_1, \ldots]$ is not Noetherian.

We have proved that $\mathbb{Z}$ is a PID, as it is clearly an ID and all ideals are of the form $n\mathbb{Z}$, and hence principal.

Chapter 3

Factorisation in Integral Domains

The purpose of this chapter is to axiomatise and generalise the proof that any $n \in \mathbb{Z} \geq 2$ is uniquely a product of primes. It will turn out that an analogous theorem is true in $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{2}]$, but not $\mathbb{Z}[\sqrt{5}]$.

Throughout this chapter, R will denote an integral domain (so R is commutative).

Definition 3.1. Say $x \in R$ is a unit if $\exists y \in R$ such that $xy = 1$. Write $R^\times =$ the set of units in R (note that $R^\times$ is a group under multiplication with identity 1). We say x divides y (denoted $x \mid y$) if $\exists q \in R$ such that $y = qx$. We call x and y associatives if $y = ux$ for some unit $u \in R$.

Exercise. Show that $x \in R$ is a unit $\iff (x) = R$. Show also that $x \mid y \iff y \in (x) \iff (y) \subseteq (x)$.

Note. The notion of "divides" is the usual one in, for example, $\mathbb{Z}$ or $\mathbb{R}[x]$ etc.

Lemma 3.2. *x and y are associatives* $\iff (x) = (y)$.

Proof. First note that if $y = ux$ and $u \in R^\times$, then $\exists v$ such that $uv = 1$ and $vy = vux = x$. Note that the notion of being associatives is symmetric. If $x = 0$, then $ux = 0$, and the only associative of 0 is $0 = 0 \cdot 1$. On the other hand, if $(0) = (y)$, then $y \in (0) = \{0\}$, and so $y = 0$. Hence the lemma is true for $x = 0$ (or $y = 0$, by symmetry). Now say $x \neq 0$. Then $y = ux$, u a unit. $\implies x = vy$ (where $v = u^{-1}$) and then $(x) = Rx = Rvy = Ry = (y)$ as $Rv = R$. Conversely, if $(x) = (y)$, then $x \in (y) \implies x = ry$ and $y \in (x) \implies y = sx$. Hence

$$x = rsx \implies x(rs - 1) = 0$$

and as $x \neq 0$ and R is an integral domain, $\implies rs - 1 = 0 \implies r \in R^\times$and x and y are associatives. $\square$

Corollary. *Being associatives is an equivalence relation.*

Example. $R = \mathbb{Z}$. The units of $\mathbb{Z}$ are $\{r \in \mathbb{Z} : r \mid 1\} = \{\pm 1\}$. Hence the associatives of n are $\pm n$.

Definition 3.3. We say $r \in R$ is irreducible if $r \neq 0, r$ not a unit, and if $r = ab$, then either a or b is a unit (as an example, $R = \mathbb{Z}$: irreducible $=$ usual notion of prime, up to sign: $r \in \mathbb{Z}$ irreducible $\iff r = \pm p$, p prime). We say $r \in R$ is prime if $r \neq 0, r \neq$ an unit, and if $r \mid ab \implies r \mid a$ or $r \mid b$.

Exercise. Assume that the integers factor uniquely into primes. Check that the primes of $\mathbb{Z}$ are exactly $\pm p$, for p a prime number.

Example. _

1. Let $R = \mathbb{Z}$. 2 is irreducible (as is any prime number) and 3 is too.

2. $R = \mathbb{Z}[i] = \{a + bi : a.b \in \mathbb{Z}\}$. The units of R are found as follows: Define $N : R \to \mathbb{Z}_{\geq 0}$ by $N(a + ib) = a^2 + b^2$, i.e. $N(z) = z\overline{z} = |z|^2$. It is easy to see that $N(rs) = N(r)N(s)$. Say $r \in R^\times$, i.e. $\exists s$ such that $rs = 1$. Then $N(r)N(s) = 1 \implies N(r) = 1$ as $N(r) \in \mathbb{Z}_{\geq 0}$. So if $r = a + ib$ and $r \in R^\times$, then $a^2 + b^2 = 1 \implies r = \pm 1, \pm i$. Conversely, ± 1 and $\pm i$ are units. But $2 \in \mathbb{Z}[i]$ is no longer irreducible, because $2 = (1 + i)(1 - i)$, which is a product of two non-units (hence irreducibility of 2 depends on R). But 3 is still irreducible in $\mathbb{Z}[i]$, as if $3 = rs$, $r, s \in \mathbb{Z}[i]$, then $9 = N(3) = N(r)N(s)$. Let $r = a + bi$, $s = c + di$. Then $(a^2 + b^2)(c^2 + d^2) = 9 \implies a^2 + b^2 \in \{1, 3, 9\}$. But $a^2 + b^2 = 3$ has no solutions in $\mathbb{Z}$. So either $N(r) = 1$ or $N(s) = 1$. So r or s is a unit.

3. Consider $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$. Define $N : R \to \mathbb{Z}_{\geq 0}$ by $N(a + b\sqrt{-5}) = a^2 + 5b^2$ $(= z\overline{z})$. If r is a unit, then $rs = 1$ for some $s \in R$. Then $N(rs) = N(r)N(s) = 1 \implies N(r) = 1$. $r = a + b\sqrt{-5}$ and $a^2 + 5b^2 = 1$. So $b = 0, a = \pm 1$. Hence $r = \pm 1$ and these are both units. Here, there is no solution to $a^2 + 5b^2 = 2$ or $a^2 + 5b^2 = 3$ with $a, b \in \mathbb{Z}$. Hence $2, 3$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$. For example,

   $$2 = rs \implies 4 = N(2) = N(r)N(s) \implies N(r) \in \{1, 2, 4\} \therefore N(r) = 1 \text{ or } N(s) = 1$$

   and $1 + \sqrt{-5}$ is irreducible as $N(1 + \sqrt{-5}) = 6$ and factors of 6 in $\mathbb{Z}_{\geq 1}$ are 1,2,3,6 and 2,3 are not possible. Also $1 - \sqrt{-5}$ is irreducible (norm is also 6). Now $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, i.e. there are two factorisations of 6 into irreducibles. On the other hand, 6 has no factorisations into primes, because none of 2,3,$1 + \sqrt{-5}, 1 - \sqrt{-5}$ are prime. For example, 2 divides

   $$6 = (1 + \underset{a}{\sqrt{-5}})(1 - \underset{b}{\sqrt{-5}})$$

   but$2 \nmid 1 + \sqrt{-5}, 1 - \sqrt{-5}$ (as $\frac{1 \pm \sqrt{-5}}{2} \notin R$) etc. Hence we see that $\mathbb{Z}[\sqrt{-5}]$ has irreducibles that are not prime and some elements factor into irreducibles in more that one way.

On the other hand,

Lemma 3.4. *All primes are irreducible in an integral domain.*

Proof. Say r is prime. Then $r \neq 0$ and r is not a unit. Say $r = ab$. We will show that one of a, b must be a unit. Now, $r = ab \implies r \mid ab$. But r is prime, hence, wlog, $r \mid a$ (could be $r \mid b$ as well). So

$$a = sr, s \in R \implies r = ab = srb \implies r(bs - 1) = 0.$$

As $r \neq 0$, we must have that $bs = 1$, since we are in an integral domain, and hence b is a unit. □

Lemma 3.5. *If $0 \neq r \in R$, then r is prime $\iff$ (r) is a prime ideal.*

Proof. If r is a unit, then r is not prime and $(r) = R$ is not a prime ideal. So say that r is not a unit. Then (r) is a prime ideal $\iff$ $ab \in (r) \implies a \in (r)$ or $b \in (r)$ $\iff$ $r \mid ab \implies r \mid a$ or $r \mid b$. This is equivalent with saying that r is prime. □

Definition 3.6. An integral domain is called an Euclidean domain (ED) if there is some function $\varphi : R\backslash\{0\} \to \mathbb{Z}_{\geq 0}$ such that

(1) $\varphi(ab) \geq \varphi(a)$ if $a, b \neq 0$

(2) If $a, b \in R$ and $b \neq 0$, then one can write $a = qb + r$ with $q, r \in R$ (we call q the quotient and r the remainder) such that either $r = 0$ or $\varphi(r) < \varphi(b)$.

Example.

1. $R = \mathbb{Z}$ and $\varphi(r) = |r|$.
2. For F a field, $R = F[x]$, $\varphi(r) = \deg(f)$.

Exercise. Verify whether the last two examples are indeed Euclidean domains.

Theorem 3.7. *R is an Euclidean Domain $\implies$ R is a prime integral domain.*

Remark. Compare this with the proof that all ideals of $\mathbb{Z}$ are principal.

Proof. Say that R is an Euclidean domain and $I \subseteq R$ is an ideal. If $I = \{0\} = (0)$ than this is clear. Now, assume that $I \neq \{0\}$. Choose $n \in I\backslash\{0\}$ with $\varphi(n)$ minimal. We claim that $I = (n)$. Certainly $(n) \subseteq I$. Now say $i \in I$. We want to show that $i \in (n)$. For $(i = a, n = b)$, we can write $i = qn + r$ with either $r = 0$ or $\varphi(r) < \varphi(n)$. But $r = i - qn \in I$. Hence $\varphi(r) < \varphi(n)$ cannot be true by the definition of n. Hence $r = 0$ and so $i = qn \in (n)$. Hence $I = (n)$. □

Our next goal is to show that things factor uniquely into primes if we are in an prime integral domain.

Corollary 3.8. *F a field $\implies$ $F[x]$ is a PID.*

Proof. Obvious □

At this stage, recall that in $\mathbb{Z}$, prime $=$ irreducible, but in $\mathbb{Z}[\sqrt{-5}]$, prime $\neq$ irreducible. In an general integral domain R, prime $\implies$ irreducible.

Lemma 3.9. *In a PID, all irreducibles are prime.*

Proof. Say R is a PID and r is irreducible. Then $r \neq 0$ and r is not a unit. Say $r \mid ab, a, b \in R$ and assume $r \nmid a$. We want to show that $r \mid b$. Define $I = (r, a)$. As R is a PID, we must have that $I = (x)$ for some $x \in R$. So $r, a \in (x)$, and so $r = sx$ and $a = tx$. But r is irreducible, therefore either s or x is a unit. But s cannot be a unit. For if s is a unit, $su = 1$ for $u \in R$ and

$$r = sx \implies ur = x \implies a = tx = tur \implies r \mid a$$

contradiction. So x must be a unit. Hence $I = (x) = R \implies i \in I$, and therefore $\exists \lambda, \mu \in R$ such that $\lambda r + \mu a = 1 \implies b = \lambda rb + \mu ab$ and $r \mid \lambda rb, r \mid \mu ab$ (as $r \mid ab$). Hence $r \mid b$. $\square$

Definition 3.10. An integral domain R is a unique factorisation domain (UFD) if

UF1 (factorisation) Any non-zero $r \in R$ can be written $r = ur_1 \dots r_n$ for some $n \geq 0$ with u a unit and r_i irreducible

UF2 (uniqueness) If $r = ur_1 \dots r_n = vs_1 \dots s_m$ with $m, n \geq 0$ with and u, v units and r_i, s_i irreducibles, then $m = n$ and after reordering the s_i, if necessary, r_i and s_i are associates $\forall i$.

Remark. UF2 is necessary to deal with, e.g, $15 = 3 \times 5 = 5 \times 3 = -3 \times -5 = -1 \times 3 \times -5$ etc.

Example.

1. $\mathbb{Z}$ is a UFD.
2. $F[x]$ is a UFD.
3. Any ED is a UFD.

Remark. We have seen that in any PID, prime = irreducible. This is, more generally, true in a UFD:

For prime $\implies$ irreducible in an ID (shown before). For the converse, say r is irreducible. Then $r \neq 0$ and r is not a unit. Hence we only need to check $r \mid ab \implies r \mid a$ or $r \mid b$. So say $r \mid ab$. If $a = 0 \implies r \mid 0 \implies$ done. Say $a, b \mid 0$.

Say $rs = ab$. Factor s, a, b :

- $s = us_1 \dots s_m$
- $a = va_1 \dots a_n$
- $b = wb_1 \dots b_p$

where u, v, w are units and s_i, r_j, b_k irreducible. Now, get two factorisations of $rs = ab$:

$$rs = us_1 \dots s_m r = vwa_1 \dots a_n b_1 \dots b_p.$$

By UF2, these two factorisations are the same up to order and associates. Hence r is an associate of some a_i or some b_j. Wlog, say $a_i = ur$. Then $r \mid a_i \mid a \implies r \mid a$. Hence prime = irreducible in a UFD.

Remark. We have seen that ED $\implies$ PID and we will see that PID $\implies$ UFD. The converses, however, are both false. In fact it is a theorem that if R is a UFD, then so is $R[x]$. In particular, we see that $\mathbb{C}[x,y]$ is a UFD: $\mathbb{C}$ is a field $\therefore$ $\mathbb{C}$ is a PID (the only ideals are (0) and (1)) Hence $\mathbb{C}[x]$ is a UFD, and so $\mathbb{C}[x,y]$ is a UFD.

But the ideal (x,y) is not principal. In fact, we have that PID $\implies$ "dim ≤ 1", and $\mathbb{C}[x,y]$ has $\dim 2$.

It is much harder to find a PID that is not an ED.

Example. $\mathbb{Z}\left[\alpha = \frac{1+\sqrt{-19}}{2}\right] = \{a + b\alpha : a, b \in \mathbb{Z}\}$. Note,

$$\alpha^2 = \left(\frac{1+\sqrt{-19}}{2}\right)^2 = \frac{-18+2\sqrt{-19}}{4} = -\frac{9+\sqrt{-19}}{2} = \alpha - 5.$$

$\implies \mathbb{Z}[\alpha]$ is a ring. By M3P15, this is also a PID, and, by a messy calculation, is it not a ED.

Example. $\mathbb{Z}[i]$ is a UFD. It suffices to prove that $\mathbb{Z}[i]$ is an ED. Define $\varphi(a + ib) = a^2 + b^2$. We need to check that if $x, y \in \mathbb{Z}[i]$, then $x = qy + r$ with $\varphi(r) < \varphi(y)$ or $r = 0$.

How to find q : consider $\frac{x}{y} \in \mathbb{C}$. So $\mathbb{Z}[i]$ is an ED $\therefore$ $\mathbb{Z}[i]$ is a UFD.

Exercise. _

1. Show that $\mathbb{Z}[\sqrt{-2}]$ is a UFD.
2. Why does the above procedure fail to work for $\mathbb{Z}[\sqrt{-5}]$?

Theorem 3.11. *A PID is a UFD.*

Proof. Say R is a PID. Assume UF1 fails. Choose $r \in R$ such that $r \neq 0$ and $r \neq ur_1 \dots r_n$, r_i irreducible for $i = 1 \to n$. ||||| Clearly r is not a unit ($n = 0$) and r is irreducible ($n = 1$). Hence $r = r_1 s_1$ for some r_1, s_1, not units in R. If $r_1 = ut_1 \dots t_n$ and $s_1 = vw_1 \dots w_m$, t_i, w_j irreducible and u, v units, then $r = uvt_1 t_2 \dots w_1 \dots w_m$ is a factorsation of r. This is a contradiction to the definition of r. Hence one of r_1, s_1 does not factor into irreducibles either. Wlog, take r_1. By the same trick, $r_1 = r_2 s_2$ where s_2 is not a unit and r_2 is not the product of irreducibles. Similarly, $r_2 = r_3 s_3$, s_3 not a unit and r_3 not the product of irreducibles. By repeating this procedure, we obtain an infinite sequence

$$r = r_0 r_1 \dots$$

where $r_i = r_{i+1} s_{i+1}$, s_{i+1} not a unit. Now, $r = r_1 s_1$ $\therefore$ ideal (r_1) contains r and hence (r). Furthermore, $(r) \subset (r_1)$ (for if $(r_1) = (r)$, then

$$r_1 = rt, t \in R, \implies r = r_1 s_1 = rts_1 \implies r(1 - ts_1) = 0 \text{ and } r \neq 0 \implies s_1 \text{ is a unit}$$

contradiction). Similarly, $(r_1) \subset (r_2)$ with $(r_1) \neq (r_2)$, and so we get an increasing chain of ideals

$$(r_0) \subset (r_1) \subset \dots$$

where all containments are strict. Now, let $I = \bigcup_{n \geq 0} (r_n)$. I is an ideal, since if $i, j \in I$, then $\exists N \gg 0$ such that

$$i, j \in (r_N) \implies i \pm j \in (r_N) \subseteq I.$$

As R is a PID, I is pricipal. Hence $I = (d)$ for some $d \in R$ and $d \in I \implies d \in (r_N)$ for some $N \geq 0$. Therefore

$$(d) \subseteq (r_N) \subsetneq (r_{N+1}) \subsetneq \cdots \subseteq I = (d)$$

contradiction. Hence PID $\implies$ UF1.

For PID $\implies$ UF2, consider lemma 3.9: irreducibles are prime in a PID. So, as $r \neq 0$ and $r = ur_1 r_2 \ldots r_n = vs_1 \ldots s_m$. We will prove that $n = m$ and after re-ordering r_i and s_i are accociates by induction on n. If $n = 0$, then $r = u$ is a unit and if $m > 0$, then $s_1 \mid u \implies s_1 = 1$. But s_1 is irreducible, hence s_1 is not a unit, contradiction. Hence $m = 0$, and so the base case of induction holds. Now the inductive step: Let $n \geq 1$ and assume the statement is true for $n' < n$. Then $r = ur_1 \ldots r_n, n \geq 1$ and $r = vs_1 \ldots s_m$. So $r_1 \mid r = vs_1 s_2 \ldots s_m$ and r_1 is irreducible, hence r_1 is prime by 3.9. Therefore $r_1 \mid v$ or $r_1 \mid s_i$ for some i. As v is a unit $v \mid 1$, so $r_1 \mid v \implies r_1 \mid 1$, contradiction. Hence $r_1 \mid s_i$ for some $i, 1 \leq i \leq m$ (and in particular $m \geq 1$). After re-ordering the, wlog, s_i, $r_1 \mid s_1$. Say $s_1 = r_1 t$ for some t. s_1 is irreducible, hence either r_1 or t must be a unit. But r_1 is not a unit (see above), so t must be a unit. Hence r_1 and s_1 are associates. Now, cancel r_1 (which is fine, as R is an ID). So

$$ur_1 r_2 \ldots r_n = vs_1 s_2 \ldots s_m = vr_1 t s_2 \ldots s_m$$

$$\implies ur_2 \ldots r_n = \underbrace{vt}_{\text{unit}} s_2 \ldots s_m$$

and by our inductive hypothesis, we must have $n - 1 = m - 1 \implies n = m$ and r_i and s_i are associatives for all $i \geq 2$ after re-ordering, if necessary. $\square$

Remark. As a consequence, if $n \geq 1$ and $\exists t \in \mathbb{Z}$ such that $t^2 \equiv -1 \mod n$, then $n = a^2 + b^2, a, b \in \mathbb{Z}$.

Remark. If p is prime and $p \equiv 1 \mod 4$, then $\exists t$ such that $t^2 \equiv -1 \mod p$, for example $t = \frac{p-1}{2}$. To show this we could, alternatively, use the fact that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic $\therefore \exists$ elements of order 4 (namely t).

Note. $\mathbb{Z}[\sqrt{-3}] = \subset \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ = algebraic integers in $\mathbb{Q}(\sqrt{-3}) = a + b\left(\frac{1+\sqrt{-3}}{2}\right), a, b \in \mathbb{Z}$.

Questions:

(Q1) What are the algebraic integers in $\mathbb{Q}(\sqrt{d}), d \in \mathbb{Z}$ not being a multiple of a square number?

(A1) This question will be answered in M3P15: $\mathbb{Z}[\sqrt{d}]$ if $d \not\equiv 1 \mod 4$ or $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ if $d \not\equiv 1 \mod 4$.