Algebra II Course Notes

Isaac Holt

January 23, 2023

1 Rings and fields

1.1 Rings, subrings and fields

Definition 1.1.1. A **ring** $(R, +, \cdot)$ is a set R with two binary opertaions: addition $(+)$ and multiplication $(\cdot)$, such that $(R, +)$ is an abelian group and these conditions hold:

1. (**Identity**) for some element $1 \in R$, $\forall x \in R,\ 1 \cdot x = x \cdot 1 = x$.
2. (**Associativity**) $\forall (x, y, z) \in R^3,\ x \cdot (y \cdot z) = (x \cdot y) \cdot z$.
3. (**Distributivity**) $\forall (x, y, z) \in R^3,\ x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$.

Remark. Often we write R to mean the entire ring instead of just the set of the ring.

Definition 1.1.2. A ring R is **commutative** if $\forall x, y \in R^2,\ x \cdot y = y \cdot x$ and is **non-commutative** otherwise.

Example 1.1.3. Let V be a finite dimensional vector space over $\mathbb{C}$. The set of **linear endomorphisms** is defined as

$$\mathrm{End}(V) = \{f : V \to V : f \text{ is a linear map}\}$$

For $f \in \mathrm{End}(V)$ and $g \in \mathrm{End}(V)$, addition is defined as

$$(f + g)(v) := f(v) + g(v)$$

Multiplication is defined as function composition:

$$f \cdot g := f \circ g$$

where $(f \circ g)(v) := f(g(v))$. $\mathrm{End}(v)$ is an abelian group under addition, and it forms a ring with the addition and multiplication operations defined as above:

1. The identity element is defined as the identity map $\mathrm{id} : V \to V$, $\mathrm{id}(v) := v$.
2. Associativity: $f \circ (g \circ h)(v) = f((g \circ h)(v)) = f(g(h(v)))$ and $((f \circ g) \circ h)(v) = (f \circ g)(h(v)) = f(g(h(v))) = f \circ (g \circ h)(v)$.
3. Distributivity is similarly easy to check.

Definition 1.1.4. For $n \in \mathbb{N}$, the set of remainders modulo n is

$$\mathbb{Z}/n := \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$$

The elements of $\mathbb{Z}/n$ are called **residue classes**.

Definition 1.1.5.

- Addition in $\mathbb{Z}/n$ is defined as $\overline{a} + \overline{b} = \overline{a + b}$.
- Subtraction in $\mathbb{Z}/n$ is defined as $\overline{a} - \overline{b} = \overline{a - b}$.
- Multiplication in $\mathbb{Z}/n$ is defined as $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$.

Example 1.1.6. $\mathbb{Z}/n$ is a commutative ring.

- Commutativity: $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{ba} = \overline{b} \cdot \overline{a} \quad \forall \overline{a}, \overline{b} \in (\mathbb{Z}/n)^2$, by commutativity of $\mathbb{Z}$.
- Identity: $\overline{1} \cdot \overline{a} = \overline{1 \cdot a} = \overline{a \cdot 1} = \overline{a} \cdot \overline{1} \quad \forall \overline{a} \in \mathbb{Z}/n$ so $\overline{1}$ is the identity element.
- Associativity: $\overline{a}(\overline{a}\overline{c}) = \overline{a}(\overline{bc}) = \overline{a(bc)} = \overline{(ab)c} = (\overline{ab})\overline{c} = (\overline{a}\overline{b})\overline{c} \quad \forall \overline{a}, \overline{b}, \overline{c} \in (\mathbb{Z}/n)^3$.

Definition 1.1.7. A **subring** S of a ring R is a set $S \subset R$ that satisfies:

1. $0 \in S$ and $1 \in S$.
2. $\forall a, b \in S^2, a + b \in S$.
3. $\forall a, b \in S^2, a \cdot b \in S$,
4. $\forall a \in S, -a \in S$.

Note that the addition and multiplication operations for S are the same as those for R.

Example 1.1.8. $\mathbb{Q}$ is a subring of $\mathbb{Q}[x]$. For every $a \in \mathbb{Q}$, a is a constant polynomial in $\mathbb{Q}[x]$. $0 \in \mathbb{Q}$ and $1 \in \mathbb{Q}$. $\forall a, b \in \mathbb{Q}^2, a + b \in \mathbb{Q}$ and $-a \in \mathbb{Q}$ and $ab \in \mathbb{Q}$.

Example 1.1.9. $\mathbb{Z}[\sqrt{2}]\{a + b\sqrt{2} : a, b \in \mathbb{Z}^2\}$ is a ring. Instead of proving this using the definition of a ring, we can prove that it is a subring of $\mathbb{R}$, which requires less work.

Example 1.1.10. A subset of a ring can be a ring without being a subring. For example, $R = \{\overline{0}, \overline{2}, \overline{4}\} \subset \mathbb{Z}/6$ but R is not a subring of $\mathbb{Z}/6$ since $\overline{1} \notin R$. However, R is a ring itself, with identity $\overline{4}$.

Definition 1.1.11. A ring R is a **field** if

1. R is commutative.
2. $0 \in R$ and $1 \in R$, with $0 \neq 1$, so R has at least two elements.
3. $\forall a \in R$ with $a \neq 0$, for some $b \in R$, $ab = 1$. b is called the **inverse** of a.

Remark. For a field F, if $a, b \in F^2$ satisfy $ab = 0$, then if $b \neq 0$, $a = abb^{-1} = 0b^{-1} = 0$. Similarly, if $a \neq 0$, then $b = 0$. So $ab = 0 \iff a = 0$ or $b = 0$.

This is not true in all rings, and if a ring doesn't satisfy this property, then it can't be a field.

Definition 1.1.12. Let R be a ring and let $a \in R$ such that for some $b \neq 0$, $ab = 0$. Then a is called a **zero divisor**.

1.2 Integral domains

Definition 1.2.1. A ring R is called an **integral domain** if it is commutative, has at least two elements ($0 \neq 1$), and has no zero divisors except for 0 ($\forall a, b \in R^2, ab = 0 \implies a = 0$ or $b = 0$).

Remark. Every ring that is a subring of a field is an integral domain.

Example 1.2.2. $\mathbb{Z}/3$ is an integral domain, because $\forall a, b \in (\mathbb{Z}/3)^2, a \neq 0$ and $b \neq 0 \implies ab \neq 0$. $\mathbb{Z}/4$ is not an integral domain, because $\overline{2} \cdot \overline{2} = \overline{0}$ in $\mathbb{Z}/4$.

Proposition 1.2.3. If a ring R is an integral domain, then the ring of polynomials $R[x] := \{a_0 + a_1 x + \cdots + a_n x^n : \underline{a} \in R^n\}$ is an integral domain as well.

Proof. $R[x]$ is obviously commutative, and $0 \in R[x], 1 \in R[x], 0 \neq 1$, as this is true for R. To show that the only zero divisor is 0, assume the opposite, so for some $f(x), g(x) \in (R[x])^2, f(x)g(x) = 0$. Let

$$f(x) = a_0 + \cdots + a_m x^m, a_m \neq 0$$
$$g(x) = b_0 + \cdots + b_n x_n, b_n \neq 0$$

Then

$$f(x)g(x) = a_m b_n x^{m+n} + \cdots + a_0 b_0 = 0$$

so $a_m b_n = 0$. But $a_m \in R$ and $b_n \in R$ and R is an integral domain, so $a_m = 0$ or $b_n = 0$, so we have a contradiction. □

Definition 1.2.4. For a ring R, $a \in R$ is called a **unit** if for some $b \in R$, $ab = ba = 1$, so $b = a^{-1}$ is the inverse of a.

Proposition 1.2.5. The inverse of $a \in R$ is unique.

Proof. Assume that for some $b_1, b_2 \in R^2$, with $b_1 \neq b_2$, $ab_1 = b_1 a = 1$ and $ab_2 = b_2 a = 1$. But then

$$b_1(ab_1) = (b_1 a)b_1 = b_1 = b_1 ab_2 = b_2$$

so we have a contradiction. □

Definition 1.2.6. The **set of all units** of a ring R is written as $R^\times$.

Definition 1.2.7. For a ring R, $R^\times$ is a group under multiplication from R.

Proof.

1. Closure: if $a, b \in (R^\times)^2$, for some $c, d \in R^2$, $ac = 1$ and $bd = 1$ so $(ab)(dc) = a(bd)c = ac = 1$ so $ab \in R^\times$.
2. Identity: $1 \cdot 1 = 1$ so $1 \in R^\times$ is the identity.
3. Associativity: this is automatically satisfied by associativity in R.
4. Inverse element: every $a \in R^\times$ has an inverse by definition.

□

Example 1.2.8. For a field F, $F^\times = F - \{0\}$ since every $a \neq 0 \in F$ is a unit.

Example 1.2.9. $\mathbb{Z}^\times = \{1, -1\}$.

Example 1.2.10. For a field F, $F[x]^\times = F^\times = F - \{0\}$, since if $f(x), g(x) \in (F[x])^2$ and $f(x)g(x) = 1$, then $\deg(f) = \deg(g) = 0$, otherwise $\deg(fg) \geq 1$. Therefore if f is a unit, it is a constant non-zero polynomial, so $f \in F$.

Example 1.2.11. $M_n(\mathbb{Q})^\times = \{A \in M_n(\mathbb{Q}) : \det(A) \neq 0\}$.

Proposition 1.2.12. Let $\overline{a} \in \mathbb{Z}/n$. $\overline{a}$ is a unit iff $\gcd(a, n) = 1$.

Proof. Let $d = \gcd(a, n)$, so $d \mid a$ and $d \mid n$. Assume $\overline{a}$ is a unit, so let $\overline{b} = \overline{a}^{-1}$, so $\overline{a}\overline{b} = \overline{1} \Rightarrow ab \equiv 1 \pmod{n} \Rightarrow \exists x \in \mathbb{Z}, ab = xn + 1$. Now $d \mid (ab)$ and $d \mid xn$ so $d \mid (ab + xn)$, hence $d \mid 1 \Rightarrow d = 1$.

Now assume that $d = 1$, then by the Euclidean algorithm, $\exists x, y \in \mathbb{Z}^2, xa + ny = d = 1$. So $xa \equiv 1 \pmod{n} \Rightarrow \overline{ax} = \overline{1}$, so $\overline{a}$ is a unit, with $\overline{a}^{-1} = \overline{x}$. □

Corollary 1.2.13. $(\mathbb{Z}/n)^\times = \{\overline{a} \in \mathbb{Z}/n : \gcd(a, n) = 1\}$.

Proof. It's pretty much already there. □

Corollary 1.2.14. $\mathbb{Z}/p$ is a field iff p is prime.

Proof. If p is prime, then $\overline{1}, \overline{2}, \dots, \overline{p-1}$ are all units by Proposition 1.2.12, so $\mathbb{Z}/p$ is a field.

If $\mathbb{Z}/p$ is a field, then every $\overline{0} \neq \overline{a} \in \mathbb{Z}/p$ is a unit, hence $\gcd(a, p) = 1\ \forall 1 \leq a \leq p - 1$ by Proposition 1.2.12. This means p must be prime. □

Proposition 1.2.15. $\mathbb{Z}/p$ is an integral domain iff p is prime (iff $\mathbb{Z}/p$ is a field).

Proposition 1.2.16. If p is prime, $\mathbb{Z}/p$ is a field by Corollary 1.2.14, and every field is an integral domain.

If p is not prime, $\exists a, b \in \mathbb{Z}^2, p = ab$, with $2 \leq a, b \leq n - 1$. But then $\overline{a}\overline{b} = \overline{p} = \overline{0}$, meaning that $\overline{a}$ and $\overline{b}$ are zero divisors in $\mathbb{Z}/p$, so $\mathbb{Z}/p$ is not an integral domain. The contrapositive of this statement completes the proof.

1.3 Polynomials over a field

Definition 1.3.1. For a field F and $f(x) = a_0 + \cdots + a_n x_n \in F[x]$, the **degree** of f is defined as

$$\deg(f) = \begin{cases} \max\{i : a_i \neq 0\} & \text{if } f(x) \neq 0 \\ -\infty & \text{if } f(x) = 0 \end{cases}$$

It satisfies the following properties for every $f(x), g(x) \in (F[x])^2$:

- $\deg(fg) = \deg(f) + \deg(g)$
- $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$ with equality if $\deg(f) \neq \deg(g)$.

The degree of the zero polynomial is $-\infty$ for the following reason:

- Let f be the zero polynomial and let $g, h \in (F[x])^2$, with $\deg(g) \neq \deg(h)$. So $f = fg = fh$.
- By the first property, $\deg(g) + \deg(f) = \deg(gf) = \deg(f) = \deg(hf) = \deg(h) + \deg(f)$, but $\deg(g) \neq \deg(h)$. So for this equality to be true, $\deg(f) = \pm\infty$. But by the second property, $\deg(f + g) = \max\{\deg(f), \deg(g)\}$ when $\deg(g) \neq 0$, which would not hold if $\deg(f) = \infty$. So $\deg(f) = -\infty$.

Proposition 1.3.2. Let $f(x), g(x) \in (F[x])^2$ and $g(x) \neq 0$. Then there are unique polynomials $q(x), r(x) \in (F[x])^2$, where $\deg(r) < \deg(g)$, such that

$$f(x) = q(x)g(x) + r(x)$$

Proof. First we show the existence of $q(x)$ and $r(x)$. If $\deg(g) > \deg(f)$, $q(x) = 0$ and $r(x) = f(x)$. If $\deg(g) \leq \deg(f)$, let

$$f(x) = a_0 + \cdots + a_m x^m, \quad a_m \neq 0$$
$$g(x) = b_0 + \cdots + b_n x^n, \quad b_n \neq 0$$

Use induction on $d = m - n \geq 0$.

- When $d = 0$, $m = n$, then let $q(x) = a_m/b_n$ and let

  $$r(x) = f(x) - q(x)g(x)$$

  which satisifes $\deg(r) < m = \deg(g) \leq \deg(f)$.

- Assume $q(x)$ and $r(x)$ exist for every $0 \leq d < k$ for some $k \geq 1$.

- When $d = k$, $m = n + k$ and let

  $$f_1(x) = f(x) - \frac{a_m}{b_n} x^{m-n} g(x)$$

  so $\deg(f_1) < \deg(f)$. By the inductive assumption, for some $q_1(x)$ and $r(x)$,

  $$f_1(x) = q_1(x)g(x) + r(x)$$

  which gives

  $$\begin{aligned} f(x) &= f_1(x) + \frac{a_m}{b_n} x^{m-n} g(x) \\ &= \left(q_1(x) + \frac{a_m}{b_n} x^{m-n} \right) g(x) + r(x) \quad = q(x)g(x) + r(x) \end{aligned}$$

  where we let $q(x) = q_1(x) + \frac{a_m}{b_n} x^{m-n}$. So the result holds for $d = k$, and this completes the induction.

Now we show the uniqueness of $q(x)$ and $r(x)$. Let $f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$, where $\deg(r_1) < \deg(g)$ and $\deg(r_2) < \deg(g)$, so $\deg(R - r) < \deg(g)$. Then

$$r_2(x) - r_1(x) = (q_1(x) - q_2(x))g(x)$$

so by the properties of deg,

$$\deg(q_1 - q_2) + \deg(g) = \deg(r_2 - r_1) < \deg(g)$$

Hence $\deg(q_1 - q_2) < 0$ so $q_1(x) = q_2(x)$, and since $r_2(x) - r_1(x) = (q_1(x) - q_2(x))g(x)$, $r_1(x) = r_2(x)$. ☐

1.4 Divisibility and greatest common divisor in a ring

Definition 1.4.1. Let R be a commutative ring and $a, b \in R^2$. a **divides** b if for some $r \in R$, $b = ra$ and we write $a \mid b$.

Definition 1.4.2. Let R be a commutative ring and $a, b \in R^2$. $d \in R$ is a **greatest common divisor**, written $d = \gcd(a, b)$, if

- $d \mid a$ and $d \mid b$.

- For every $e \in R$, if $e \mid a$ and $e \mid b$, $e \mid d$.

Remark. This definition does not require that $\gcd(a, b)$ be unique. For example, by this definition 1 and -1 are greatest common divisors of 4 and 5 in $\mathbb{Z}$. $\mathbb{Z}$ has a total ordering so in this case we can define the **greatest** common divisor to be the larger of the two. But in some rings, a total ordering does not exist, so multiple gcd's exist. Some rings exist where a gcd of two elements does not exist at all.

Lemma 1.4.3. For every ring R, $\gcd(0, 0) = 0$.

Proof. $\forall x \in R, 0 = 0 \cdot x$ so every element divides 0, so the first property is satisfied. By the second property, every element that divides 0 must also divide $\gcd(0, 0)$. But every $x \in R$ divides 0, so in particular $0 \in R$ divides 0, so 0 must divide $\gcd(0, 0)$ hence

$$\exists m \in R,\ \gcd(0, 0) = 0 \cdot m = 0$$

so $\gcd(0, 0) = 0$, which is unique. □

Lemma 1.4.4. Let R be an integral domain. Let $a, b \in R^2$ and assume $d = \gcd(a, b)$ exists. Then for every unit $u \in R^\times$, ud is also a gcd of a and b. Also, for any two gcd's d_1 and d_2 of a and b, for some unit $u \in R^\times$, $d_1 = d_2 u$. So the gcd is unique up to units.

Proof. We first prove that ud is a gcd of a and b. $d \mid a$ so for some $m \in R$, $dm = a$, hence

$$du(u^{-1}m) = a \Longrightarrow du \mid a$$

Similarly, $du \mid b$.

For every $e \in R$ such that $e \mid a$ and $e \mid b$, $e \mid d \Longrightarrow \exists k \in R, ek = d$. Then $eku = du \Rightarrow e \mid du$. So by Definition 1.4.2, du is a gcd.

Now we prove that the gcd is unique up to units. Let d_1 and d_2 be gcd's. Then by Definition 1.4.2, d_1 and d_2 divide a and b and both divide each other. Hence

$$\exists u, v \in R^2, \quad d_1 = d_2 u, \quad d_2 = d_1 v$$

So $d_1 = d_1 uv$. If $d_1 = 0$ then $d_2 = 0$ so let $u = 1$. If $d_1 \neq 0$, since R is an integral domain, $uv = 1$, hence u and v are units. □

Definition 1.4.5. Let F be a field. A polynomial

$$p(x) = a_0 + \cdots + a_n x^n \in F[x]$$

is called **monic** if its leading coefficient $a_n = 1$.

Corollary 1.4.6. Let F be a field. Then for every $p_1(x), p_2(x) \in (F[x])^2$, there is a unique monic gcd.

Proof. Let $g(x) = a_0 + \cdots + a_n x^n$ be a gcd of p_1 and p_2. a_n is a unit in $F[x]$ by Example 1.2.10, so $\frac{1}{a_n} g(x)$ is a gcd and is monic. Now assume

$$h(x) = b_0 + \cdots x^m$$

is another monic gcd. Then by Lemma 1.4.4, for some unit $u \in F[x]^\times = F^\times$,

$$uh(x) = u(b_0 + \cdots + x_m) = \frac{1}{a_n} g(x)$$

Then $ux^m = x^n$ so $u = 1$ and $m = n$. Hence $h(x) = \frac{1}{a_n} g(x)$. □

Theorem 1.4.7. Let R be either $\mathbb{Z}$ or $F[x]$, and $a, b \in R^2$. Then

1. A gcd of a and b exists.
2. If $a \neq 0$ and $b \neq 0$, a gcd can be computed by the **Euclidean algorithm** (the algorithm is shown in the proof).
3. If d is a gcd(a, b), then for some $x, y \in R^2$, $ax + by = d$.

Proof. The proof is shown for $R = F[x]$. For $R = \mathbb{Z}$, the proof is the same, but $\deg(r_i(x)) < \deg(r_{i-1}(x))$ is replaced with just $r_i < r_{i-1}$ and so on.

Let $r_{-1}(x) = a$ and $r_0(x) = b$. We have

$$\begin{aligned}
\exists q_1(x), r_1(x) \in (F[x])^2, r_{-1}(x) &= q_1(x)r_0(x) + r_1(x), \quad \deg(r_1(x)) < \deg(r_0(x)) \\
&\vdots \\
\exists q_i(x), r_i(x) \in (F[x])^2, r_{i-2}(x) &= q_i(x)r_{i-1}(x) + r_i(x), \quad \deg(r_i(x)) < \deg(r_{i-1}(x)) \\
&\vdots \\
\exists q_n(x), r_n(x) \in (F[x])^2, r_{n-2}(x) &= q_n(x)r_{n-1}(x) + r_n(x), \quad \deg(r_n(x)) < \deg(r_{n-1}(x)) \\
\exists q_{n+1} \in F[x], r_{n-1}(x) &= q_{n+1}r_n(x) + 0
\end{aligned}$$

This process must terminate after a finite number of iterations, since the degree of $r_i(x)$ is a non-negative integer and it decreases by at least 1 each time.

The last non-zero remainder, $r_n(x)$ divides $rn - 1(x)$, hence divides $r_{n-2}(x)$, and so on, so divides $r_{-1}(x)$ and $r_0(x)$. Now for every divisor $d(x)$ of $r_{-1}(x)$ and $r_0(x)$, $d(x)$ must divide $r_1(x)$, so also divides $r_2(x)$, and so on, so divides $r_n(x)$. Therefore $r_n(x)$ satisfies the properties of a gcd, so is a gcd of a and b.

To prove part 3 of the theorem, start from $r_n(x) = r_{n-2}(x) - q_n(x)r_{n-1}(x)$ and replace $r_{n-1}(x)$ with $r_{n-3}(x) - q_{n-1}(x)r_{n-2}(x)$ from the equation above. So we have

$$r_n(x) = h(x)r_{n-2}(x) + g(x)r_{n-3}(x)$$

for some $h(x), g(x)$. Continuing this process from bottom to top, we get

$$r_n(x) = a(x)r_{-1}(x) + b(x)r_0(x)$$

for some $a(x), b(x) \in (F[x])^2$. $\square$

2 Homomorphisms between Rings

Let R and S be two rings. A map $f : R \to S$ is called a (ring)-homomorphism if:

1. $f(1) = 1$
2. $f(a + b) = f(a) + f(b)$
3. $f(ab) = f(a)f(b)$

Lemma 2.0.1. $f(0) = 0$ and $f(-a) = -f(a)$

Proof. $f(0) = f(0 + 0) = f(0) + f(0)$
$0 = f(0) = f(a + (-a)) = f(a) + f(-a)$
Hence $-f(a) = f(-a)$ □

Definition 2.0.2. Two rings R and S are **isomorphic** if there exists a bijective homomorphism between R and S. The map between them is an **isomorphism**. We write $R \cong S$.

Lemma 2.0.3. A homomorphism $f : R \to S$ is injective iff $\ker f = 0$.

Proof. If f is injective, $f(x) = f(y) \Rightarrow x = y$. Assume f is injective. $\ker f = a \in \mathbb{R} : f(a) = 0$ so $f(a) = 0 \Rightarrow f(a) = f(0) \Rightarrow a = 0$.

For the other direction: assume $\ker f = 0$. $f(x) = f(y) \Rightarrow f(x) - f(y) = 0 \Rightarrow f(x) + f(-y) = 0 \Rightarrow f(x - y) = 0 \Rightarrow x - y \in \ker f$. Since $\ker f = 0$, $x - y = 0$ and so $x = y$. □

Definition 2.0.4. Let R and S be two rings.

- The **product** of R and S is defined as $R \times S := \{(r, s) : r \in R, s \in S\}$ which is itself a ring.
- **Addition** is defined as $(r_1, s_1) + (r_2, s_2) := (r_1 + r_2, s_1 + s_2)$.
- **Multiplication** is defined as $(r_1, s_1) \cdot (r_2, s_2) := (r_1 r_2, s_1 s_2)$
- The multiplicative identity is $(1, 1)$.

Definition 2.0.5. We have two ring homomorphisms:

1. $p_1 : R \times S \to R = (r, s) \to r$
2. $p_2 : R \times S \to S = (r, s) \to s$

$\ker p_1 = \{(r, s) \in R \times S : p_1((r, s)) = 0\} = \{(r, s) \in R \times S : r = 0\} = \{(0, s) : s \in S\}$

Remark. Note $\ker p_1$ is not a subring of $R \times S$ since $(1, 1) \notin \ker p_1$.
But we can consider $\ker p_1$ as a ring by taking $(0, 1)$ as the multiplicative identity.
Then $\ker p_1 \cong S$ as we map $(0, s) \to s$.
Similarly, $\ker p_2 \cong R$ and so $\ker p_1 \times \ker p_2 \cong S \times R \cong R \times S$.

Lemma 2.0.6. Let $f : R \to S$ be a ring homomorphism. Then $\ker f$ has the following two properties:

1. $\ker f$ is closed under addition.

2. For every $r \in R$ and $x \ker f$ we have $r \cdot x \in \ker f$ and $x \cdot r \in \ker f$.

Proof.

1. If $x, y \in \ker f$ then $f(x+y) = f(x) + f(y) = 0 + 0 = 0$. That is $x + y \in \ker f$.

2. For every $r \in R$ and $x \ker f$, $f(r \cdot x) = f(r) \cdot f(x) = f(r) \cdot 0 = 0$. Thus $r \cdot x \in \ker f$. Similarly for $x \cdot r$.

□

Definition 2.0.7. Let I be an ideal in a ring R. Then for an element $x \in R$, the **coset** of I generated by x to be the set $\bar{x} := x + I := \{x + r : r \in I\} \subset R$.

x is said to be a representative of this coset.

Lemma 2.0.8. Let $x \in R$ and $y \in R$. Then the following statements are equivalent

1. $x + I = y + I$

2. $x + I \cap y + I \neq \emptyset$

3. $x - y \in I$

Proof. $((1) \Rightarrow (2))$ is obvious

$((2) \Rightarrow (3))$: if $x + I \cap y + I \neq \emptyset$, for some $r_1 \in I, r_2 \in I$, $x + r_1 = y + r_2$ and so $x - y = r_2 - r_1 \in I$.

$((3) \Rightarrow (1))$: since $x - y \in I$, for some $r' \in I$, $x = y + r'$. Then $x + I = \{x + r : r \in I\} = \{y + r' + r : r \in I\} \subseteq y + I$ as ideals are closed under addition, and $r' + r \in I$. $y + I = \{y + r : r \in I\} = x - r' + r : r \in I \subseteq x + I$ and so $x + I = y + I$. □

Notation: $\bar{x} = \bar{y} \Leftrightarrow x + I = y + I \Leftrightarrow x \equiv y \pmod{I} \Leftrightarrow x - y \in I$

Definition 2.0.9. $R/I := \{\bar{x} : x \in R\} = \{x + I : x \in R\}$ is the set of all distinct cosets of $R \pmod{I}$

Remark. If $R = \mathbb{Z}$ and $I = (n)$, $n \in \mathbb{N}$, $R/I = \mathbb{Z}/n = \{\bar{0}, \ldots, n \bar{-} 1\}$.

Definition 2.0.10.

- Addition: $(x + I) + (y + I) = x + y + I$

- Multiplication: $(x + I) \cdot (y + I) = xy + I$

A coset $x + I$ has many representatives, for example $x + r$ with $r \in I$ gives the same coset, since $x + r - x = r \in I$.

Assume $x, x' \in R$ such that $x + I = x' + I$ and $y, y' \in R$ such that $y + I = y' + I$.

Proof.

- Addition: $x + I = x' + I \Leftrightarrow x - x' \in I$ and similarly $y - y' \in I$. I is closed under addition so $(x - x') + (y - y') \in I \Leftrightarrow (x + y) - (x' + y') \in I \Leftrightarrow x + y + I = x' + y' + I$.

- $x - x' \in I$ and $y - y' \in I$, so $(x - x')y \in I$ and $x(y - y') \in I$. $(x - x')y + x(y - y') = xy - x'y' \in I \Leftrightarrow xy + I = x'y' + I$.

□

R/I with the two binary operations of addition and multiplication is a ring:

- The zero element is $0 + I$ as $(x + I) + (0 + I) = x + I$.
- The multiplicative identity is $1 + I$.
- All properties follow from the corresponding properties of R:
- e.g. distributivity: $\bar{x} = x + I$, $\bar{y} = y + I$, $\bar{z} = z + I$. $\bar{x}(\bar{y} + \bar{z}) = \bar{x}(\overline{y + z}) = \overline{x(y + z)} = \overline{xy + xz} = \overline{xy} + \overline{xz} = \overline{xy} + \overline{xz}$.

Definition 2.0.11. Let R be a ring, and $I \subseteq R$ be an ideal of R. Then the ring R/I is called the **quotient** of R by I (R mod I). Its elements, $x + I$, $x \in R$ are called cosets (or residue classes or equivalence classes) and we denote them $\bar{x}$.

R/I may be commutative or non-commutative, but if R is commutative, so is R/I.

If $I = R$, then R/R consists of a single element, since for every $x \in R$, $y \in R$, we have $x - y \in R$ and hence $x + R = y + R$.

If $I = 0 = 0$ is the zero ideal, if $x \in R$, $x + I = x + 0 = x$. Hence $R/I = R$.

Definition 2.0.12. Given R, $I \subsetneq R$ an ideal, the **quotient map** (or **canonical homomorphism**) is defined as $\Pi : R \to R/I = x \to \overline{x} = x + I$ and is a ring hoomomorphism.

$\ker \Pi = \{r \in R : \overline{r} = \overline{0}\} = \{r \in R : r - 0 = r \in I\} = I$.

Hence, given a ring R and an ideal $I \subseteq R$, there exists a ring homomorphism (Π) such that $\ker \Pi = I$.

Theorem 2.0.13. (First Isomorphism Theorem or FIT) Let $\phi : R \to S$ be a ring homomorphism. The map $\bar{\phi} : R/\ker\phi \to \text{Im } \phi = \bar{x} \to \phi(x)$ is well-defined and it is a ring isomorphism: $R/\ker\phi \cong \text{Im } \phi$.

Proof. Let $x, x' \in R$ such that $\overline{x} = \overline{x'}$, i.e. $x + \ker\phi = x' + \ker\phi$. So $x - x' \in \ker\phi$, hence $\phi(x - x') = 0 \Leftrightarrow \phi(x) - \phi(x') = 0 \Leftrightarrow \phi(x) = \phi(x')$. Hence $\overline{\phi}$ is well-defined.

1. $\overline{\phi}(\bar{1}) = \phi(1) = 1$
2. $\overline{\phi}(\bar{x} + \bar{y}) = \overline{\phi}(\overline{x + y}) = \phi(x + y) = \phi(x) + \phi(y) = \bar{\phi}(\bar{x}) + \bar{\phi}(\bar{y})$.
3. Similarly, $\bar{\phi}(\bar{x} \cdot \bar{y}) = \bar{\phi}(\bar{x}) \cdot \bar{\phi}(\bar{y})$.

Hence $\bar{\phi}$ is a ring homomorphism.

$\bar{\phi}(\bar{x}) = 0 \Leftrightarrow \phi(x) = 0 \Leftrightarrow x \in \ker\phi \Leftrightarrow \bar{x} = 0$, hence $\ker\bar{\phi} = \{\bar{0}\}$. Let $y \in \text{Im } \phi \Leftrightarrow$ for some $x \in R$, $\phi(x) = y$. Hence $\bar{\phi}(\bar{x}) = \phi(x) = y$, hence $\bar{\phi}$ is also surjective, hence it is bijective. □

Definition 2.0.14. Let R be a commutative ring. An ideal $I \subseteq R$ is a **prime ideal** if $I \neq R$ (I is proper) and for every $a, b \in R$ such that $a \cdot b \in I$ then $a \in I$ or $b \in I$.

The ideal $I \neq R$ is **maximal** if the only ideals that contain I is I itself and R. i.e. there is no ideal J such that $I \subsetneq J \subsetneq R$.

Theorem 2.0.15. Recall $x \in R$ is prime if $0 \neq x \notin R^\times$ and $x|ab \Rightarrow x|a$ or $x|b$.

If x is a prime element then (x) is a prime ideal.

Proof. $ab \in (x) \Rightarrow$ for some $r \in R$, $ab = rx \Rightarrow x|ab$ so because x is prime, $x|a$ or $x|b$ so $a \in (x)$ or $b \in (x)$. □

Lemma 2.0.16. Let (x) be a non-zero prime ideal. The x is a prime element.

Proof. If $x|ab$, $ab \in (x)$, so because (x) is a prime ideal, $a \in (x)$ or $b \in (x)$, so $x|a$ or $x|b$. $\square$

Remark. $x|a \Leftrightarrow a \in (x) \Leftrightarrow (a) \subseteq (x)$.
This can be described as "to divide is to contain".

Corollary 2.0.17. The zero ideal $(0) = 0$ is a prime ideal iff R is an integral domain, since an integral means $ab = 0 \Rightarrow a = 0$ or $b = 0$.

Theorem 2.0.18. Let R be a commutative ring and $I \subseteq R$ an ideal.

1. I is prime iff R/I is an integral domain.
2. I is maximal iff R/I is a field.

Proof.

1. Assume I is prime. Assume $\bar{a}\bar{b} = \bar{0}$ with $a, b \in R$, $\bar{a}, \bar{b} \in R/I$. $\bar{a}\bar{b} = \bar{0} \Rightarrow \overline{ab} = \bar{0} \Rightarrow ab \in I \Rightarrow a \in I$ or $b \in I \Rightarrow \bar{a} = \bar{0}$ or $\bar{b} = 0$, hence R/I is an integral domain.

   Now assume R/I is an integral domain. $ab \in I \Rightarrow \overline{ab} = \bar{0}$. Since R/I is an integral domain, $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0} \Rightarrow a \in I$ or $b \in I$.

2. ($\Rightarrow$): Assume that I is maximal. Let $\bar{x} \neq \bar{0}$, $\bar{x} \in R/I$, then $x \in R$ with $x \notin I$. Consider $(I, x) := \{r + r'x : r \in I, r' \in R\}$. This is an ideal, as $r_1 + r_1'x + r_2 + r_2'x = (r_1 + r_2) + (r_1' + r_2')x \in R$, and $r''(r + r'x) = r''r + r''r'x \in R$.

   $I \subsetneq (I, x) \subseteq R$. I is maximal so $(I, x) = R \Rightarrow 1 \in (I, x)$. Hence for some $y \in R$, $yx + m = 1$ for some $m \in I$.

   Hence $yx - 1 \in I \Rightarrow \overline{yx} = \bar{y}\bar{x} = \bar{1}$ hence $\bar{x}$ is invertible, so R/I is a field.

   ($\Leftarrow$): Assume R/I is a field. If $\bar{0} \neq \bar{x} \in R/I$, then for some $y \in R/I$, $\bar{x}\bar{y} = 1 \Rightarrow xy - 1 \in I \Rightarrow xy = 1 + m$ for some $m \in I$. That is, $1 = xy - m$ hence $1 \in (I, x) \Rightarrow (I, x) = R$.

   Now let J be an ideal such that $I \subsetneq J \subseteq R$. Since $I \subsetneq J$, for some $x \in J$, $x \notin I$. Then $I \subsetneq (I, x) \subseteq J \subseteq R$. But $(I, x) = R$, hence $J = R$. Hence there is no ideal J such that $I \subsetneq J \subsetneq R$, hence I is maximal.

$\square$

Corollary 2.0.19. If I is maximal then I is prime.

Proof. I is maximal $\Rightarrow R/I$ is a field $\Rightarrow R/I$ is an integral domain $\Rightarrow I$ is a prime ideal. $\square$

2.1 Principal Ideal Domains (PIDs)

Example 2.1.1. Let $a, b \in \mathbb{Z}$. Then let $d = (a, b) = \gcd(a, b)$. $(a, b) \subseteq (d)$ since $d|a$ and $d|b \Leftrightarrow a = dr_1$ and $b = dr_2$, $r_1, r_2 \in \mathbb{Z} \Rightarrow a \in (d)$ and $b \in (d)$.
Moreover, for some $r_1, r_2 \in \mathbb{Z}$, $d = r_1 + r_2 b \Rightarrow d \in (a, b) \Rightarrow (d) \subseteq (a, b)$.
The same argument holds for $F[x]$ with F a field.
i.e. $(f(x), g(x)) = (\gcd(f(x), g(x)))$.

Definition 2.1.2. An integral domain in which **all** ideals are principle is called a **principle ideal domain (PID)**.

Theorem 2.1.3. Let R be a either $\mathbb{Z}$ or $F[x]$ with F a field. Then R is a PID.

Proof. Define the following "degree" function $d : R\backslash\{0\} \to \mathbb{N}$ by

$$d(a) := \begin{cases} |a| & \text{if } a \in \mathbb{Z} \\ \deg(a) & \text{if } a \in F[x] \end{cases}$$

By division, for every $a, m \in R\backslash\{0\}$, we can find unique $q, R \in R$ such that $a = qm + r$ with $r = 0$ of $d(r) < d(m)$.

Let $I \subseteq R$ be an ideal. If $I = 0 = \{0\}$ we are done. So now let $I \neq 0$. Let $0 \neq m \in I$ such that $d(m)$ is minimal among elements of I. We claim that $I = (m)$.

Let $a \in I$. $a \in (m) \Leftrightarrow m|a$. Dividing a by m, we get $a = qm + r$, with $r = 0$ or $d(r) < d(m)$. But since $r = a - qm \in I$, $d(r) < d(m)$ would contradict the minimality of $d(m)$. Hence $r = 0$, so $m|a \Leftrightarrow a \in (m)$. $(m) \subseteq I$ so $a \in I \Leftrightarrow a \in (m)$. □

Theorem 2.1.4. (Stated without proof) Any PID is a UFD.

Remark. There are integral domains which are not PIDs, e.g. $\mathbb{Z}[\sqrt{-5}]$ which is not a UFD and hence not a PID.

Proposition 2.1.5. Let R be a PID and $a, b \in R$. Then $\gcd(a, b)$ exists and $(a, b) = (\gcd(a, b))$.

Proof. Since R is a PID, for some $d \in R$, $(a, b) = (d)$. We claim that $d = \gcd(a, b)$.

$(a, b) = (d) \Rightarrow a \in (d)$ and $b \in (d) \Rightarrow d|a$ and $d|b$. Suppose $e \in R$ such that $e|a \Rightarrow a \in (e)$ and $e|b \Rightarrow b \in (e)$. $(d) = (a, b) \subseteq (e) \Rightarrow e|d$. Therefore $d = \gcd(a, b)$. □

Theorem 2.1.6. (Stated without proof): $\mathbb{Z}[i], \mathbb{Z}[\pm\sqrt{2}]$ are PID's.

Lemma 2.1.7. Let R be a PID and let $a \in R$ be irreducible. Then the principle ideal genereated by a is a maximal ideal.

Proof. Suppose $(a) \subseteq I$, with I an ideal. We must show $I = (a)$ or $I = R$. Since R is a PID, for some $t \in R$, $I = (t)$. So $(a) \subseteq (t)$ so for some $m \in R$, $a = tm$. But a is irreducible, so either t is a unit or m is a unit.

If $t \in R^\times$ then $I = (t) = R$. If $m \in R^\times$ then $(a) = (t) = I$ (last question of assignment 3). □

2.2 Fields on quotients

Theorem 2.2.1. Let F be a field and $f(x) \in F[x]$, with $f(x)$ irreducible. Then $F[x]/(f(x))$ is a field and a vector space over F with basis

$$B := \{\bar{1}, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{n-1}\}$$

where $n = \deg f$.

That is, every element of $F[x]/(f(x))$ can be uniquely written as

$$\overline{a_0 1 + a_1 x + \cdots + a_{n-1} x^{n-1}}$$

Proof. Since $f(x)$ is irreducible, $F[x]/(f(x))$ is a field. $F[x]/(f(x))$ is a vector space over F and an abelian group with respect to addition and scalar multiplication with elements of F: if $\overline{g(x)} \in F[x]/(f(x))$ and $\alpha \in F$ then $\alpha\overline{g(x)} = \overline{\alpha g(x)} \in F[x]/(f(x))$.

We must prove B spans $F[x]/(f(x))$. For every $\overline{g(x)} \in F[x]/(f(x))$, $g(x) = q(x)f(x) + r(x)$ with $\deg(r) < \deg(f) = n \Rightarrow g(x) - r(x) = q(x)f(x) \in (f(x)) \Rightarrow \overline{g(x)} = \overline{r(x)}$, $\deg(r) < n$. Hence $\overline{g(x)} = \overline{r(x)} = a_0 + a_1\bar{x} + \cdots + a_{n-1}\bar{x}^{n-1}$ with $a_i \in F$. Hence B spans $F[x]/(f(x))$.

We must show B is linearly independent over F, i.e. show if $\sum_{i=0}^{n-1} a_i\bar{x}^i = \bar{0}$ then $\forall i, a_i = 0$.

$\sum_{i=0}^{n-1} a_i\bar{x}^i = \bar{0} \Leftrightarrow \sum_{i=0}^{n-1} a_i x^i \in (f(x)) \Rightarrow f(x) | \sum_{i=0}^{n-1} a_i x^i$. But $\deg(f) = n$ and $\deg(\sum_{i=0}^{n-1} a_i x^i) < n$ so $\sum_{i=0}^{n-1} a_i x^i$ is the zero polynomial so $\forall i, a_i = 0$. Therefore B is linearly independent.

So B is a basis. $\square$

3 Finite fields

Theorem 3.0.1. For every prime p and $n \in \mathbb{N}$, for some irreducible polynomial $f(x) \in (\mathbb{Z}/p)[x]$, $\deg(f) = n$. Thus $(\mathbb{Z}/p)[x]/(f(x))$ is a field with p^n elements (since there are p choices for each a_i in $a_0 + a_1\bar{x} + \cdots + a_{n-1}\bar{x}^{n-1}$).

Any two such fields are isomorphic and we denote the unique, up to isomorphism, field with p^n elements with $\mathbb{F}_{p^n}$.

Proof. Not examinable. □

Remark. If $n = 1$ then $\mathbb{F}_p \cong \mathbb{Z}/p$ with p prime. However if $n > 1$ then $\mathbb{F}_{p^n} \ncong \mathbb{Z}/p^n$ since $\mathbb{Z}/p^n$ is not a field.

Example 3.0.2. Find an irreducible polynomial f in $(\mathbb{Z}/3)[x]$ of degree 3.

$f(x) = x^3 + x^2 + x + \bar{2}$. This has no roots in $\mathbb{Z}/3$ so $f(x)$ is irreducible since $\deg(f) = 3$. Then $\mathbb{F}_{27} = \mathbb{F}_{3^3} \cong (\mathbb{Z}/3)[x]/(f(x))$. All elements can be written as $a_0 + a_1\bar{x} + a_2\bar{x}^2$, $a_i \in \mathbb{Z}/3$.

$\overline{f(x)} = \bar{0} = \overline{x^3 + x^2 + x + \bar{2}} \Rightarrow \bar{x}^3 = -\bar{x}^2 - \bar{x} - \bar{2}$.

3.1 The Chinese Remainder Theorem (CRT)

Definition 3.1.1. Let $a, b \in R$. a and b are **coprime** if $\nexists r$ irreducible in R such that $r|a$ and $r|b$.

Lemma 3.1.2. Let R be a PID and $a, b \in R$ be coprime. Then $(a, b) = R$ and hence $\exists x, y \in R$ such that $xa + yb = 1$.

Proof. Since R is a PID, $(a, b) = (r)$ for some $r \in R$. So $a, b \in (r) \Rightarrow r|a$ and $r|b$. So $a = rn$ and $b = rm$ for some $n, m \in R$. r must be a unit in R since otherwise, $r = p_1 \cdots p_k$ for some p_i irreducible, but then $a = p_1 \cdots p_k n$, $b = p_k \cdot p_k m$, which would contradict a and b being coprime.

So $r \in R^\times \Rightarrow (r) = R \Rightarrow (a, b) = R$. □

Corollary 3.1.3. For $a, b \in R$ coprime, any $\gcd(a, b) \in R^\times$.

Proof. In a PID, $(a, b) = (\gcd(a, b))$. By the lemma above, if a and b are coprime, $(a, b) = R \Rightarrow (\gcd(a, b)) = R = (1) \Rightarrow \gcd(a, b) \in R^\times$. □

Theorem 3.1.4. (CRT for PID's) Let R be a PID and let $a_1, \ldots, a_k \in R$ be pairwise coprime elements. Then the map from $R/(a_1, \ldots, a_k) \to R/(a_1) \times \cdots \times R/(a_k)$ given by $r + (a_1, \ldots, a_k) \to (r + (a_1), \ldots, r + (a_k))$ is a ring isomorphism.

Proof. Let $\psi : R \to R/(a_1) \times \cdots \times R/(a_k)$, $\psi(r) = (r + (a_1), \ldots, r + (a_k))$. Clearly, ψ is a ring homomorphism.

For every $i = 1, 2, \ldots, k$, the elements a_i and $a_1 \ldots a_{i-1}a_{i+1} \ldots a_k$ are coprime. (If not, there exists an irreducible p such that $p|a_i$ and $p|a_1 \ldots a_{i-1}a_{i+1} \ldots a_k$. But then $p$irreducible $\Leftrightarrow p$ prime hence $p|a_j$ for some $j \neq i$, but this contradicts that a_i and a_j are coprime).

By the above lemma, for some $x_i, y_i \in R$, $x_i a_i + y_i(a_1 \ldots a_{i-1}a_{i+1} \ldots a_k) = 1$. Set $e_i := 1 - a_i x_i$ for each $i = 1, \ldots, k$. Then $e_i = 1 + (a_i)$ and $e_i = 0 + (a_j)$ for $j \neq i$, since $e_i = 1 - a_i x_i = y_i(a_1 \ldots a_{i-1}a_{i+1} \ldots a_k)$.

Let $(r_1 + (a_1), \ldots, r_k + (a_k))$ be any element in $R/(a_1) \times \cdots \times R/(a_k)$. We claim that

$$\psi\left(\sum_{i=1}^{k} r_i e_i\right) = (r_1 + (a_1), \ldots, r_k + (a_k))$$

$$\psi\left(\sum_{i=1}^{k} r_i e_i\right) = \sum_{i=1}^{k} \psi(r_i e_i) = \sum_{i=1}^{k} \psi(r_i)\psi(e_i)$$

$$\psi(e_1) = (0 + (a_1), \ldots, 1 + (a_i), 0 + (a_{i+1}), \ldots, 0 + (a_k))$$

since $e_i = 1 + (a_i)$ and $e_i = 0 + (a_j)$ for $j \neq i$ and

$$\psi(r_i) = (r_i + (a_1), \ldots r_i + (a_k))$$

so

$$\psi(e_i)\psi(r_i) = TODOfinishandcheckthisproof$$

Thus ψ is surjective. $\ker\psi = \{r \in R : r \in (a_i), i = 1, \ldots, k\} = \{r \in R : a_i | r, i = 1, \ldots, k\} = \{r \in R : a_1 \ldots a_k | r\}$ since a_i and a_j are coprime. $\ker\psi = (a_1 a_2 \ldots a_k)$. Then by the FIT, $R/\ker\psi \cong R/(a_1) \times \cdots \times R/(a_k)$. $\square$

4 Group Theory

Definition 4.0.1. A **group** is a pair $(G, \circ)$ where G is a set and $\circ$ is a map

$$\circ : G \times G \to G, \quad \circ(g, h) = g \circ h$$

Satisfying these properties:

1. **Closure**: $g, h \in G \Rightarrow g \circ h \in G$.
2. **Associativity**: $x, y, z \in G \Rightarrow (x \circ y) \circ z = x \circ (y \circ z)$.
3. **Identity element**: $\exists e \in G,\ \forall g \in G,\ e \circ g = g \circ e = g$.
4. **Existence of inverse**: $\forall g \in G,\ \exists h \in G,\ g \circ h = h \circ g = e$. h is called the **inverse** of g and is written as g^{-1}.

Definition 4.0.2. A group $(G, \circ)$ is an **Abelian group** if $\forall g, h \in G,\ g \circ h = h \circ g$. Otherwise, it is called **non-Abelian**.

Remark. Often, G is written to refer to a group, not just the set of a group.

Lemma 4.0.3. Let $(R, +, \cdot)$ be a ring. Then $(G, \circ) = (R, +)$ is a group.

Proof. Properties 1 and 2 of a group are automatically satisfied. The identity element is $0 \in R$. The inverse element for any element will be the same inverse element in the ring. □

Lemma 4.0.4. Let $(F, +, \cdot)$ be a field. Then $(G, \circ) = (R, \cdot)$ is a group.

Proof. Again, group properties 1 and 2 are automatic. The identity element is $1 \in F$. The inverse element for any element will be the same inverse element in the field. □

Example 4.0.5. (**Symmetries of a square**): The following are all symmetries of a square:

- Rotation by $\frac{\pi}{2}$.
- Reflection about the y-axis, x-axis, $y = x$ axis, $y = -x$ axis.
- Any of the above symmetries can be combined to form a new symmetry.

Define the group $G(, \circ)$ where G is the symmetries of the square and $\circ$ is composition of the symmetries. The identity e is the map which does nothing to the square. The inverse of a rotation is rotation in the opposite direction, and the inverse of a reflection is the same reflection.

Definition 4.0.6. The group in the above example is the **dihedral group**.

Definition 4.0.7. The **general linear group** is defined as the set $GL_2(\mathbb{R}) := \{A \in M_2(\mathbb{R}) : \det A \neq 0\}$ together with $\circ$ being matrix multiplication.

Lemma 4.0.8. The general linear group is a group.

Proof.

1. $\det(AB) = \det A \det B \neq 0$ so $A, B \in GL_2(\mathbb{R}) \Rightarrow AB \in GL_2(\mathbb{R})$.
2. Matrix multiplication is associative.
3. The identity is I_2.
4. The inverse of $A \in GL_2(\mathbb{R})$ is A^{-1}, which exists since $\det A \neq 0$.

□

Remark. $GL_2(\mathbb{R})$ is non-abelian.

4.1 Subgroups

Definition 4.1.1. A subset $H \subseteq G$ is a **subgroup** of $(G, \circ)$ if $(H, \circ)$ is also a group. We write $H \leq G$.

Remark. $H = G$ is a subgroup of a group G.

Definition 4.1.2. Every group $(G, \circ)$ has a **trivial subgroup**, $H = \{e\}$, where $e \in G$ is the identity element.

Definition 4.1.3. A subgroup H of G is **proper** if $H \neq \{e\}$ and $H \neq G$. We write $H < G$.

Proposition 4.1.4. (**Subgroup criteria**) Let $(G, \circ)$ be a group. Then $H \subseteq G$ is a subgroup iff all these conditions hold:

1. $H \neq \emptyset$
2. $h_1, h_2 \in H \Rightarrow h_1 \circ h_2 \in H$.
3. $h \in H \Rightarrow h^{-1} \in H$.

Proof. We only need to show that H contains an identity: $h \in H \Rightarrow h^{-1} \in H \Rightarrow e = h \circ h^{-1} \in H$. □

Example 4.1.5. If $(S, +, \cdot)$ is a subring, then $(S, +)$ is a subgroup.

Proposition 4.1.6. Let $I \subseteq R$ be a non-empty ideal of a ring $(R, +, \cdot)$. Then $(I, +)$ is a subgroup of $(R, +)$.

Proof. Criteria 1 and 2 are satisfied by definition. Now we must show that $x \in I \Rightarrow -x \in I$: if $x \in I$, then $(-1_R)x = -x \in I$ where $-1_R + 1_R = 0_R$. □

Definition 4.1.7. The **special linear group** is defined as $SL_2(\mathbb{R}) = \{A \in M_2(\mathbb{R}) : \det A = 1\}$, which satisfies $(SL_2(\mathbb{R}), \cdot) \leq (Gl_2(\mathbb{R}), \cdot)$.

Example 4.1.8. Let $q \in \mathbb{N}$, then $q\mathbb{Z} = \{mq : m \in \mathbb{Z}\}$ is an ideal in $\mathbb{Z}$. For example, the even numbers, $2\mathbb{Z}$, is a subgroup.

However, the odd numbers are not subgroup, as they do not contain 0, nor is $\bar{a} = \{a + mq : m \in \mathbb{Z}\}$ for $1 \leq a \leq q - 1$.

4.2 Cosets

Definition 4.2.1. Let $(G, \circ)$ be a group and $H \leq G$. A **left coset** of H is a set of the form

$$g \circ H := \{g \circ h : h \in H\} \quad \text{for } g \in G$$

A **right coset** of H is a set of the form

$$H \circ g := \{h \circ g : h \in H\} \quad \text{for } g \in G$$

Remark. $x \in g \circ H \iff g^{-1} \circ x \in H$.

Remark. If G is Abelian, then $g \circ H = H \circ g$, but this isn't true in general for non-Abelian groups.

Proposition 4.2.2. Let $(G, \circ)$ be a group and $H \leq G$. Then:

1. For every $g \in G$, $g \circ H$ and H are in bijection. (So $|H| < \infty \Rightarrow |g \circ H| = |H|$).
2. If $g \in G$, then $g \in H \iff g \circ H = H$.
3. If $g_1, g_2 \in G$, then either $g_1 \circ H = g_2 \circ H$ or $(g_1 \circ H) \cap (g_2 \circ H) = \emptyset$.

Proof.

1. Let $g \in G$. Define $\phi_g : H \to g \circ H$ as

$$\phi_g(h) := g \circ h$$

   $\forall x \in g \circ H, \exists h_x \in H, x = g \circ h_x = \phi_g(h_x)$ so ϕ_g is surjective. Let $h_1, h_2 \in H$ such that $\phi_g(h_1) = \phi_g(h_2) \Leftrightarrow g \circ h_1 = g \circ h_2 \Rightarrow h_1 = e \circ h_1 = (g^{-1} \circ g) \circ h_1 = g^{-1} \circ (g \circ h_1)$. Similarly, $h_2 = e \circ h_2 = (g^{-1} \circ g) \circ h_2 = g^{-1} \circ (g \circ h_2)$. Hence $h_1 = h_2$, so ϕ_g is injective, and so also bijective.

2. ($\Rightarrow$) Let $g \in H$. If $h \in H$, then $g \circ h \in H \implies g \circ H \subseteq H$. To show that $H \subseteq g \circ H$, we will show that if $h \in H$, then $\exists h' \in H, h = g \circ h' \in g \circ H \iff h' = g^{-1} \circ h \in H \iff h = g \circ (g^{-1} \circ h) \in g \circ H \iff H \subseteq g \in H$. ($\Leftarrow$) If $g \circ H = H$, $g = g \circ e \in g \circ H$ since $e \in H$, hence $g \in H$.

3. Let $(g_1, g_2) \in G^2$ and assume that $g_1 \circ H \neq g_2 \circ H$, and that $(g_1 \circ H) \cap (g_2 \circ H) \neq \emptyset$. Let $x \in (g_1 \circ H) \cap (g_2 \circ H)$, then $\exists (h_1, h_2) \in H^2$, $x = g_1 \circ h_1 = g_2 \circ h_2 \iff g_2^{-1} \circ g_1 = h_2 \circ h_1^{-1} \in H$. By part 2, $(g_2^{-1} \circ g_1) \circ H = H \implies g_1 \circ H = g_2 \circ H$, but this is a contradiction, which completes the proof.

□

Theorem 4.2.3. (Lagrange) If G is a **finite** group and $H \leq G$, then $|H|$ divides $|G|$. So if $|H| \nmid |G|$ then $H \not\leq G$.

Proof. Let $G_0 = G$ and let $G_1 = G_0 \backslash H$. If $|G_1| = 0$, we are done, otherwise for some $g_1 \in G$, $H \cap g_1 \circ H = \emptyset$. Then set $G_2 = G_1 \backslash G_1 \backslash (g_1 \circ H)$. If $|G_2| = 0$, we are done, otherwise for some $g_2 \in G$, $(H \cup (g_1 \circ H)) \cap (g_2 \circ H) = \emptyset$, and set $G_3 = G_2 \backslash (g_2 \circ H)$.

This process must terminate since $|g_i \circ H| = |H| \geq 1$ elements are removed each time. At the end of this process, for some $S \subseteq G$,

$$G = \bigcup_{g \in S} (g \circ H)$$

and for $g, g' \in S$, $g \circ H \cap g' \circ H = \emptyset$. So

$$|G| = \left| \bigcup_{g \in S} (g \circ H) \right| = \sum_{g \in S} |g \circ H|$$

Since $|g \circ H| = |H| \forall g \in S$, $|G| = |S||H| \implies |H| \mid |G|$. □

4.3 Normal subgroups

Definition 4.3.1. A subgroup $H \leq G$ is **normal** if $\forall g \in G, \ g \circ H = H \circ g$. Equivalently, H is normal if either:

1. $\forall g \in G, \ g \circ H \circ g^{-1} \subseteq H$.

2. $\forall g \in G, h \in H,\ g \circ h \circ g^{-1} \in H$.

We write $H \lhd G$.

Remark. This means that $\forall h \in H,\ \exists h' \in H, g \circ h = h' \circ g$, but $h \neq h'$ in general.

Example 4.3.2. If G is **abelian**, then every subgroup $H \leq G$ is normal, since if $g \in G, h \in H$, then $g \circ h \circ g^{-1} = g \circ (g^{-1} \circ h) = h \in H$.

Definition 4.3.3. For a group G and $g \in G$, g^k for $k \in \mathbb{Z}$ is defined as

$$g^k = \begin{cases} g \circ g \circ \cdots \circ g \quad (k \text{ times}) & \text{if } k \geq 1 \\ g^{-1} \circ g^{-1} \circ \cdots \circ g^{-1} \quad (-k \text{ times}) & \text{if } k < 0 \\ e & \text{if } k = 0 \end{cases}$$

Definition 4.3.4. For a group G and $g \in G$, the **group generated by** g, H, is defined as

$$H := \langle g \rangle = \left\{ g^k : k \in \mathbb{Z} \right\}$$

Proposition 4.3.5. H is a Abelian group.

Proof.

1. $g^{n+m} = g^n \circ g^m = g^m \circ g^n$.

2. $g^{-n} = (g^n)^{-1}$.

□

Definition 4.3.6. Let $S \subsetneq G$ be finite, so $S = \{g_1, \ldots, g_k\}$. The **subgroup of** G **generated by** S is defined as

$$H := \langle S \rangle = \{ g_1^{a_1} \circ \cdots \circ g_k^{a_k} \circ g_1^{b_1} \circ \cdots \circ g_k^{b_k} : a_i, b_j \in \mathbb{Z}^2 \}$$

H is the set of finite products of g_i and g_j^{-1}, for $1 \leq i, j \leq k$.

Example 4.3.7. Let $q \in \mathbb{N}$ be odd, so $\bar{2} \in \mathbb{Z}/q$. Then $\langle \bar{2} \rangle = \mathbb{Z}/q$, since every $\bar{a} \in \mathbb{Z}/q$ is of the form $\bar{2} \cdot x, x \in \mathbb{Z}$.

Example 4.3.8. Let $q = p^2$ for p prime. Then $\langle \bar{p} \rangle = \{\bar{p}, \overline{2p}, \ldots, \overline{p(p-1)}, \bar{0}\}$.

Example 4.3.9. Let $(G, \circ) = (\mathbb{R}^\times, \cdot)$ and $S = \{\sqrt{2}, \pi\}$. Then $\langle S \rangle = \{\sqrt{2}^a \cdot \pi^b : a, b \in \mathbb{Z}^2\}$. Since $(\mathbb{R}^\times, \cdot)$ is Abelian.

Definition 4.3.10. Let G be a group, and let $g \in G$. The **order** of g in G, written as $\mathrm{ord}_G(g)$ or $\mathrm{ord}(g)$ is the smallest $d \in \mathbb{N}$ such that $g^d = e$.

If d does not exist, $\mathrm{ord}_G(g) = \infty$. If $\mathrm{ord}_G(g) < \infty$, g has **finite order**, otherwise, g has **infinite order**.

Example 4.3.11. For $(G, \circ) = (\mathbb{Z}, +)$, every $x \in \mathbb{Z} - \{0\}$ has infinite order, because $x + \cdots + x = dx = 0$, and since $\mathbb{Z}$ is an integral domain, $d = 0$, but $d \in \mathbb{N}$.

Example 4.3.12. In D_4, the symmetries of a square,

- The rotation by $\frac{\pi}{2}$, r, has $\mathrm{ord}(r) = 4$.
- Reflection, s, has $\mathrm{ord}(s) = 2$.

4.4 Cyclic groups

Definition 4.4.1. A group G is **cyclic** if $\exists g \in G, G = \langle g \rangle$.

Theorem 4.4.2. Let a group G be finite and let $|G| = p$ for p prime. Then G is cyclic.

Proof. Since $|G| = p > 1$, $\exists g \in G, g \neq e$. Let $H = \langle g \rangle$, so $H \leq G$. By Lagrange's theorem, $|H| \mid |G|$. Since $|G|$ is prime, $|H| = 1$ or $|H| = p$. Since $\{e, g\} \subset H$, $|H| \geq 2$, so $|H| = p$. $H \subseteq G$, so $G = H = \langle g \rangle$. $\square$

Remark. For every $g \neq e$ in G of prime order, $G = \langle g \rangle$, and $\mathrm{ord}_G(g) = p$.