Algebra II Course Notes

Isaac Holt

March 10, 2023

Contents

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: $\overline{a}(\overline{ac}) = \overline{a}(\overline{bc}) = \overline{a(bc)} = \overline{(ab)c} = (\overline{ab})\overline{c} = (\overline{a}\overline{b})\overline{c} \quad \forall \overline{a}, \overline{b}, \overline{c} \in (\mathbb{Z}/n)^3$.

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. $\square$

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

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

so we have a contradiction. $\square$

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.

$\square$

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 $\overline{a}^{-1} = \overline{x}$. $\square$

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. $\square$

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

Proof. If p is prime, then $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ 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. $\square$

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

$$\begin{aligned} f(x) &= a_0 + \cdots + a_m x^m, \quad a_m \neq 0 \\ g(x) &= b_0 + \cdots + b_n x^n, \quad b_n \neq 0 \end{aligned}$$

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 $r_2(x) - r_1(x) = (q_1(x) - q_2(x))g(x)$, $r_1(x) = r_2(x)$. $\square$

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 $a(x), b(x) \in (F[x])^2$. □

Example 1.4.8. Find a gcd of $f(x) = x^2 + 1$ and $g(x) = x^2 + 3x + 1$ in $\mathbb{Q}[x]$. Using the Euclidean algorithm, we obtain

$$\begin{aligned}
f(x) &= g(x) - 3x \\
g(x) &= (-\frac{1}{3}x - 1)(-3x) + 1 \\
-3x &= 1(-3x) + 0
\end{aligned}$$

The algorithm terminates as the remainder is now 0. A gcd is the last non-zero remainder, in this case 1. Now we write 1 as a linear combination of $f(x)$ and $g(x)$:

$$\begin{aligned}
1 &= g(x) - \left(-\frac{1}{3}x - 1\right)(-3x) \\
&= g(x) + \left(\frac{1}{3}x + 1\right)(f(x) - g(x)) \\
&= \left(\frac{1}{3}x + 1\right) f(x) - \frac{1}{3}xg(x)
\end{aligned}$$

2 Factorisations in rings

2.1 Irreducible polynomials over a field

Definition 2.1.1. Let R be a commutative ring. $0 \neq r \in R$ is called **irreducible** if:

1. r is not a unit and
2. if for some $a, b \in R^2, r = ab$, then a is a unit or b is a unit.

Example 2.1.2. For a field F, a non-zero polynomial in $F[x]$ is irreducible if it is not constant and cannot be written as the product of two non-constant polynomials in $F[x]$.

Example 2.1.3. $x^2 + 1 \in \mathbb{R}$ is irreducible in $\mathbb{R}[x]$, but is not irreducible in $\mathbb{C}$, since $x^2 + 1 = (x - i)(x + i)$.

Example 2.1.4. The irreducible elements in $\mathbb{Z}$ are the prime numbers.

Definition 2.1.5. For a field F, let $f(x) \in F[x]$. $a \in F$ is called a **root** (or a **zero**) of f in F if $f(a) = 0$.

Proposition 2.1.6.

- If $\deg(f) = 1$, then f is irreducible in $F[x]$.
- If $\deg(f) = 2$ or 3, then f is irreducible in $F[x]$ iff f has no roots in F.
- If $\deg(f) = 4$, then f is irreducible iff f has no roots in F and f is not the product of two quadratic polynomials.

Proof.

- If $\deg(f) = 1$, then $f(x) = ax + b$ for some $a, b \in F^2$, $a \neq 0$. By Example 1.2.10, f is not a unit. Now let $f(x) = g(x)h(x)$ for some $g(x), h(x) \in (F[x])^2$. But $1 = \deg(f) = \deg(g) + \deg(h)$ so either $\deg(g) = 1$ and $\deg(h) = 0$ or $\deg(g) = 0$ and $\deg(h) = 1$. Therefore one of g and h has degree 0 so is a constant polynomial, therefore is a unit.
- If $\deg(f) = 2$ or 3, let $\alpha \in F$ be a root of f, so $f(x) = q(x)(x - \alpha) + r(x)$ for some $q(x), r(x)$ where $\deg(r) \leq 0$, by Proposition 1.3.2. Hence $r(x)$ is constant.

  Now, $0 = f(\alpha) = r(\alpha)$ but since $r(x)$ is constant, $r(x) = 0$ so $f(x) = q(x)(x - \alpha)$. Therefore f is not irreducible as $\deg(q) \geq 1$.

  Conversely, if f is not irreducible, $f(x) = g(x)h(x)$ for some $g(x), h(x)$ where $\deg(g) \geq 1$ and $\deg(h) \geq 1$. $\deg(f) = \deg(g) + \deg(h)$ so either $\deg(g) = 1$ or $\deg(h) = 1$. WLOG, assume $\deg(g) = 1$, then $g(x) = ax + b$ for some $a, b \in F^2$, $a \neq 0$.

  Then $g(-b/a) = 0 = f(-b/a)$ so f has a root.
- The proof when $\deg(f) = 4$ is similar to the proof for $\deg(f) = 2$ or 3.

$\square$

Proposition 2.1.7. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$, where $\deg(f) \geq 1$. For every $p, q \in \mathbb{Z}^2$, if $f(p/q) = 0$ and $\gcd(p, q) = 1$, then

$$p \mid a_0 \quad \text{and} \quad q \mid a_n$$

Proof.

$$\begin{aligned} 0 &= f(p/q) \\ &= a_0 + a_1(p/q) + \cdots + a_n(p/q)^n \\ &= a_0q^n + p\left(a_1q^{n-1} + a_2pq^{n-2} + \cdots + a_np^{n-1}\right) = 0 \\ &= q(a_0q^{n-1} + a_1pq^{n-2} + \cdots + a_{n-1}p^{n-1}) + a_np^n = 0 \end{aligned}$$

So $p \mid a_0q^n$ and $q \mid a_np^n$ and since $\gcd(p,q) = 1$, $p \mid a_0$ and $q \mid a_n$. □

Example 2.1.8. $f(x) = x^3 - 3x + 2$ is irreducible in $\mathbb{Q}[x]$.

By Proposition 2.1.6, it is sufficient to show that f has no roots in $\mathbb{Q}$. Let $p/q \in \mathbb{Q}$, and assume $\gcd(p,q) = 1$ (if $\gcd(p,q) \neq 1$, then the fraction can be cancelled by $\gcd(p,q)$ to leave the same value). If p/q was a root of f, then $q \mid 1$ and $p \mid 2$. So the only possible values of p and q are $\{\pm 1, \pm 2\}$ but none of these values is a root, so f is irreducible in $\mathbb{Q}[x]$.

Lemma 2.1.9. (**Gauss's lemma**) Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ be a non-constant polynomial. Then $f(x)$ is irreducible in $\mathbb{Z}[x]$ iff $f(x)$ is irreducible in $\mathbb{Q}[x]$ and $\gcd(a_0, \ldots, a_n) = 1$.

Proof. ($\Longleftarrow$): Let $f(x)$ be irreducible in $\mathbb{Q}[x]$ and $\gcd(a_0, \ldots, a_n) = 1$. Let $f(x) = g(x)h(x)$ for some $g(x), h(x) \in (\mathbb{Z})^2$. If $\deg(g) \geq 1$ and $\deg(h) \geq 1$ then f would have a proper factorisation in $\mathbb{Q}[x]$, contradicting the fact that it is irreducible in $\mathbb{Q}[x]$. So $\deg(g) = 0$ or $\deg(h) = 0$. WLOG, assume that $\deg(g) = 0$, hence $g(x) \in \mathbb{Z}$. If $g(x) \neq \pm 1$, for some prime number $p \in \mathbb{Z}$, $p \mid g(x) \Longrightarrow p \mid f(x)$, but $\gcd(a_0, \ldots, a_n) = 1$. Hence $g(x) = \pm 1$ which is a unit, so $f(x)$ is irreducible in $\mathbb{Z}[x]$.

($\Longrightarrow$): Omitted. □

Corollary 2.1.10. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ and $\gcd(a_0, \ldots, a_n) = 1$. Then $f(x)$ is irreducible in $\mathbb{Z}[x]$ iff $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Lemma 2.1.11. Let $f(x) = a_0 + a_1 + \cdots + a_nx^n \in \mathbb{Z}[x]$, $a_n = 1$, be a monic polynomial. If $f(x)$ factors in $\mathbb{Q}[x]$, then $f(x)$ factors into integer monic polynomials.

Proof. Clearly $\gcd(a_0, \ldots, a_n) = 1$, so by Corollary 2.1.10, if f factors in $\mathbb{Q}[x]$, f factors in $\mathbb{Z}[x]$. Hence

$$f(x) = g(x)h(x) = (b_0 + \cdots + b_mx^m)(c_0 + \cdots + c_mx^m)$$

where $m + l = n$ and $\forall i,\ b_i, c_i \in \mathbb{Z}^2$. Equating the coefficients of x^n on both sides gives $b_mc_l = 1$ so $b_m = c_l = 1$, or $b_m = c_l = -1$. So either g and h are monic or $-g$ and $-h$ are monic, and $f(x) = (-g(x))(-h(x))$. □

Lemma 2.1.12. Let R be a commutative ring, let $x \in R$ be irreducible and let $u \in R^\times$. Then ux is irreducible.

Proof. $x \neq 0$ so $ux \neq 0$. If ux is a unit, then for some $b \in R$, $b(ux) = 1 = (bu)x \Longrightarrow x \in R^\times$, which is a contradiction, hence x is not a unit.

Let $ux = ab$ for some $a, b \in R^2$, then we must show that a or b is a unit. $x = abu^{-1} = a(bu^{-1})$ and as x is irreducible, $a \in R^\times$ or $bu^{-1} \in R^\times$. And $bu^{-1} \in R^\times \Rightarrow b \in \mathbb{R}^\times$, as units form a group under multiplication, hence either a or b is a unit. □

Proposition 2.1.13. (**Eisenstein's criterion**) Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ and let p be a prime with $p \mid a_0, \ldots, p \mid a_{n-1}$, $p \nmid a_n$ and $p^2 \nmid a_0$. Then f is irreducible in $\mathbb{Q}[x]$.

Proof. Let $d = \gcd(a_0, \dots, a_n)$, $b_i = a_i/d$ and

$$F(x) = \frac{1}{d}f(x) = b_0 + b_1x + \cdots + b_nx^n \in \mathbb{Z}[x]$$

Then $\gcd(b_0, \dots, b_n) = 1$. Note that $p \nmid a_n$ so $p \nmid d$, so $p \mid b_0, p \mid b_1, \dots, p \mid b_{n-1}, p \nmid b_n$ and $p^2 \nmid b_0$. By Lemma 2.1.12, if F is irreducible in $\mathbb{Q}[x]$, then f is also irreducible in $\mathbb{Q}[x]$.

Assume that F is not irreducible in $\mathbb{Q}[x]$. By Gauss's lemma, $F(x) = g(x)h(x)$ for some $g(x), h(x) \in (\mathbb{Z})^2$ with $\deg(g) \geq 1$ and $\deg(h) \geq 1$. Reducing this by modulo p gives

$$\bar{g}(x)\bar{h}(x) = \bar{F}(x) = \bar{b_0} + \bar{b_1}x + \cdots + \bar{b_n}x^n = \bar{b_n}x^n$$

Let

$$\bar{g}(x) = \bar{\alpha_0} + \bar{\alpha_1}x + \cdots + \bar{\alpha_m}x^m$$
$$\bar{h}(x) = \bar{\beta_0} + \bar{\beta_1}x + \cdots + \bar{\beta_k}x^k$$

$\deg(\bar{g}) = \deg(g)$ and $\deg(\bar{h}) = \deg(h)$, otherwise $p \mid b_n$. This gives

$$\overline{\alpha_0}\overline{\beta_0} + \overline{\alpha_0}\overline{\beta_1}x + \cdots + \overline{\alpha_0}\overline{\beta_k}x^k + \overline{\alpha_1}\overline{\beta_0}x + \cdots + \overline{\alpha_m}\overline{\beta_k}x^{m+k} = \overline{b_n}x^n$$

hence $\overline{\alpha_0}\overline{\beta_0} = \overline{0}$. p is prime so $\mathbb{Z}/p$ is a field, so this implies $\overline{\alpha_0} = \overline{0}$ or $\overline{\beta_0} = \overline{0}$. WLOG, let $\overline{\alpha_0} = \overline{0}$, then we have $\overline{\beta_0}\overline{\alpha_m} = \overline{0}$ and $\overline{\alpha_m} \neq \overline{0}$ so $\overline{\beta_0} = \overline{0}$.

So $p \mid \alpha_0$ and $p \mid \beta_0$, thus $p^2 \mid \alpha_0\beta_0 = b_0$ so $p^2 \mid b_0$ which is a contradiction. Hence F is irreducible, so f is also. □

2.2 Unique factorisation in $F[x]$

Lemma 2.2.1. Let F be a field. If $p(x) \in F[x]$ is irreducible and $p(x) \mid a(x)b(x)$ for some $a(x), b(x) \in (F[x])^2$, then $p(x) \mid a(x)$ or $p(x) \mid b(x)$.

Proof. If $p(x) \nmid a(x)$, then $\gcd(p(x), a(x)) = 1$ so by Theorem 1.4.7 (3.), for some $A(x), B(x) \in (F[x])^2$,

$$A(x)p(x) + B(x)a(x) = 1 \implies A(x)p(x)b(x) + B(x)a(x)b(x) = b(x)$$

But $p(x) \mid B(x)a(x)b(x)$ and $p(x) \mid A(x)p(x)b(x)$ hence $p(x) \mid b(x)$. Hence $p(x) \mid a(x)$ or $p(x) \mid b(x)$. □

Theorem 2.2.2. Let F be a field and let $f(x) \in F[x]$ with $\deg(f) \geq 1$. Then $f(x)$ can be uniquely factorised into a product of irreducible elements, up to order of the factors and multiplication by units.

Proof.

- First we prove the existence of a factorisation. Use induction on $\deg(f)$. If $\deg(f) = 1$, then f is irreducible already. Assume now that we have such a factorisation for $f'(x) \in F[x]$ with $\deg(f') < n$, for some $n \in \mathbb{N}$. Let $\deg(f) = n$. If f is irreducible we are done. If not, then $f(x) = g(x)h(x)$ for some $g(x), h(x) \in (F[x])^2$ with $1 \leq \deg(f) < n$ and $1 \leq \deg(h) < n$. By the induction hypothesis, g and h have factorisations into irreducible elements, hence f also does.

- Now we prove the uniqueness. Let

$$f(x) = p_1(x) \cdots p_m(x) = q_1(x) \cdots q_n(x)$$

where for every i, p_i and q_i are irreducible. Then $p_1(x) \mid q_1(x) \cdots q_n(x)$ so by Lemma 2.2.1, p_1 must divide one of the q_i. WLOG, assume $p_1 \mid q_1$. So $q_1(x) = u_1(x)p_1(x)$ for some $u_1(x) \in F[x]$, but p_1 and q_1 are irreducible so u_1 is a unit. Hence

$$f(x) = p_1(x) \cdots p_m(x) = u_1(x)p_1(x)q_2(x) \cdots q_n(x)$$
$$\implies p_2(x) \cdots p_m(x) = u_1(x)q_2(x) \cdots q_n(x)$$

Repeat these steps for $p_2, p_3, \ldots$ until all factors are cancelled. This gives $m = n$ and $q_i = u_i p_i$ for every i and some unit u_i. This completes the proof.

$\square$

Definition 2.2.3. Let R be a commutative ring. $x \in R$ is called **prime** if these conditions hold:

1. $x \neq 0$ and $x \notin R^\times$ and
2. $\forall a, b \in R^2,\ x \mid ab \implies a \mid a$ or $x \mid b$.

Example 2.2.4. $p \in \mathbb{Z}$ is prime iff p is irreducible.

Example 2.2.5. For a field F, $f(x) \in F[x]$ is prime iff it is irreducible.

Lemma 2.2.6. Let R be an integral domain. Let $x \in R$ be prime. Then x is irreducible.

Proof. The ring $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} : a, b \in \mathbb{Z}^2$ is a subring of $\mathbb{C}$. Define

$$N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}, quad N(a + b\sqrt{-5}) = a^b + 5b^2$$

$N(z) = z\bar{z}$ where $\bar{z}$ is the complex conjugate of z. So $N(z)N(w) = z\bar{z}w\bar{w} = zw\bar{z}\bar{w} = N(zw)$. We show that 2 is irreducible.

Assume $2 = (x + y\sqrt{-5})(z + w\sqrt{-5})$ for some $x, y, z, w \in \mathbb{Z}^4$. Then

$$N(2) = N(x + y\sqrt{-5})N(z + w\sqrt{-5})$$

So $N(x + y\sqrt{-5}) \mid 4$, so $N(x + y\sqrt{-5}) \in \{\pm 1, \pm 2, \pm 4\}$. The only possibilities from these are 1 and 4. If $x^2 + 5y^2 = 1$ then $y = 0$ and $x = \pm 1$ so $x + y\sqrt{-5}$ is a unit. If $x^2 + 5y^2 = 4$ then $y = 0$ and $x = \pm 2$ so $2 = \pm 2(z + w\sqrt{-5})$, hence $(z + w\sqrt{-5})$ is a unit. Hence 2 is irreducible.

However, 2 is not prime, since

$$2 \mid (1 - \sqrt{-5})(1 + \sqrt{-5}) = 6$$

but $2 \nmid (1 - \sqrt{-5})$ and $2 \nmid (1 + \sqrt{-5})$, since $2(x + y\sqrt{-5}) = 1 \pm \sqrt{-5}$ for some $x, y \in \mathbb{Z}^2$ then $2x = 1$, a contradiction. $\square$

Definition 2.2.7. Let R be an integral domain. R is called a **unique factorization domain** (**UFD**) if every non-zero non-unit element of R has a unique factorization into a product of irreducible elements, which is unique up to order of factors and multiplication by units.

Example 2.2.8. $\mathbb{Z}$ is a UFD.

Example 2.2.9. For a field F, $F[x]$ is a UFD by Theorem 2.2.2.

Example 2.2.10. $\mathbb{Z}[-\sqrt{5}]$ is not a UFD, as 6 has two factorisations:

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \cdot 3 = 6$$

NOTES directly from lecture notes up to here

3 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 3.0.1. $f(0) = 0$ 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 $-f(a) = f(-a)$ $\square$

Definition 3.0.2. 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 3.0.3. 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 $x = y$. $\square$

Definition 3.0.4. 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 3.0.5. 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 3.0.6. 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 3.0.7. 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 3.0.8. 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 3.0.9. $R/I := \{\bar{x} : x \in R\} = \{x + I : x \in R\}$ is the set of all distinct cosets of $R \pmod{I}$

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

Definition 3.0.10.

- 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 3.0.11. 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 3.0.12. Given R, $I \subseteq R$ 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 3.0.13. (First Isomorphism Theorem or FIT) Let $\phi : R \to S$ be a ring homomorphism. The map $\bar{\phi} : R/\ker\phi \to \mathrm{Im}(\phi) = \bar{x} \to \phi(x)$ is well-defined and it is a ring isomorphism: $R/\ker\phi \cong \mathrm{Im}(\phi)$.

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 $y \in \mathrm{Im}(\phi) \Leftrightarrow$ 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. $\square$

Definition 3.0.14. 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 3.0.15. 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 $b \in (x)$. $\square$

Lemma 3.0.16. 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 3.0.17. 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 3.0.18. 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.

□

Corollary 3.0.19. 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. □

3.1 Principal Ideal Domains (PIDs)

Example 3.1.1. 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 3.1.2. An integral domain in which **all** ideals are principle is called a **principle ideal domain (PID)**.

Theorem 3.1.3. 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 3.1.4. (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 3.1.5. 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 3.1.6. (Stated without proof): $\mathbb{Z}[i], \mathbb{Z}[\pm\sqrt{2}]$ are PID's.

Lemma 3.1.7. 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). □

3.2 Fields on quotients

Theorem 3.2.1. 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. □

4 Finite fields

Theorem 4.0.1. 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 $\mathbb{F}_{p^n} \not\cong \mathbb{Z}/p^n$ since $\mathbb{Z}/p^n$ is not a field.

Example 4.0.2. 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 $a_0 + a_1\bar{x} + a_2\bar{x}^2$, $a_i \in \mathbb{Z}/3$.

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

4.1 The Chinese Remainder Theorem (CRT)

Definition 4.1.1. Let $a, b \in R$. a and b are **coprime** if $\nexists r$ irreducible in R such that $r|a$ and $r|b$.

Lemma 4.1.2. 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 4.1.3. 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 4.1.4. (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

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

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

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

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

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

so

$$\psi(e_i)\psi(r_i) = TODO finish and check this proof$$

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

5 Group Theory

Definition 5.0.1. 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 5.0.2. 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 5.0.3. 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. $\square$

Lemma 5.0.4. 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. $\square$

Example 5.0.5. (**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 5.0.6. The group in the above example is the **dihedral group**.

Definition 5.0.7. The **general linear group** is defined as the set $\mathrm{GL}_2(\mathbb{R}) := \{A \in M_2(\mathbb{R}) : \det A \neq 0\}$ together with $\circ$ being matrix multiplication.

Lemma 5.0.8. The general linear group is a group.

Proof.

1. $\det(AB) = \det A \det B \neq 0$ so $A, B \in \mathrm{GL}_2(\mathbb{R}) \Rightarrow AB \in \mathrm{GL}_2(\mathbb{R})$.
2. Matrix multiplication is associative.
3. The identity is I_2.
4. The inverse of $A \in \mathrm{GL}_2(\mathbb{R})$ is A^{-1}, which exists since $\det A \neq 0$.

$\square$

Remark. $\mathrm{GL}_2(\mathbb{R})$ is non-abelian.

5.1 Subgroups

Definition 5.1.1. 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 5.1.2. Every group $(G, \circ)$ has a **trivial subgroup**, $H = \{e\}$, where $e \in G$ is the identity element.

Definition 5.1.3. A subgroup H of G is **proper** if $H \neq \{e\}$ and $H \neq G$. We write $H < G$.

Proposition 5.1.4. (**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 5.1.5. If $(S, +, \cdot)$ is a subring, then $(S, +)$ is a subgroup.

Proposition 5.1.6. 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 5.1.7. 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 5.1.8. 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 $1 \leq a \leq q - 1$.

5.2 Cosets

Definition 5.2.1. 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 5.2.2. 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.

$\square$

Theorem 5.2.3. (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 $|g \circ H| = |H| \forall g \in S$, $|G| = |S||H| \implies |H| \mid |G|$. $\square$

5.3 Normal subgroups

Definition 5.3.1. 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 $H \triangleleft G$.

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 5.3.2. 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 5.3.3. 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 5.3.4. 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 5.3.5. *H is a Abelian group.*

Proof.

1. $g^{n+m} = g^n \circ g^m = g^m \circ g^n$.
2. $g^{-n} = (g^n)^{-1}$.

$\square$

Definition 5.3.6. Let $S \subseteq G$ 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 5.3.7. 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 5.3.8. Let $q = p^2$ for p prime. Then $\langle \bar{p} \rangle = \{\bar{p}, \overline{2p}, \ldots, \overline{p(p-1)}, \bar{0}\}$.

Example 5.3.9. 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 5.3.10. Let G be a group, and let $g \in G$. The **order** of g in G, written as $\text{ord}_G(g)$ or $\text{ord}(g)$ is the smallest $d \in \mathbb{N}$ such that $g^d = e$.

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

Example 5.3.11. 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 5.3.12. In D_4, the symmetries of a square,

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

5.4 Cyclic groups

Definition 5.4.1. A group G is **cyclic** if $\exists g \in G, G = \langle g \rangle$.

Theorem 5.4.2. 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 $\mathrm{ord}_G(g) = p$.

5.5 Permutation groups

Definition 5.5.1. A **permutation** of a non-empty set X is a bijection from X to itself. We define S_X to be the set of all bijections from X to itself. For $n \geq 1$, we write

$$S_n = S_{\{1,\dots,n\}}$$

Lemma 5.5.2. $(S_X, \circ)$ is a group where $\circ$ is the composition of bijections.

Proof. Associativity and closure are automatic due to the associativity and closure of composition of functions. The identity element is the identity function on X. The inverse of a bijection is given by reversing it: for a permutation $\sigma(x) : X \to X$ where $\sigma(x) = y$ its inverse is given by σ^{-1} where

$$\sigma^{-1}(y) = x$$

$\square$

Lemma 5.5.3. $\forall n \geq 1, |S_n| = n!$.

Proof. There are n choices to map 1 to, then $n-1$ choices to map 2 to, etc., and 1 choice to map n to. So there are $n(n-1)\cdots 1$ choices in total. $\square$

Definition 5.5.4. $(S_n, \circ)$ is called the **symmetric group of degree** n (or **symmetric group on** n **letters**).

Definition 5.5.5. For a permutation $\phi : \{1, \dots, n\} \to \{1, \dots, n\}$, we can write ϕ as

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \phi(1) & \phi(2) & \cdots & \phi(n) \end{pmatrix}$$

Definition 5.5.6. Some permutations in S_n can be subdivided into simpler units called **cycles**. Let $n \geq 1$ and $1 \leq k \leq n$. A k**-cycle** is an element $\sigma \in S_n$ which satisfies, with $I = \{i_1, i_2, \dots, i_k\} \subseteq \{1, \dots, n\}$:

1. $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_{k-1}) = i_k$ and $\sigma(i_k) = i_1$ and
2. if $i \notin I$, $\sigma(i) = i$.

We often denote a k-cycle $\sigma \in S_n$ as

$$(i_1 \; i_2 \; \dots \; i_k)$$

or equivalently,

$$(i_2 \; i_3 \; \dots \; i_k \; i_1)$$

etc.

Definition 5.5.7. A 2-cycle is called a **transposition**.

Definition 5.5.8. Let $n \geq 1$, and $\sigma, \tau \in (S_n)^2$ be cycles. σ and τ are called **disjoint** if their associated index sets, $\{i_1, \dots, i_k\} = I$ for σ and $\{j_1, \dots, j_l\} = J$ for τ are disjoint, so

$$I \cap J = \emptyset$$

Example 5.5.9. (1 3 5) and (2 4) are disjoint, while (1 3 5) and (1 2 4) are not.

Remark. S_n is not an abelian group. For example, if $\sigma = (1\ 2)$ and $\tau = (2\ 3)$,

$$\begin{array}{ll} (\sigma \circ \tau)(1) = 2 & (\tau \circ \sigma)(1) = 3 \\ (\sigma \circ \tau)(2) = 3 & (\tau \circ \sigma)(2) = 1 \\ (\sigma \circ \tau)(3) = 1 & (\tau \circ \sigma)(3) = 2 \end{array}$$

Lemma 5.5.10. If $\sigma, \tau \in (S_n)^2$ are disjoint cycles then $\sigma \circ \tau = \tau \circ \sigma$.

Proof. Let $1 \leq k \leq n$. Let T be the set of indices changed by τ and S be the set of indices changed by σ.

- Let $k \in T$, so $k \notin S$. Then $\tau(k) \notin S$, so $(\sigma \circ \tau)(k) = \tau(k)$ and $(\tau \circ \sigma)(k) = \tau(k)$.
- Similarly, if $k \in S$, then $k \notin T$. So $(\tau \circ \sigma)(k) = \sigma(k)$ and $(\sigma \circ \tau)(k) = \sigma(k)$.
- The remaining case is that $k \notin S \cup T$. Then $\tau(k) = \sigma(k) = k$ so $(\sigma \circ \tau)(k) = \sigma(k) = k$ and $(\tau \circ \sigma)(k) = \tau(k) = k$.

□

Example 5.5.11. The permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 2 & 1 & 5 & 4 & 7 \end{pmatrix}$$

can be written as $(2\ 3) \circ (1\ 6\ 4) \circ (5) \circ (7)$.

Proposition 5.5.12. Let $n \geq 1$. Any $\sigma \in S_n$ can be written as a composition of disjoint cycles, which is unique up to rearrangement of cycles and shifts within cycles.

Proof. TODO. □

Lemma 5.5.13. Let $\sigma = (i_1\ \dots\ i_k)$ be a k-cycle in S_n, $1 \leq k \leq n$. Then σ can be written in one of the following forms:

1. $\sigma = (i_1\ \dots\ i_k) = (i_1\ i_2) \circ (i_2\ i_3) \circ \cdots \circ (i_{k-1}\ i_k)$
2. $\sigma = (i_1\ \dots\ i_k) = (i_1\ i_k) \circ (i_1\ i_{k-1}) \circ \cdots \circ (i_1\ i_2)$

Proof. TODO. □

Remark. Often, when it is clearly what n is, 1-cycles are omitted when writing cycles. For example, $(1\ 3\ 5)(2)(4)$ in S_5 can be written as $(1\ 3\ 5)$.

Example 5.5.14. Let

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{bmatrix}, \quad \tau = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{bmatrix}$$

To determine $\sigma \circ \tau$, write τ on top of σ, but rearranging the columns of σ to line up with the columns of τ:

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \\ 2 & 3 & 4 & 1 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{bmatrix}$$

so

$$\sigma \circ \tau = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{bmatrix}$$

Example 5.5.15. Let $\sigma = (1\ 2)$ and $\tau = (1\ 3)$ in S_3, then

$$\sigma \circ \tau = (1\ 2) \circ (1\ 3) = (1\ 3\ 2)$$

Example 5.5.16. $(1\ 2\ 3) = (1\ 2) \circ (2\ 3) = (1\ 3) \circ (1\ 2)$.

Definition 5.5.17. Let G be a group and $g_1, g_2 \in G^2$. g_1 and g_2 are called **conjugate** in G to each other if

$$\exists h \in G, \quad h g_1 h^{-1} = g_2$$

Lemma 5.5.18. Let $n \geq 2$ and $G = S_n$. Every conjugate of a transposition in G is also a transposition.

Proof. By Proposition 5.5.12, each permutation can be expressed as a composition of disjoint cycles, and by Lemma 5.5.13, each cycle is a product of transpositions. So we just need to show that the conjugate of a transposition $(a\ b)$ by another transposition $(c\ d)$ is also a transposition. There are three cases:

1. If $\{a, b\}$ and $\{c, d\}$ are disjoint then $(a\ b)$ and $(c\ d)$ commute, hence

   $$(c\ d)(a\ b)(c\ d)^{-1} = (a\ b)$$

   is a transposition.

2. If $\{a, b\}$ and $\{c, d\}$ have one common element, then say the common element is $b = c$ WLOG. Then

   $$(b\ d)(a\ b)(b\ d)^{-1} = (a\ d)$$

   is a transposition.

3. If $\{a, b\} = \{c, d\}$ then clearly

   $$(c\ d)(a\ b)(c\ d)^{-1} = (a\ b)$$

   is a transposition.

□

Example 5.5.19. (Problems class) Find a normal subgroup of S_3.

$|S_3| = 3! = 6$ so look for a subgroup of size 3 (this will be a normal subgroup). Let $\sigma = (1\ 2\ 3)$ and let

$$H = \langle \sigma \rangle = \{e, \sigma, \sigma \circ \sigma\}$$

H is a group of order 3 because $\sigma \circ \sigma \circ \sigma = e \neq \sigma \circ \sigma$ (for example, $(\sigma \circ \sigma)(1) = 3 \neq 1 = e(1)$). $|H| = 3$ so $H \lhd S_3$.

Example 5.5.20. (Problems class) Let G be a group and $H, K \leq G$. Prove that $H \cap K \leq G$.

Using the criteria for subgroups, we check:

1. $H \cap K \neq \emptyset$: since H and K are subgroups, they both contain e, so $e \in H \cap K$.
2. if $x, y \in (H \cap K)^2$ then $x \circ y \in H \cap K$: if $x, y \in H^2$ and $x, y \in K^2$, $x \circ y \in H$ and $x \circ y \in K$ so $x \circ y \in H \cap K$.
3. if $x \in H \cap K$, then $x^{-1} \in H \cap K$: if $x \in H$ and $x \in K$, then $x^{-1} \in H$ and $x^{-1} \in K$ so $x^{-1} \in H \cap K$.

Example 5.5.21. Let G be a group, $H \lhd G$ and $K \lhd G$. Prove that $H \cap K \lhd G$.

$H \cap K$ is normal iff for every $g \in G, x \in H \cap K$, $gxg^{-1} \in H \cap K$. Let $g \in G, x \in H \cap K$. Since $x \in H$ and $H \lhd G$, $gxg^{-1} \in H$. Similarly, $gxg^{-1} \in K$. So $gxg^{-1} \in H \cap K$.

Example 5.5.22. (Problems class) Given a group G, define

$$\mathrm{Tor}(G) := \{x \in G : \mathrm{ord}(x) < \infty\}$$

so $x \in \mathrm{Tor}(G)$ iff $\exists d \geq 1, x^d = e$. Let $x, y \in (\mathrm{Tor}(G))^2$, such that $x \circ y = y \circ x$. Prove that $x \circ y \in \mathrm{Tor}(G)$ and $\mathrm{ord}(x \circ y) \leq \mathrm{lcm}(\mathrm{ord}(x), \mathrm{ord}(y))$.

Let $k \geq 1$. We use induction to show that

$$(x \circ y)^k = x^k \circ y^k$$

For $k = 1$, this is trivial. $(x \circ y)^{k+1} = (x \circ y)^k \circ (x \circ y) = x^k \circ y^k \circ x \circ y$. By the induction step, $y^k \circ x = x \circ y^k$. So

$$x^k \circ y^k \circ x \circ y = x^k \circ x \circ y^k \circ y = x^{k+1} \circ y^{k+1}$$

Let $\mathrm{ord}(x) = a$ and $\mathrm{ord}(y) = b$, then let $d = \mathrm{lcm}(a, b)$ (d which a and b divide works). Then

$$(x \circ y)^d = x^d \circ y^d = (x^a)^b \circ (y^b)^a = e^b \circ e^a = e$$

So $\mathrm{ord}(xy) \leq \mathrm{lcm}(\mathrm{ord}(x), \mathrm{ord}(y)) < \infty$.

TODO: 3.19, 3.20, 3.21, 3.22

5.6 Even permutations and alternating groups

Definition 5.6.1. For $n \geq 2$, let A_n be the subgroup of S_n which contains the even permutations. A_n is called the **alternating group**.

Example 5.6.2. For $n = 3$, $(1\ 2\ 3) = (1\ 2) \circ (2\ 3) \in A_3$. Also, $\mathrm{sgn}(e) = 1$ so $e \in A_3$.

Lemma 5.6.3. $A_n \leq S_n$ for every $n \geq 2$.

Proof. Using the subgroup criteria,

1. $e \in A_n$ so $A_n \neq \emptyset$.

2. For every $\sigma_1, \sigma_2 \in (A_n)^2$,

$$\sigma_1 = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_{2r}$$
$$\sigma_2 = \tau_1' \circ \tau_2' \circ \cdots \circ \tau_{2s}'$$

   where $r \geq 0$, $s \geq 0$, and the τ_i and τ_i' are transpositions. So

$$\sigma_1 \circ \sigma_2 = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_{2r} \circ \tau_1' \circ \tau_2' \circ \cdots \circ \tau_{2s}'$$

   so $\sigma_1 \circ \sigma_2$ has even parity, so $\operatorname{sgn}(\sigma_1 \circ \sigma_2) = 1 \implies \sigma_1 \circ \sigma_2 \in A_n$.

3. For every $\sigma \in A_n$,

$$\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_{2r}$$

   where $r \geq 0$, so

$$\sigma^{-1} = (\tau_1 \circ \tau_2 \circ \cdots \circ \tau_{2r})^{-1} = \tau_{2r} \circ \cdots \circ \tau_1$$

   hence $\operatorname{sgn}(\sigma^{-1}) = 1$ so $\sigma^{-1} \in A_n$.

□

Example 5.6.4. $\{\sigma \in S_n : \operatorname{sgn}(\sigma) = -1\}$ is not a group since it does not contain e. But if $\tau \in S_n$ is a transposition,

$$\tau A_n = \{\tau \circ \sigma : \sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_{2r}, r \geq 0\} = \{\sigma \in S_n : \operatorname{sgn}(\sigma) = -1\}$$

So $S_n = \tau A_n \cup A_n$, and $\tau A_n \cap A_n = \emptyset$.

Proposition 5.6.5.

1. $|A_n| = |S_n|/2 = n!/2$.

2. $A_n \lhd S_n$.

3. A_n is generated by 3-cycles, for $n \geq 3$.

Proof.

1. By the above example and the properties of cosets, $|S_n| = |\tau A_n| + |A_n| = 2|A_n|$ for $t \in S_n$ a transposition.

2. If $H \leq G$ for a finite group G, then $|H| = 2|H| \implies H \lhd G$. So let $G = S_n$, $H = A_n$, then $A_n \lhd S_n$ by 1.

3. Given any τ_1, τ_2 transpositions, $\tau_1 \circ \tau_2$ is either 0, 1 or 2 3-cycles composed together. There are three cases:

   (a) $\tau_1 = \tau_2 = (i\ j)$, then $\tau_1 \circ \tau_2 = e$.

   (b) $\tau_1 = (i\ j)$, $\tau_2 = (i\ k)$, where $j \neq k$, then $\tau_1 \circ \tau_2 = (j\ i\ k)$.

   (c) $\tau_1 = (i\ j)$, $\tau_2 = (k\ l)$, where $\{i, j\{\cap\{k, l\} = \emptyset$. Then

$$\tau_1 \circ \tau_2 = (i\ j) \circ ((i\ k) \circ (k\ i)) \circ (k\ l) = ((i\ j) \circ (i\ k)) \circ ((k\ i) \circ (k\ l))$$

   and from case 2, this gives 2 3-cycles.

   Since every $\sigma \in A_n$ can be written as

$$\sigma = \alpha_1 \circ \cdots \circ \alpha_k$$

   where the α_i are pairs of transpositions, σ can be written as a composition of 3-cycles.

□

5.7 Dihedral groups

TODO: 3.25, 3.26, 3.27, 3.28, 3.29

Definition 5.7.1. The **dihedral group** of order $2n$, D_n, is the group generated by rotations r by $2\pi/n$ anticlockwise and reflections s about a fixed axis, where $r^n = e$, $s^2 = e$, $srs = r^{-1}$.

Proposition 5.7.2. Every $x \in D_n$ can be uniquely written as

$$r^a s^b, \quad 0 \leq a \leq n-1, 0 \leq b \leq 1$$

In particular, $|D_n| = 2n$.

Proof. If $x \in D_n$, then

$$x = r^{a_1} s^{b_1} r^{a_2} s^{b_2} \cdots r^{a_k} b^{b_k}$$

where $a_i \geq 0, b_j \geq 0$ and $\forall i \in \{1, \ldots, k-1\}, b_i \geq 1$ and $\forall i \in \{2, \ldots, k\}, a_i \geq 1$. Suppose k is minimal (so this is the shortest representation). We claim that $k = 1$.

If $k \neq 1$, we can shorten a representation with $k \geq 2$ factors as

$$y = r^{a_1} s^{b_1} r^{a_2} s^{b_2} \cdots r^{a_{k-2}} b^{b_{k-2}} \implies x = y r^{a_{k-1}} s^{b_{k-1}} r^{a_k} s^{b_k}$$

Note that we can assume that $0 \leq a_i \leq n-1$ and $0 \leq b_i \leq 1$ for every i, since if $a_i > n$, then $r_{a_i} = r^{a_i - n} \circ r^n = r^{a_i - n} \circ e = r^{a_i - n}$, and let $a_i = k_i n + u_i$, for $0 \leq u_i < n$, then $r^{a_i} = r^{k_i n + u_i} = (r^n)^{k_i} \circ r^{u_i} = r^{u_i}$. Similarly, if $b_i = 2l_i + v_i$, for $0 \leq v_i < 2$, then $s^{b_i} = (s^2)^{l_i} \circ s^{v_i} = s^{v_i}$.

Hence $b_{k-1} = 1$ and $x = y \circ r^{a_{k-1}} \circ (s \circ r^{a_k}) \circ s^{b_k}$. Now $s \circ r^{a_k} s = r^{-a_k} \implies s \circ r^{a_k} = r^{-a_k} s$, and so

$$\begin{aligned} x &= y \circ r^{a_{k-1}} \circ (r^{-a_k} \circ s) \circ s^{b_k} \\ &= y \circ r^{a_{k-1} - a_k} \circ s^{1 + b_k} \\ &= y \circ r^{a'_{k-1}} \circ s^{b'_{k-1}} \end{aligned}$$

where $a'_{k-1} = a_{k-1} - a_k$, $b'_{k-1} = 1 + b_k$. This representation has $k-1$ terms $r^{a_i} s^{b_i}$, contradicting the minimality of k. Hence $k = 1$.

To prove the uniqueness, TODO. $\square$

5.8 Homomorphisms of Groups

Definition 5.8.1. Let $(G_1, \circ_1), (G_2, \circ_2)$. A map $\phi : G_1 \to G_2$ is a **group homomorphism** if

$$\forall g, h \in G^2, \quad \phi(g \circ_1 h) = \phi(g) \circ_2 \phi(h)$$

Definition 5.8.2. A group homomorphism ϕ is a **isomorphism** if it is also a bijection.

Definition 5.8.3. Groups G_1 and G_2 are called **isomorphic** if there exists an isomorphism from G_1 to G_2. We write $G_1 \cong G_2$.

Proposition 5.8.4. Properties of a homomorphism $\phi : G_1 \to G_2$:

1. For e_{G_1} the identity in G_1 and e_{G_2} the identity in G_2, $\phi(e_{G_1}) = e_{G_2}$.
2. $\forall g \in G_1, \phi(g^{-1}) = \phi(g)^{-1}$.
3. If $G_1 = \langle \{g_1, \ldots, g_k\} \rangle$ then ϕ is determined by $\phi(g_1), \ldots, \phi(g_k)$. In particular, if $G_1 = \langle g \rangle = \{g^k : k \in \mathbb{Z}\}$, then $\phi : G_1 \to G_2$ gives the image $\{\phi(g)^k : k \in \mathbb{Z}\}$.

Proof.

1. $\forall g \in G_1, \phi(g) = \phi(g \circ_1 e_{G_1}) = \phi(g) \circ_2 \phi(e_{G_1}) \implies \phi(e_{G_1}) = \phi(g)^{-1} \circ_2 \phi(g) = e_{G_2}$.
2. $e_{G_1} = g \circ_1 g^{-1} \Rightarrow e_{G_2} = \phi(g \circ_1 g^{-1})$. Hence $e_{G_2} = \phi(g) \circ_2 \phi(g^{-1}) \implies \phi(g)^{-1} = \phi(g)^{-1} \circ_2 \phi(g) \circ_2 \phi(g^{-1}) = \phi(g^{-1})$.
3. TODO.

□

Definition 5.8.5. Let $\phi : G_1 \to G_2$ be a group homomorphism. The **kernel** of ϕ is defined as

$$\ker(\phi) := \{g \in G_1 : \phi(g) = e_{G_2}\} \subseteq G_1$$

Definition 5.8.6. Let $\phi : G_1 \to G_2$ be a group homomorphism. The **image** of ϕ is defined as

$$\mathrm{Im}(\phi) := \{\phi(g) : g \in G_1\} \subseteq G_2$$

Lemma 5.8.7. Let $\phi : G_1 \to G_2$ be a group homomorphism. Then $\ker \phi \leq G_1$, $\mathrm{Im} \leq G_2$ and $\ker(\phi) \lhd G_1$.

Example 5.8.8. Let G be a group and $g \in G$. Define the homomorphism $\phi : \mathbb{Z} \to G$ by

$$\phi(k) := g^k$$

Then $\phi(k_1 + k_2) = g^{k_1+k_2} = g^{k_1} \circ g^{k_2} = \phi(k_1) \circ \phi(k_2)$.

$$\ker(\phi) = \{kd : k \in \mathbb{Z}\}$$

where $d = \mathrm{ord}(g)$. If $d = \infty$ then $\ker(\phi) = \{0\}$, otherwise $\ker(\phi) = d\mathbb{Z}$.

$$\mathrm{Im}(\phi) = \langle g \rangle$$

So if $G = D_n$ and $g = s$ then $\mathrm{ord}(g) = 2$ so $\ker(\phi) = 2\mathbb{Z}$ and $\mathrm{Im}(\phi) = \{e, s\}$.

Example 5.8.9. Consider the sign map $\mathrm{sgn} : S_n \to \{1, -1\}$. If $\sigma_1, \sigma_2 \in (S_n)^2$, $\sigma = \tau_1 \circ \cdots \circ \tau_r$, $\sigma = \tau_1' \circ \cdots \circ \tau_s'$, where the τ_i and τ_i' are transpositions. So

$$\sigma_1 \circ \sigma_2 = \tau_1 \circ \cdots \circ \tau_r \circ \tau_1' \circ \cdots \circ \tau_s'$$

which gives $\mathrm{sgn}(\sigma_1 \circ \sigma_2) = (-1)^{r+s} = (-1)^r (-1)^s = \mathrm{sgn}(\sigma_1)\mathrm{sgn}(\sigma_2)$. Then

$$\ker(\mathrm{sgn}) = \{\sigma \in S_n : \mathrm{sgn}(\sigma) = 1\} = A_n$$
$$\mathrm{Im}(\mathrm{sgn}) = \{1, -1\}$$

Example 5.8.10. Let $n \geq 1$ and let the homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}/n$ be defined by

$$\phi(k) = \bar{k} = k \pmod{n}$$

Then

$$\ker(\phi) = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$$
$$\mathrm{Im}(\phi) = \mathbb{Z}/n$$

Proposition 5.8.11. Let $\phi : G_1 \to G_2$. Then

1. $\mathrm{Im}(\phi) \leq G_2$.

2. $\ker(\phi) \leq G_1$.

3. $\ker(\phi) \triangleleft G_1$.

Proof.

1. TODO.

2. TODO.

3. We must show that $\forall g \in G_1, h \in \ker(\phi)$, $ghg^{-1} \in \ker(\phi)$, i.e. $\phi(ghg^{-1}) = e_{G_2}$.

$$\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g)^{-1} = \phi(g) \circ_2 e_{G_2} \circ_2 \phi(g)^{-1} = \phi(g) \circ_2 \phi(g)^{-1} = e_{G_2}$$

$\square$

5.9 Quotient groups

Definition 5.9.1. Let G be a group and $H \leq G$. The **quotient group** of G by H, G/H is defined as

$$G/H := \{g \circ H : g \in G\}$$

Proposition 5.9.2. If $H \triangleleft G$, then

1. $(g_1 \circ H) \circ_{G/H} (g_2 \circ H) = (g_1 \circ g_2) \circ_{G/H} H$.

2. $(g \circ H) \circ_{G/H} (g^{-1} \circ H) = H$.

Proof.

1. The set $(g_1 \circ H) \circ_{G/H} (g_2 \circ H)$ is $\{g_1 \circ h_1 \circ g_2 \circ h_2 : h_1, h_2 \in H^2\}$. WE claim this is equal to $\{g_1 \circ g_2 \circ h' : h' \in H\}$. As these are both cosets, if they intersect then they are equal.

   Let $g_1 \circ h_1 \circ g_2 \circ h_2 \in (g_1 \circ H) \circ_{G/H} (g_2 \circ H)$. Note that $h_1 \circ g_2 \in H \circ g_2$. Since $H \triangleleft G$, $H \circ g_2 = g_2 \circ H$. So $\exists h' \in H, h_1 \circ g_2 = g_2 \circ h' \implies g_1 \circ (h_1 \circ g_2) \circ h_2 = g_1 \circ (g_2 \circ h')h_2 = g_1 \circ g_2 \circ (h' \circ h_2) \in g_1 \circ g_2 \circ H$. So the cosets intersect and so are equal.

2. $(g \circ H) \circ_{G/H} (g^{-1} \circ H) = (g \circ g^{-1}) \circ H = e \circ H = H$.

$\square$

Remark. There is a natrual homomorphism $\phi : G \to G/H$, where $H \triangleleft G$, given by

$$\phi(g) = g \circ H$$

Remark. The identity in G/H is $H = e \circ H$ since $(g \circ H) \circ_{G/H} H = (g \circ e) \circ H = g \circ H$.

Example 5.9.3. Let $G = (\mathbb{Z}, +)$ and $H = n\mathbb{Z}$ for some $n \in \mathbb{N}$. Since G is Abelian, $H \triangleleft G$. Then

$$G/H = \mathbb{Z}/n$$

Example 5.9.4. Let $G = S_n$, $H = A_n$. $A_n \triangleleft S_n$, so

$$G/H = \{A_n, \tau A_n\}$$

where $\tau \in S_n$ is a transposition. The composition rule on S_n/A_n gives

$$A_n \circ A_n = A_n$$
$$A_n \circ (\tau \circ A_n) = (e \circ \tau) \circ A_n = \tau \circ A_n$$
$$(\tau \circ A_n) \circ (\tau \circ A_n) = (\tau \circ \tau) \circ A_n = e \circ A_n = A_n$$

Example 5.9.5. Let $G = D_n$, $H = \langle r \rangle$. $H \triangleleft G$, so

$$G/H = \{s \circ \langle r \rangle, \langle r \rangle\}$$

since

$$\begin{aligned} D_n &= \{r^i \circ s^j : 0 \leq i \leq n-1, 0 \leq j \leq n-1\} \\ &= \{r^i : 0 \leq i \leq n-1\} \cup \{r^i \circ s : 0 \leq i \leq n-1\} \\ &= \{s \circ r^i : 0 \leq i \leq n-1\} \end{aligned}$$

since $s \circ r \circ s = r^{-1}$.

Theorem 5.9.6. (**First isomorphism theorem (FIT) for groups**) Let $\phi : G_1 \to G_2$ be a group homomorphism. Then

$$\mathrm{Im}(\phi) \cong G_1/\ker(\phi)$$

Proof. We construct an isomorphism $\tilde{\phi} : G/\ker(\phi) \to \mathrm{Im}(\phi)$ by

$$\tilde{\phi}(g \circ \ker(\phi)) = \phi(g)$$

We need to show that $\tilde{\phi}$ is an homomorphism. Let $g_1 \circ \ker(\phi), g_2 \circ \ker(\phi) \in (G/\ker(\phi))^2$.

$$\begin{aligned} \tilde{\phi}((g_1 \circ \ker(\phi)) \circ (g_2 \circ \ker(\phi))) &= \tilde{\phi}(g_1 \circ g_2 \circ \ker(\phi)) \\ &= \phi(g_1 \circ g_2) = \phi(g_1) \circ \phi(g_2) \\ &= \tilde{\phi}(g_1 \circ \ker(\phi)) \circ \tilde{\phi}(g_2 \circ \ker(\phi)) \end{aligned}$$

Hence $\tilde{\phi}$ is an homomorphism. We now need to show that $\tilde{\phi}$ is injective, i.e. $\ker(\tilde{\phi}) = \{\ker(\phi)\}$. Suppose $g \circ \ker(\phi) \in \ker(\phi)$, then

$$\begin{aligned} \phi(g) &= \tilde{\phi}(g \circ \ker(\phi)) \\ &= e_{G_2} \implies g \in \ker(\phi) \\ &\implies g \circ \ker(\phi) = \ker(\phi) \\ &\implies \ker(\tilde{\phi}) = \{\ker(\phi)\} \end{aligned}$$

Finally, we need to show that $\tilde{\phi}$ is surjective. Since $x \in \mathrm{Im}(\phi) \iff \exists g \in G_1,\ \phi(g) = x$, $x = \tilde{\phi}(g \circ \ker(\phi))$ hence $\tilde{\phi}$ is surjective. ☐

Corollary 5.9.7. Let G be a group and $g \in G$ with $\mathrm{ord}(g) = n < \infty$. Then

$$\langle g \rangle \cong (\mathbb{Z}/n, +)$$

If $\mathrm{ord}(g) = \infty$, then $\langle g \rangle \cong (\mathbb{Z}, +)$.

Proof. Define a map $\phi : \mathbb{Z} \to \langle g \rangle$ by

$$\phi(k) = g^k$$

This is a homomorphism, and if $\mathrm{ord}(g) = n < \infty$ then

$$\ker(\phi) = n\mathbb{Z} \implies \mathbb{Z}/\ker(\phi) = \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n$$

So by FIT for groups,

$$\mathbb{Z}/n = \mathrm{Im}(\phi_n) \cong \mathbb{Z}/\ker(\phi_n) = \mathbb{Z}/n\mathbb{Z}$$

$\mathrm{Im}(\phi) = \langle g \rangle$ by definition, so by FIT for groups, $\mathbb{Z}/n \cong \langle g \rangle$. The case $\mathrm{ord}(g) = \infty$ is similar, except that $\ker(\phi) = \{0\}$. ☐

Corollary 5.9.8. Let G be a finite group with $|G| = p$ where p is prime. Then $G \cong (\mathbb{Z}/p, +)$.

Proof. G is a cyclic group since $|G|$ is prime. Thus, $G = \langle g \rangle$ where $\text{ord}(g) = p$. By the previous corollary, $G \cong (\mathbb{Z}/p, +)$. $\square$

Example 5.9.9. Let $\phi_n : \mathbb{Z} \to \mathbb{Z}/n$ by defined by

$$\phi_n(k) = \bar{k} = \{k + nm : m \in \mathbb{Z}\}$$

Then $\ker(\phi_n) = n\mathbb{Z}$ and $\text{Im}(\phi_n) = \mathbb{Z}/n$ since $\forall 0 \leq j \leq n-1,\ \phi(j) = j$.

Example 5.9.10. We have seen that $\ker(\text{sgn}) = A_n$ and $\text{Im}(\text{sgn}) = \{\pm 1\}$. So by FIT for groups,

$$\{\pm 1\} \cong S_n/A_n$$

Also note that $\{\pm 1\} \cong \mathbb{Z}/2$. So $S_n/A_n \cong \mathbb{Z}/2$.

Example 5.9.11. Let $\phi : D_n \to \mathbb{Z}/2$ be defined as

$$\phi(r^i s^j) = j \pmod 2$$

$\text{Im}(\phi) = \mathbb{Z}/2$ and $\ker(\phi) = \{r^i : 0 \leq i \leq n-1\} = \langle r \rangle$. So by FIT for groups,

$$D_n/\langle r \rangle \cong \mathbb{Z}/2$$

5.10 Isomorphisms invariants

Lemma 5.10.1. Let $\phi : G_1 \to G_2$ be a group isomorphism. Then

1. If $g \in G$ then $\text{ord}_{G_1}(g) = \text{ord}_{G_2}(\phi(g))$. In particular, the sets $\{\text{ord}_{G_1}(g) : g \in G_1\}$ and $\{\text{ord}_{G_2}(g) : g \in G_2\}$ are equal.
2. $|G_1| = |G_2|$.
3. G_1 is Abelian iff G_2 is also Abelian.
4. The sets $|H| : H \leq G_1$ and $|H| : H \leq G_2$ are equal.

Proof.

1. Let $g \in G_1$ and let $d_1 := \text{ord}_{G_1}(g), d_2 := \text{ord}_{G_2}(\phi(g))$. Note that

   $$e_{G_2} = \phi(e_{G_1}) = \phi(g^{d_1}) = \phi(g)^{d_1} \implies d_2 \leq d_1$$

   But also,

   $$e_{G_2} = \phi(g)^{d_2} = \phi(g^{d_2})$$

   Since ϕ is injective, $g^{d_2} = e_{G_1}$, so $d_1 \leq d_2$, hence $d_1 = d_2$.
2. TODO.
3. TODO.
4. TODO.

$\square$

Example 5.10.2. Give a reason why each of these pairs of groups are not isomorphic:

1. D_4 and $\mathbb{Z}/4$: $|D_4| = 8$ and $|\mathbb{Z}/4| = 4$.

2. S_3 and $\mathbb{Z}/6$: S_3 is not Abelian, but $\mathbb{Z}/6$ is.

3. A_4 and D_6: in D_6, $\mathrm{ord}(r) = 6$ but in A_4, the permutations have orders of $1, 2$ or 3.

Example 5.10.3. (Problems class) Decompose D_6 into left cosets with respect to $H = \{e, r^3, s, r^3, s\}$. Is every left coset also a right coset?

We want to express D_6 as

$$D_6 = H \cup x \circ H \cup y \circ H$$

where $x, y \in (D_6)^2, x \circ H \neq H, x \circ H \neq y \circ H$. (Since $|H| = |x \circ H| = |y \circ H| = 4$ and they are disjoint so $|H \cup x \circ H \cup y \circ H) = 12 = |D_6|$). We have that

$$D_6 = \{r^i \circ s^j : 0 \leq i \leq 5, 0 \leq j \leq 1\}$$

- If $j = 0, 0 \leq i \leq 2$ then $r^i \circ s^j = r^i \circ e \in r^i \circ H$.
- If $j = 0, 3 \leq i \leq 5$ then $r^i \circ s^j = r^{i-3} \circ r^3 \in r^{i-3} \circ H$.
- If $j = 1, 0 \leq i \leq 2$ then $r^i \circ s^j = r^i \circ s \in r^i \circ H$.
- If $j = 1, 3 \leq i \leq 5$ then $r^i \circ s^j = r^{i-3} \circ r^3 \circ s \in r^{i-3} \circ H$.

So $\forall x \in D_6, x \in H \cup r \circ H \cup r^2 \circ H$ so $D_6 \subseteq H \cup r \circ H \cup r^2 \circ H$. But each of $H, r \circ H, r^2 \circ H$ are a subset of D_6 so $D_6 = H \cup r \circ H \cup r^2 \circ H$. Now we determine whether every left coset is a right coset. If this were true, then

$$r \circ H = \{r, r^4, r \circ s, r^4 \circ s\} = H \circ x = \{x, r^3 \circ x, s \circ x, r^3 \circ s \circ s\}$$

for some $x \in D_6$. Using the fact that $s \circ r \circ s = r^{-1}$, $r \circ H = \{r, r^4, s \circ r^5, s \circ r^2\}$. $r \in H \circ r$ and $r^4 \in H \circ r$ but $s \circ r^5 = s \circ r^3 \circ r^2 = (r^3 \circ s) \circ r^2 \in H \circ r^2$ and $s \circ r^2 \in H \circ r^2$. So $r \circ H \subseteq H \circ r \cup H \circ r^2$ and intersects both, so it can't be a right coset (since if $r \circ H = H \circ x$ then $H \circ x = H \circ r$ or $H \circ x \cap H \circ r = \emptyset$, but $H \circ r \neq H \circ r^2$, $H \circ x \cap H \circ r \neq \emptyset$ and $H \circ x \cap H \circ r^2 \neq \emptyset$).

Example 5.10.4. (Problems class) Show that A_4 has no subgroup of order 6.

We use the fact that there only two groups of order 6 (up to isomorphism): $\mathbb{Z}/6$ and S_3. So to show any $H \leq |A_4|$ has $|H| \neq 6$, we can show that $H \ncong \mathbb{Z}/6$ and $H \ncong S_3$. Since $H \leq A_4$, if $x \in H$, then $\mathrm{ord}(x) \in \{1, 2, 3\}$. But $\bar{1} \in \mathbb{Z}/6$ has order 6. But isomorphisms preserve order so $\mathbb{Z}/6 \ncong H$.

$S_3 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ has 1 element of order 1, three elements of order 2 and two elements of order 2. Consider $\tau \circ \sigma$ where $\tau, \sigma \in H^2, \mathrm{ord}(2) = 2, \mathrm{ord}(\sigma) = 3$. A_4 contains only the order 2 elements $\{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. As H has three order 2 elements, H must contain all of these. Up to relabelling, we can assume that $(1\ 2\ 3) \in H$. But then $(1\ 2)(3\ 4)(1\ 2\ 3) = (2\ 4\ 3)$, $(1\ 3)(2\ 4)(1\ 2\ 3) = (1\ 4\ 2)$, and $(1\ 4)(2\ 3)(1\ 2\ 3) = (1\ 3\ 4)$ which are distinct 3-cycles. So there are at least 3 elements of order 3 in H, but there should only be 2.

Example 5.10.5. (Problems class) Construct an isomorphism $\phi : D_3 \to S_3$. How many such isomorphisms exist?

As D_3 is generated by r and s, it is enough to determine $\phi(r)$ and $\phi(s)$ in order to determine ϕ. Since isomorphisms fix the orders of elements, $\mathrm{ord}_{S_3}(\phi(r)) = \mathrm{ord}_{D_3}(r) = 3$ and $\mathrm{ord}_{S_3}(\phi(s)) = \mathrm{ord}_{D_3}(s) = 2$. There are two elements of order 3 in S_3 and 3 elements of order 2 in S_3, so there are $2 \cdot 3 = 6$ possible values of $(\phi(r), \phi(s))$. So there are six possible isomorphisms. For example $\phi(r) = (1\ 2\ 3), \phi(s) = (1\ 2)$.

5.11 Direct products

Definition 5.11.1. Let $(G_1, \circ_1)$ and $(G_2, \circ_2)$ be groups. The **direct product** of G_1 and G_2 is the set

$$G \times H = \{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\}$$

equipped with the operation $\circ_{G_1 \times G_2}$ defined by

$$(g_1, g_2) \circ_{G_1 \times G_2} (h_1, h_2) = (g_1 \circ_1 h_1, g_2 \circ_2 h_2)$$

We can also define, by induction,

$$G_1 \times G_2 \times \cdots \times G_n = \{(g_1, g_2, \ldots, g_n) : \forall i \in \{1, \ldots, n\},\ g_i \in G_i\}$$

Example 5.11.2. Let $G_1 = \mathbb{Z}/3, G_2 = \mathbb{Z}/4$, then

$$G_1 \times G_2 = \{(a \pmod 3), b \pmod 4)) : a, b \in \mathbb{Z}^2\}$$

and $(\bar{a} + \bar{b}) + (\bar{c}, \bar{d}) = (\overline{a+c}, \overline{b+d})$.

Example 5.11.3. Let $G_1 = S_3, G_2 = S_4$, then for every $\sigma_1, \sigma_2 \in (S_3)^2, \alpha_1, \alpha_2 \in (S_4)^2$,

$$(\sigma_1, \alpha_1) \circ (\sigma_2, \alpha_2)(i, j) = (\sigma_1 \circ \sigma_2, \alpha_1 \circ \alpha_2)(i, j)$$

where $i \in \{1, 2, 3\}, j \in \{1, 2, 3, 4\}$.

Lemma 5.11.4. If G_1 and G_2 are groups, then $G_1 \times G_2$ is a group.

Proof. Using the properties of a group,

- $\circ_{G_1 \times G_2}$ is associative.
- By definition, $G_1 \times G_2$ is closed under $\circ_{G_1 \times G_2}$.
- The identity element is (e_G, e_H).
- The inverse of (g_1, g_2) is (g_1^{-1}, g_2^{-1}).

□

Proposition 5.11.5. (**Properties of the direct product**)

1. $\forall d \in \mathbb{Z}, (g, h) \in G_1 \times G_2$, $(g_1, g_2)^d = (g_1^d, g_2^d)$.
2. If $\mathrm{ord}_{G_1}(g_1) = n$ and $\mathrm{ord}_{G_2}(g_2) = m$, then $\mathrm{ord}_{G_1 \times G_2}((g_1, g_2)) = \mathrm{lcm}(n, m)$.
3. If $H_1 \leq G_1$ and $H_2 \leq G$ then $H_1 \times H_2 \leq G_1 \times G_2$. Note that if $H_2 = \{e_{G_2}\}$, then $H_1 \times H_2 \cong H_2$, with $(h_1, h_2) \to h_1$ as the isomorphism.

5.12 Subgroups in direct products

Example 5.12.1. There exist subgroups of $G_1 \times G_2$ that are not direct products of subgroups of G_1 and G_2.

Let $G_1 = G_2 = \mathbb{Z}$, then $G_1 \times G_2 = \{(a,b) : a, b \in \mathbb{Z}^2\}$. Let $K = \{(a,a) : a \in \mathbb{Z}\}$, the diagonal subgroup. But K is not a direct product of two subgroups of G_1 and G_2.

Theorem 5.12.2. Let G be a group that contains subgroups H, K such that

1. $H \times K = \{hk : h \in H, k \in K\} = G$.
2. $H \cap K = \{e_G\}$.
3. For every $h \in H, k \in K,\ hk = kh$.

Then $G \cong H \times K$.

Proof. Omitted. □

Theorem 5.12.3. (**Chinese remainder theorem (CRT)**) Let $m, n \in \mathbb{N}^2$ be coprime. Then

$$\mathbb{Z}/(mn) \cong \mathbb{Z}/n \times \mathbb{Z}/n$$

Proof. Let $G = \mathbb{Z}/(mn)$. Let $H = \{nx \pmod{mn} : 0 \leq x \leq m-1\}$ and $K = \{ny \pmod{mn} : 0 \leq y \leq n-1\}$. Then $H \cong \mathbb{Z}/m$ and $K \cong \mathbb{Z}/n$. We have

1. $HK = \{nx + my \pmod{mn} : 0 \leq x \leq m-1, 0 \leq y \leq n-1\} = \{z \pmod{mn} : 0 \leq z \leq mn-1$.
2. If $z \in H \cap K$ for some z then $z = nx = ny$ for some $0 \leq x \leq m-1$, $0 \leq y \leq n-1$. Since m and n are coprime, $x = y = 0$ so $H \cap K = \{\bar{0}\}$.
3. G is abelian so $hk = kh$ for every $h \in H$, $k \in K$.

So by Theorem 5.12.2, $G \cong H \times K$ so $\mathbb{Z}/(mn) \cong \mathbb{Z}/n \times \mathbb{Z}/n$. □

Example 5.12.4. $D_{10} \cong D_5 \times \mathbb{Z}/2$.

Let $G = D_{10}$. Let $H = \{r^{2k}s^j : 0 \leq k \leq 4, 0 \leq j \leq 1\}$ and $K = \{e, r^5\} = \langle r^5 \rangle$. Then $H \cong D_5$ and $K \cong \mathbb{Z}/2$. So by Theorem 5.12.2, $H \cong G \times K$.

Theorem 5.12.5. (**Cayley's theorem**) Let $(G, \cdot)$ be a group. Then $(G, \cdot)$ is isomorphic to a subgroup of S_G, the group of bijections $\phi : G \to G$, with the group operation as composition.

Proof. Let $\psi : G \to S_G$ be the bijection defined by

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

ψ is a homomorphism, since

$$\psi(g_1 g_2)(h) = (g_1 g_2)h = g_1(g_2 h) = \psi(g_1)(\psi(g_2)(h)) = (\psi(g_1) \circ \psi(g_2))(h)$$

$\ker(\psi) = \{e_G\}$, since if $g \in \ker(\psi)$, then $\psi(g)$ is the identity map, so $\psi(g)(h) = gh = h$ for every $h \in G$, so $g = e_G$. We have seen that $G/\ker(\psi) \cong \mathrm{Im}(\psi)$, so $G \cong G/\{e_G\} \cong \mathrm{Im}(\psi)$. And $\mathrm{Im}(\psi) \leq S_G$, since ψ is a homomorphism. □

Example 5.12.6. Let $(G, \circ) = (\mathbb{Z}/4, +)$ and let $\psi(\bar{a})(\bar{b}) = \bar{a} + \bar{b}$. The group table is

$$\begin{array}{ccccc} + & \bar{1} & \bar{2} & \bar{3} & \bar{4} \\ \psi(\bar{1}) & \bar{3} & \bar{4} & \bar{1} & \bar{2} \\ \psi(\bar{2}) & \bar{4} & \bar{1} & \bar{2} & \bar{3} \\ \psi(\bar{3}) & \bar{4} & \bar{1} & \bar{2} & \bar{3} \\ \psi(\bar{4}) & \bar{1} & \bar{2} & \bar{3} & \bar{4} \end{array}$$

So $\psi(\bar{1})$ corresponds to the cycle

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} = (1\ 2\ 3\ 4)$$

etc. We see $\mathbb{Z}/4$ is isomorphic to a subgroup o S_4.

Example 5.12.7. Let $G = D_3 = \{r^i s^j : 0 \leq i \leq 2, 0 \leq j \leq 1\}$. A section of the group table looks like

$$\begin{array}{ccccccc} \circ & e & r & r^2 & s & rs & r^2s \\ \psi(r) & r & r^2 & e & rs & r^2s & s \\ \psi(s) & s & r^2s & rs & e & r^2 & r \end{array}$$

so $\psi(r)$ corresponds to the cycle

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{bmatrix} = (1\ 2\ 3)(4\ 5\ 6)$$

6 Group Actions

6.1 Group actions

Definition 6.1.1. Let G be a group and X be a set. A **group action** of G on X is a homomorphism $\psi : G \to S_X$ (S_X is the set of bijections on X) such that

1. $\psi_g : X \to X$ is a bijection for every $g \in G$, and
2. $\psi_{g_1 g_2} = \psi_{g_1} \circ \psi_{g_2}$ for every $g_1, g_2 \in G^2$.

We say that G acts on X. We sometimes use the notation $g \cdot x$ to mean $\psi_g(x)$.

Definition 6.1.2. Let $\psi : G \to S_X$ be a group action. Let $x \in X$.

- The **orbit** of x, denoted $\mathcal{O}(x)$, is defined as

$$\mathcal{O}(x) := \{y \in X : \exists g \in G : \psi_g(x) = y\}$$

- The **stabiliser** of x, denoted $\mathrm{Stab}_G(x)$, is defined as

$$\mathrm{Stab}_G(x) := \{g \in G : \psi_g(x) = x\}$$

Lemma 6.1.3. For every $x \in X$, $\mathrm{Stab}_G(x) \leq G$.

Proof. Check the subgroup criteria:

1. $e \in \mathrm{Stab}_G(x)$, since $\psi_e(x) = x$ (ψ_e is the identity map).
2. Let $g_1, g_2 \in (\mathrm{Stab}_G(x))^2$. Then $\psi_{g_1 g_2}(x) = (\psi_{g_1} \circ \psi_{g_2})(x) = \psi_{g_1}(\psi_{g_2}(x)) = \psi_{g_1}(x) = x$. Hence $g_1 g_2 \in \mathrm{Stab}_G(x)$.
3. Let $g \in \mathrm{Stab}_G(x)$. Then $\psi_{g^{-1}}(x) = \psi_g^{-1}(\psi_g(x)) = \psi_{g^{-1}g}(x) = \psi_e(x) = x$. Hence $g^{-1} \in \mathrm{Stab}_G(x)$.

$\square$

Example 6.1.4. Let $(G, \circ) = (\mathbb{Z}, +)$, $X = \mathbb{R}$, $\psi_n(x) = n + x$. Then

$$\psi_{n_1+n_2}(x) = (n_1 + n_2) + x = n_1 + (n_2 + x) = \psi_{n_1}(n_2 + x) = \psi_{n_1}(\psi_{n_2}(x))$$

So ψ is a group action of G on X. Also,

$$\mathcal{O}(x) = \{n + x : n \in \mathbb{Z}\}$$
$$\mathrm{Stab}_G(x) = \{n \in \mathbb{Z} : n + x = x\} = \{0\}$$

Example 6.1.5. Let $(G, \circ) = (\mathbb{R}_{\geq 0}, \cdot)$, $X = \mathbb{C}$, $\psi_r(z) = rz$. Then ψ is a group action of G on X.

If $z \neq 0$, then $\mathcal{O}(x)$ is the line from 0 through z. If $z = 0$, then $\mathcal{O}(x) = \{0\}$. Also,

$$\mathrm{Stab}_G(x) = \{r > 0 : rz = z\} = \begin{cases} (0, \infty) & \text{if } z = 0 \\ \{1\} & \text{if } z \neq 0 \end{cases}$$

Example 6.1.6. Let $G = \mathrm{GL}_2(\mathbb{R})$, $X = \mathbb{R}^2$, $\psi_A(x, y) = A(x, y)$. Then ψ is a group action of G on X.

$$\mathcal{O}(x, y) = \{A(x, y) : A \in \mathrm{GL}_2(\mathbb{R})\}$$
$$\mathrm{Stab}_G(x, y) = \{A \in \mathrm{GL}_2(\mathbb{R}) : A(x, y) = (x, y)\}$$

so $\mathrm{Stab}_G(x, y)$ is the set of $A \in G$ such that (x, y) is an eigenvalue of A with eigenvalue 1.

Proposition 6.1.7. Let a group G act on a set X with group action ψ. Then

$$\bigcup_{x \in X} \mathcal{O}(x) = X$$

and if $x, y \in X^2$ are such that $\mathcal{O}(x) \neq \mathcal{O}(y)$, then $\mathcal{O}(x) \cap \mathcal{O}(y) = \emptyset$.

Proof. For every $x \in X$, $x \in \mathcal{O}(x)$, since $\psi_e(x) = x$. So $\mathcal{O}(x) \neq \emptyset$ and

$$X = \bigcup_{x \in X} \{x\} \subseteq \bigcup_{x \in X} \mathcal{O}(x) \subseteq X$$

so

$$\bigcup_{x \in X} \mathcal{O}(x) = X$$

Assume that for some $x, y \in x^2$ with $\mathcal{O}(x) \neq \mathcal{O}(y)$, $\mathcal{O}(x) \cap \mathcal{O}(y) \neq \emptyset$. Then there exists $z \in \mathcal{O}(x) \cap \mathcal{O}(y)$. So for some $g, h \in G^2$, $\psi_g(x) = z = \psi_h(y) \implies (\psi_{h^{-1}} \circ \psi_g)(x) = y = \psi_{h^{-1}g}(x)$.

Hence if $g' \in G$, $\psi_{g'}(y) = (\psi_{g'} \circ \psi_{h^{-1}g}) = \psi_{g'h^{-1}g}(x)$. So for every $y' \in \mathcal{O}(y)$, $y' \in \mathcal{O}(x)$. Similarly, for every $x' \in \mathcal{O}(x)$, $x' \in \mathcal{O}(y)$. So $\mathcal{O}(x) = \mathcal{O}(y)$, which is a contradiction. $\square$

6.2 The action of a group on itself

Definition 6.2.1. The **conjugation action** for a group G is defined as $\psi : G \to S_G$,

$$\psi_g(h) := ghg^{-1}$$

Definition 6.2.2. Let G be a group and $h, h' \in G^2$. h and h' are called **conjugate** if for some $g \in G$,

$$h' = ghg^{-1}$$

Equivalently, h and h' are conjugate if and only if $h' \in \mathcal{O}(h)$ under the conjugation action.

Definition 6.2.3. The **conjugacy class** of $h \in G$ is defined as

$$\mathrm{ccl}_G(h) := \{ghg^{-1} : g \in G\}$$

Remark. Since conjugacy classes are orbits under the conjugation action, if $g \in \mathrm{ccl}_G(h)$, then $\mathrm{ccl}_G(h) = \mathrm{ccl}_G(g)$.

Proposition 6.2.4. The conjugation action is a group action.

Proof. We check the properties defined in Definition 6.1.1:

1. $\psi_{g_1g_2}(h) = g_1g_2h(g_1g_2)^{-1} = g_1(g_2hg_2^{-1})g_1^{-1} = \psi_{g_1}(g_2hg_2^{-1}) = (\psi_{g_1} \circ \psi_{g_2})(h)$.
2. $\psi_g(h_1) = \psi_g(h_2) \iff gh_1g^{-1} = gh_2g^{-1} \iff h_1 = h_2$ so ψ_g is injective. Also, if $h \in G$, then $x = g^{-1}hg$, so $\psi_g(x) = g(g^{-1}hg)g^{-1} = h$ if ψ_g is surjective.

$\square$

Example 6.2.5. $\mathrm{ccl}_G(e_G) = \{e_G\}$.

Example 6.2.6. Let G be Abelian and $h \in G$. Then $\mathrm{ccl}_G(h) = \{h\}$. So for every Abelian group G and $h \in G$, $|\mathrm{ccl}_G(h)| = 1$.

Conversely, let G be a group such that for every $h \in G$, $|\mathrm{ccl}_G(h)| = 1$. Since $h \in \mathrm{ccl}_G(h)$ ($h = ehe$), $\forall g \in G, ghg^{-1} = h$ so $gh = hg$ so G is Abelian.

Proposition 6.2.7. All elements in $\mathrm{ccl}_G(h)$ have the same order.

Proof. For every $g, h \in G^2$,

$$(ghg^{-1})^k = gh^kg^{-1} \implies \mathrm{ord}_G(h) = \mathrm{ord}_G(ghg^{-1})$$

□

Example 6.2.8. Let $G = S_3 = \{e_1, (1\ 2), (2\ 3), (1\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$. By Proposition 6.2.7, $\mathrm{ccl}_G((1\ 3))$ contains only transpositions and $\mathrm{ccl}_G((1\ 2\ 3))$ contains only 3-cycles.

$$\begin{aligned}(1\ 2)(1\ 3)(1\ 2) &= (2\ 3),\\ (2\ 3)(1\ 3)(2\ 3) &= (1\ 2),\\ e(1\ 3)e &= (1\ 3)\end{aligned}$$

so $(1\ 2), (1\ 3), (2\ 3) \in (\mathrm{ccl}_G((1\ 3)))^3$. But $\mathrm{ccl}_G((1\ 3))$ contains only transpositions so $\mathrm{ccl}_G((1\ 3)) = \{(1\ 2), (1\ 3), (2\ 3)\}$.

$(1\ 2) \in \mathrm{ccl}_G((1\ 2))$ so by Proposition 6.1.7, $\mathrm{ccl}_G((1\ 2)) = \mathrm{ccl}_G((1\ 3))$ and similarly, $\mathrm{ccl}_G((1\ 3)) = \mathrm{ccl}_G((2\ 3))$.

$(2\ 3)(1\ 2\ 3)(2\ 3) = (1\ 3\ 2)$ so $\mathrm{ccl}_G((1\ 2\ 3)) = \{(1\ 2\ 3), (1\ 3\ 2)\} = \mathrm{ccl}_G((1\ 3\ 2))$.

Example 6.2.9. Let $G = D_5 = \{r^ks^j : 0 \le k \le 4, 0 \le j \le 1\}$. Then

$$\begin{aligned}\mathrm{ccl}_G(r^k) &= \{r^is^jr^ks^jr^{-i} : 0 \le i \le 4, 0 \le j \le 1\} = \{r^k, r^{-k}\}\\ \mathrm{ccl}_G(r^ks) &= \{r^is^j(r^ks)s^jr^{-i} : 0 \le i \le 4, 0 \le k \le 4\} = \{r^is : 0 \le i \le 4\}\end{aligned}$$

6.3 The orbit stabiliser theorem

Lemma 6.3.1. Let $\psi : G \to S_G$, $\psi_g(h) = gh$. Then $\forall h \in G, |\mathcal{O}(h)| \cdot |\mathrm{Stab}_G(h)| = |G|$.

Proof. $\mathrm{Stab}_G(h) = \{e_G\}$ and $\mathcal{O}(h) = G$ for every $h \in G$. So $|\mathrm{Stab}_G(h)| = 1$ and $|\mathcal{O}(h)| = |G|$ for every $h \in G$. □

Lemma 6.3.2. Let $\psi : G \to S_G$, $\psi_g(h) = ghg^{-1}$ be the conjugation map. Then $|\mathrm{Stab}_G(e)| \cdot |\mathcal{O}(e)| = |G|$.

Proof. $\mathrm{Stab}_G(e) = G$ and $\mathcal{O}(e) = \{e\}$ so $|\mathrm{Stab}_G(e)| = |G|$ and $|\mathcal{O}(e)| = 1$. □

Theorem 6.3.3. (**The Orbit-Stabiliser Theorem**) Let $\psi : G \to S_X$ be a group action of G on X. Then $\forall x \in X$, there exists a bijection $\psi_x : \mathcal{O}(x) \to \{g \cdot \mathrm{Stab}_G(x) : g \in G\}$ defined as

$$\psi_x(\psi_g(x)) = g \cdot \mathrm{Stab}_G(x)$$

Proof. First we check that ψ_x is well-defined, i.e. if $y \in \mathcal{O}(x)$ can be written as $g_1 \cdot x = y = g_2 \cdot x$, then $\psi_x(g_1 \cdot x) = \psi_x(g_2 \cdot x)$. To show this, note if $g_1 \cdot x = g_2 \cdot x$, then $\psi_{g_1}(x) = \psi_{g_2}(x)$ so $(\psi_{g_2}^{-1} \circ \psi_{g_1})(x) = x = \psi_{g_2^{-1}g_1}(x) = (g_2^{-1}g_1) \cdot x$. So $g_2^{-1}g_1 \in \mathrm{Stab}_G(x) \implies g_1 \in g_2 \cdot \mathrm{Stab}_G(x)$ hence $\psi_x(g_1 \cdot x) = g_1 \cdot \mathrm{Stab}_G(x) = (g_2g) \cdot \mathrm{Stab}_G(x)$ where $g \in \mathrm{Stab}_G(x)$. So $\psi_x(g_1 \cdot x) = g_2 \cdot \mathrm{Stab}_G(x) = \psi_x(g_2 \cdot x)$.

We now show injectivity of ψ_x. Let $\psi_x(g_1 \cdot x) = \psi_x(g_2 \cdot x) \iff g_1 \cdot \mathrm{Stab}_G(x) = g_2\mathrm{Stab}_G(x) \iff g_2^{-1}g_1 \cdot \mathrm{Stab}_G(x) = \mathrm{Stab}_G(x) \iff g_2^{-1}g_1 \in \mathrm{Stab}_G(x) \iff g_2^{-1}g_1 \cdot x = x \iff g_1 \cdot x = g_2 \cdot x$. □

Remark. We use the notation $\psi_x(g \cdot x)$ to mean $g \cdot \mathrm{Stab}_G(x)$.

Corollary 6.3.4. Let G be a finite group. Then

$$\forall x \in X, |\mathcal{O}(x)| \cdot |\mathrm{Stab}_G(x)| = |G|$$

In particular, $|\mathcal{O}(x)|$ and $|\mathrm{Stab}_G(x)|$ divide $|G|$ for every $x \in X$.

Proof. By the orbit-stabiliser theorem,

$$|\mathcal{O}(x)| = |\{g \cdot \mathrm{Stab}_G(x) : g \in G\}|$$

Let $g_1 \cdot \mathrm{Stab}_G(x), \ldots, g_r \cdot \mathrm{Stab}_G(x)$ be the distinct cosets, with $r = |\mathcal{O}(x)|$. Since cosets of $H \geq G$ partition G,

$$G = \bigcup_{i=1}^{r} g_i \cdot \mathrm{Stab}_G(x)$$

Since these cosets are disjoint,

$$|G| = \sum_{i=1}^{r} |g_i \cdot \mathrm{Stab}_G(x)| = \sum_{i=1}^{r} |\mathrm{Stab}_G(x)| = r \cdot |\mathrm{Stab}_G(x)| = |\mathcal{O}(x)| \cdot |\mathrm{Stab}_G(x)|$$

□

7 Cauchy's Theorem and Classification of Groups

7.1 Cauchy's theorem

Theorem 7.1.1. (**Cauchy's theorem**) If G is finite and p is prime with $p \mid |G|$, then for some $g \in G$, $\mathrm{ord}_G(g) = p$.

Proof. Let $H = \mathbb{Z}/p$ and let

$$X = \{(g_1, \ldots, g_p) \in G^p : g_1 g_2 \cdots g_p = e_G\}$$

Then $\underline{e} := (e_G, \ldots, e_G) \in X$. We have that if $g \in G$,

$$\mathrm{ord}_G(g) = p \implies g^p = e \iff (g, \ldots, g) \in X$$

Also if $(g, \ldots, g) \in X$ and $g \neq e_G$, then $g^p = e_G$ so $\mathrm{ord}_G(g) \mid p \implies \mathrm{ord}_G(g) = p$. So we want to find tuples $(g, \ldots, g) \in X$ with $g \neq e_G$.

If $(g_1, \ldots, g_p) \in X$ then so are $(g_2, g_2, \ldots, g_p, g_1)$, $(g_{i+1}, \ldots, g_p, g_1, \ldots, g_i)$ for $i = 1, \ldots, p$, since if $x = (g_1 \cdots g_i)$ and $y = (g_{i+1} \cdots g_p)$ then $xy = e_G \iff yx = e_G$.

Define the group action of H on X for $\bar{i} \in H$ by

$$\bar{i} \cdot (g_1, \ldots, g_p) = (g_{i+1}, \ldots, g_p, g_1, \ldots, g_i)$$

By the orbit-stabiliser theorem,

$$|\{\bar{i} \cdot \underline{g} : \bar{i} \in \mathbb{Z}/p\}| = |\mathcal{O}(\underline{g})| \mid |H|$$

for every $\underline{g} \in X$. Hence for every $g \in X$, $|\mathcal{O}(g)| = 1$ or p. We know that X is partitioned by orbits, i.e.

$$X = \bigcup_{\underline{g} \in X} \mathcal{O}(\underline{g}) = \bigcup_{i=1}^{m} \mathcal{O}(\underline{g}_i)$$

where the $\mathcal{O}(\underline{g}_i)$ are distinct, thus disjoint. We are looking for $g \neq e_G$ such that $\underline{g} = (g, \ldots, g) \in X$, so $|\mathcal{O}(\underline{g})| = 1$. We have

$$\begin{aligned} |X| &= \left| \bigcup_{i=1}^{m} \mathcal{O}(\underline{g}_i) \right| \\ &= \sum_{i=1}^{m} |\mathcal{O}(\underline{g}_i)| \\ &= \sum_{i=1, |\mathcal{O}(\underline{g}_i)|=1}^{m} 1 + \sum_{i=1, |\mathcal{O}(\underline{g}_i)|=p}^{m} p \end{aligned}$$

Taking modulo p on both sides, we get

$$|\{1 \leq i \leq m : |\mathcal{O}(\underline{g_i})| = 1\}| \equiv 0 \pmod{p}$$

Since $\underline{e} = (e_G, \ldots, e_G) \in X$, it is cvered by $\mathcal{O}(\underline{g_1})$, without loss of generality. But then $\mathcal{O}(\underline{g}_1) = \mathcal{O}(\underline{e}) = \{\underline{e}\}$. So $\{1 \leq i \leq m : |\mathcal{O}(\underline{g_i})| = 1\} \neq \emptyset$ so $|\{1 \leq i \leq m : |\mathcal{O}(\underline{g_i})| = 1\}| \geq p$. since $p > 1$, for some $\underline{g_i} \neq \underline{e}$, $|\mathcal{O}(\underline{g_i})| = 1$. This completes the proof. □

Example 7.1.2. Let $G = S_5$, then $|G| = 5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$ and (1 2), (3 4 5) and (1 2 3 4 5) have prime orders 2, 3 and 5.

Example 7.1.3. Let $G = D_{10}$, then $|G| = 20 = 2 \cdot 2 \cdot 4$ and $\operatorname{ord}(s) = 2$, $\operatorname{ord}(r^2) = 5$.

Theorem 7.1.4. Given a finite group G with $|G| = 2p$, for p an odd prime, then either:

1. G is cyclic, so $G \cong \mathbb{Z}/2p$.

2. $G \cong D_p$.

Proof. By Cauchy's theorem, for some $a, b \in G^2$ such that $\operatorname{ord}_G(a) = 2$ and $\operatorname{ord}_G(b) = p$. Let $H := \langle b \rangle$. Then $|H| = p = \frac{1}{2}|G|$ hence $H \triangleleft G$, so $aH = Ha$. $b \in H \implies aba^{-1} = aba \in H$. Hence for some $0 \leq k \leq p-1$, $aba = b^k \implies b = ab^k a = (aba)^k = b^{k^2} \implies b^{k^2-1} = e_G$ (since a has order 2). $\operatorname{ord}_G(b) = p$ so $k^2 - 1 \equiv 0 \pmod{p}$. $\mathbb{Z}/p$ is a field and $(k+1)(k-1) \equiv 0 \pmod{p}$ so $k \equiv 1 \pmod{p}$ or $k \equiv -1 \pmod{p}$, so $k = p-1$ or $k = 1$.

If $k = p - 1$, then $aba = b^{p-1} = b^{-1}$, so $G \cong D_p$, with the isomorphism $\phi : D_p \to G$, $\phi(r) = b$, $\phi(s) = a$.

If $k = 1$, then $aba = b$, so $ab = ba$ since a has order 2. Let $x = ab$, then $\langle x \rangle = \{(ab)^k : k \in \mathbb{Z}\} = \{a^k b^k : k \in \mathbb{Z}\}$, hence $|\langle x \rangle| = 2p$ so $\langle x \rangle = G$ so $G \cong \mathbb{Z}/2p$, with the isomorphism $\phi : \mathbb{Z}/2p \to \langle x \rangle$, $\phi(i) = x^i$. $\square$

Example 7.1.5. Classify all groups G with $|G| = 74$.

$74 = 2 \cdot 37$ and 37 is prime, so by Theorem 7.1.4, $G \cong \mathbb{Z}/74$ or $G \cong D_{37}$.

Example 7.1.6. Show $S_3 \cong D_3$.

By Theorem 7.1.4, $S_3 \cong \mathbb{Z}/6$ or $S_3 \cong D_3$. Since S_3 does not contain an element of order 6, $S_3 \ncong \mathbb{Z}/6$. Hence $S_3 \cong D_3$.

Definition 7.1.7. Let G be a group. The **centre** of G is defined as

$$Z(G) := \{g \in G : gh = hg \ \forall h \in G\}$$

Definition 7.1.8. Let G be a group and $S \subseteq G$. The **centraliser** of S is defined as

$$Z(S) := \{g \in G : gh = hg \ \forall h \in S\}$$

If $S = \{h\}$ for some $h \in G$, then we write $Z(\{h\})$ as $Z(h)$.

Remark. For every $h \in G$,

$$Z(h) = \{g \in G : ghg^{-1} = h\}$$

is the stabiliser of h under the conjugation action.

Remark. For every $h \in G$, $Z(G) \subseteq Z(h)$.

Proposition 7.1.9. Let G be a finite group with $|G| = p^k$ where p is a prime and $k \in \mathbb{N}$. Then $Z(G) \neq \{e_G\}$.

Proof. Using the orbit-stabiliser theorem on the conjugation action of G on itself, $|G| = |\operatorname{ccl}(h)| \cdot |Z(h)| = |\operatorname{ccl}(h)| \cdot |\mathcal{O}(h)|$ for every $h \in G$, hence $|\operatorname{ccl}(h)| \mid |G|$. We have a partition

$$G = \bigcup_{g \in R} \operatorname{ccl}_G(g)$$

for $R \subseteq G$ a maximal subset, hence

$$|G| = \sum_{g \in R} |\operatorname{ccl}_G(g)| = \sum_{g \in R,\ |\operatorname{ccl}_G(g)=1} 1 + \sum_{g \in R,\ p || \operatorname{ccl}_G(g)|} |\operatorname{ccl}_G(p)|$$

$|\mathrm{ccl}_G(g)| = 1 \iff \mathrm{ccl}_G(g) = \{g\} \iff g = hgh^{-1}\ \forall h \in G \iff g \in Z(G)$. Therefore

$$|Z(G)| = |G| - \sum_{g \in R,\ p \mid |\mathrm{ccl}_G(g)|} |\mathrm{ccl}_G(g)| \equiv 0 \pmod p$$

since $p \mid |G|$ and $p \mid |\mathrm{ccl}_G(g)|$. Hence either $|Z(G)| = 0$ or $|Z(G)| \geq p$. Since $e_G \in Z(G)$, $|Z(G) \neq 0$ hence $|Z(G)| \geq p \geq 2$. So $Z(G) - \{e_G\} \neq \emptyset$. $\square$

Theorem 7.1.10. Given a finite group G with $|G| = p^2$, for p prime, then G is abelian and either $G \cong \mathbb{Z}/p^2$ or $G \cong \mathbb{Z}/p \times \mathbb{Z}/p$.

Proof. Since $Z(G) \geq G$, $|Z(G)| \in \{1, p, p^2\}$ by Lagrange's theorem. By Proposition 7.1.9, $|Z(G)| \neq 1$. If $|Z(G)| = p^2$ then $Z(G) = G$, so G is abelian. Now assume $Z(G) = p$.

Let $h \in G - Z(G)$. $|\mathrm{Stab}_G(h)| \mid |G|$ so $|\mathrm{Stab}_G(h)| \in \{p, p^2\}$, since $Z(G) \subseteq \mathrm{Stab}_G(h)$. If $|\mathrm{Stab}_G(h)| = p^2$ then $G = \mathrm{Stab}_G(h)$, so $ghg^{-1} = h$ for every $g \in G$, hence $h \in Z(G)$, which is a contradiction. So $|\mathrm{Stab}_G(h) = p = |Z(G)|$ hence $Z(G) = \mathrm{Stab}_G(h)$. But $h \in \mathrm{Stab}_G(h)$ since $hhh^{-1} = h$, hence $h \in Z(G)$ which is a contradiction. Thus $|Z(G)| = p^2$ and G is Abelian.

Now for every $g \in G$, $\mathrm{ord}_G(g) \mid |G|$ so $\mathrm{ord}_G(g) \in \{1, p, p^2\}$. If for some g, $\mathrm{ord}_G(g) = p^2$, then $\langle g \rangle \subseteq G$ and $|\langle g \rangle| = p^2$ so $\langle g \rangle = G$. Hence $G = \langle g \rangle \cong \mathbb{Z}/p^2$.

Otherwise, if $g \neq e_G$, then $\mathrm{ord}_G(g) = p$. We claim that if for some $x, y \in (G - \{e_G\})^2$ such that $y \neq x^j$ for every $0 \leq j \leq p-1$, then $G = \{x^i y^j : 0 \leq i, j \leq p-1\}$ (proof omitted). Thus we can construct an isomorphism

$$\phi : \mathbb{Z}/p \times \mathbb{Z}/p \to G$$

with $\phi(i, j) = x^i y^j$. $\square$

Example 7.1.11. Classify all proper subgroups of G, where $|G| = 578$. We have $578 = 2 \cdot 17^2$. The non-trivial divisors of 578 are therefore $\{2, 17, 2 \cdot 17, 17 \cdot 17\}$. Subgroups of order 2 and 17 are isomorphic to $\mathbb{Z}/2$ and $\mathbb{Z}/17$ respectively. Subgroups of order $17 \cdot 17$ are isomorphic to $\mathbb{Z}/289$ or $\mathbb{Z}/17 \times \mathbb{Z}/17$. Subgroups of order $2 \cdot 17$ are isomorphic to $\mathbb{Z}/34$ or D_{17}.

7.2 Classifying finitely generated Abelian groups

Definition 7.2.1. A group G is called **finitely generated** if for some $S \subseteq G$ with $|S| < \infty$, $S = \{g_1, \ldots, g_r\}$, then

$$G = \langle \{g_1, \ldots, g_r\} \rangle = \{g_1^{a_{1,1}} \ldots g_r^{a_{1,r}} g_2^{a_{2,1}} \ldots g_r^{a_{2,r}} \ldots g_1^{a_{n,1}} \ldots g_r^{a_{n,r}} : a_{i,j} \in \mathbb{Z}\}$$

Remark. Sometimes we use the notation $a_i g_i$ to mean $g_i^{a_i}$.

Remark. Not all groups are finitely generated, e.g. $(\mathbb{Q}, +)$ is not finitely generated, since if $\mathbb{Q} = \{a_1 \frac{m_1}{n_1} + \cdots + a_r \frac{m_r}{n_r} : a_i \in \mathbb{Z}\}$ for some generating set $\{\frac{m_1}{n_1}, \ldots, \frac{m_r}{n_r}\} \subseteq \mathbb{Q}$, then any element in $\mathbb{Q}$ can be written as

$$\frac{A}{n_1 \cdots n_r}$$

but $\frac{1}{n_1 \cdots n_r + 1}$ is not of this form.

Example 7.2.2. The size of the generating set S or its elements aren't unique.

Example 7.2.3. $(\mathbb{Z}, +) = \langle 1 \rangle = \langle \{2, -1\} \rangle = \langle \{2, 3\} \rangle$.

Example 7.2.4. $\mathbb{Z}^k = \langle \{\underline{e_1}, \ldots, \underline{e_k}\} \rangle$ where $\underline{e_i} = (0, \ldots, 1, \ldots, 0)$ with 1 in the ith position.

Example 7.2.5. Let $G = \langle\{g_1, \dots, g_r\}\rangle$, so $G = \{g_1^{a_1} + \cdots + g_r^{a_r} : a_i \in \mathbb{Z}\}$. The there is a homomorphism $\phi : \mathbb{Z}^k \to G$, $\phi(a_1, \dots, a_k) := g_1^{a_1} + \cdots + g_r^{a_r}$.

Proposition 7.2.6. If G is finitely generated by $\{g_1, \dots, g_r\}$, then G is isomorphic to $\mathbb{Z}^r/K$ where

$$K = \ker(\phi) = \{\underline{a} \in \mathbb{Z}^r : g_1^{a_1} \cdots g_r^{a_r} = e_G\}$$

Proof. Omitted (use FIT). □

Definition 7.2.7. The group $K \leq \mathbb{Z}^r$ is called the **relation subgroup of** G. Every $\underline{a} \in K$ is called a **relation of** G.

Proposition 7.2.8. Let $H \leq \mathbb{Z}^r$. Then for some $0 \leq d \leq r$, $H \cong \mathbb{Z}^d$, with the isomorphism

$$(a_1, \dots, a_r) \to (b_1, \dots, b_d, 0, \dots, 0)$$

d is called the **(free) rank** of H.

Proof. Omitted. □

Example 7.2.9. Let $r = 1$ and $H \leq \mathbb{Z}$. Then $H = \{0\}$ or $H = m\mathbb{Z}$, $m \in \mathbb{N}$. $\{0\}$ is a rank 0 subgroup. $m\mathbb{Z}$ is a rank 1 subgroup and the isomorphism is $mk \to k$.

Example 7.2.10. By Proposition 7.2.8, $K \cong \mathbb{Z}^d$ with $0 \leq d \leq r$, since if $d = 0$, $K \cong \{0\}$ so $G \cong \mathbb{Z}^r$ and if $d = r$, $K \cong \mathbb{Z}^r$ so $G \cong \{0\}$. We have $K = \langle\{\underline{a_1}, \dots, \underline{a_d}\}\rangle$ and we must have

$$\lambda_1\underline{a_1} + \cdots + \lambda_d\underline{a_d} = 0 \Longleftrightarrow \lambda_1 = \cdots = \lambda_d = 0$$

The relation subgroup of K is $\{0\}$. By studying the associated matrix

$$A(K) = \begin{bmatrix} \underline{a_1} \\ \vdots \\ \underline{a_d} \end{bmatrix} = \begin{bmatrix} a_{1,1} & \cdots & a_{1,r} \\ \vdots & \ddots & \vdots \\ a_{d,1} & \cdots & a_{d,r} \end{bmatrix}$$

we can find a reduced form of $A(K)$ by Gaussian elimination:

$$A(K) \to \begin{bmatrix} \tilde{a}_{1,1} & 0 & 0 & \cdots & 0 \\ 0 & \tilde{a}_{2,2} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & \tilde{a}_{d,d} \end{bmatrix}$$

where $\tilde{a}_{i,i} \in \mathbb{Z}$. So we see that K can be generated by

$$\begin{aligned} &\tilde{a}_{1,1} \cdot (1, 0, \cdots 0) \\ &\tilde{a}_{2,2} \cdot (0, 1, \cdots 0) \\ &\cdots \\ &\tilde{a}_{d,d} \cdot (0, 0, \cdots 1, 0, \cdots 0) \end{aligned}$$

Writing $d_i = \tilde{a}_{i,i}$, gives the following theorem.

Theorem 7.2.11. (**Fundamental theorem of finitely generated Abelian groups**) Let G be a finitely generated Abelian group. Then for some integer $1 \leq r \leq k$ and $d_1, \dots, d_r \in \mathbb{N}^r$, with $d_1 \mid d_2$, $d_2 \mid d_3$, $\cdots$, $d_{r-1} \mid d_r$ such that

$$G \cong \mathbb{Z}^{k-r} \times \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_r$$

if $G = \langle\{g_1, \dots, g_k\}$.

Corollary 7.2.12. Let G be a finite Abelian group. Then for some $r \geq 1$ and $d_1, \ldots, d_r \in \mathbb{N}^r$, with $d_1 \mid d_2$, $d_2 \mid d_3$, $\cdots$, $d_{r-1} \mid d_r$,

$$G \cong \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_r$$

(The infinite part $\mathbb{Z}^{k-r}$). In this case, $|G| = n = d_1 \cdots d_r$.

Definition 7.2.13. The d_i above are called the **torsion coefficients**.

THIS COROLLARY AND THE FOLLOWING EXAMPLE WILL APPEAR IN THE EXAM

Example 7.2.14. Find all Abelian groups of order 32. By the above corollary, $G \cong \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_r$, where $d_1 \ldots d_r = 32$ and $d_1 \mid d_2$, $d_2 \mid d_3$, $\cdots$, $d_{r-1} \mid d_r$ and $d_i > 1$.

$32 = 2^5$ so $d_i \mid 2^5$ so $d_i = 2^{a_i}$ where $1 \leq a_i \leq 5$. Also $a_1 + \cdots + a_r = 5$ and $a_i \leq a_{i+1}$ since $d_i \mid d_{i+1}$. So $1 \leq r \leq 5$. The possible tuples $(a_1, \ldots, a_r)$ are

$$\begin{aligned} &(1,1,1,1,1)\\ &(1,1,1,2)\\ &(1,1,3)\\ &(1,4)\\ &(5) \end{aligned}$$

So all Abelian groups of order 32 are $(\mathbb{Z}/2)^5$, $(\mathbb{Z}/2) \times \mathbb{Z}/4$, etc.

Example 7.2.15. (Problems class) Let G be an Abelian group, with $|G| = 100$. Show that for some $x \in G$, $\mathrm{ord}_G(x) = 10$. What are the torsion coefficients of G if no element has order > 10?

We have some torsion coefficients $1 < d_1 \leq d_2 \leq \cdots \leq d_r$ with $d_1 \mid d_2$, $d_2 \mid d_3$, $\cdots$, $d_{r-1} \mid d_r$ such that

$$G \cong \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_r$$

$|G| = 2^2 \cdot 5^2$. The maximum multiplicity of these prime factors is 2, so $1 \leq r \leq 2$. We have $|G| = d_1 \cdots d_r = 100$ so $d_i = 2^{a_i} \cdot 5^{b_i}$, $a_i \leq a_{i+1}$, $b_i \leq b_{i+1}$. We look at partitions of 2 to get possible a_i and b_i.

$$2^{a_1+\cdots+a_r} \cdot 5^{b_1+\cdots+b_r} = d_1 \cdots d_r = 2^2 \cdot 5^2 \Longrightarrow a_1 + \cdots + a_r = 2, b_1 + \cdots + b_r = 2$$

So either $a_1 = 1$ and $a_2 = 1$ or $a_1 = 0$ and $a_2 = 2$. Similarly, $b_1 = 1$ and $a_2 = 1$ or $b_1 = 0$ and $b_2 = 2$. For $r = 1$, $d_1 = 100$ so $G = \mathbb{Z}/100$. For $r = 2$, we have the possibilities:

$$\begin{aligned} (a_1, b_1) = (1,1), (a_2, b_2) = (1,1) &\Longrightarrow d_1 = 2 \cdot 5 = 10, d_2 = 2 \cdot 5 = 10\\ (a_1, b_1) = (1,0), (a_2, b_2) = (1,2) &\Longrightarrow d_1 = 2^1 \cdot 5^0 = 2, d_2 = 2^1 \cdot 5^2 = 40\\ (a_1, b_1) = (0,1), (a_2, b_2) = (2,1) &\Longrightarrow d_1 = 2^0 \cdot 5^1 = 5, d_2 = 2^2 \cdot 5^1 = 20 \end{aligned}$$

so $G \cong \mathbb{Z}/100$, $G \cong \mathbb{Z}/2 \times \mathbb{Z}/50$, $G \cong \mathbb{Z}/5 \times \mathbb{Z}/20$ or $G \cong \mathbb{Z}/10 \times \mathbb{Z}/10$.

If $G \cong \mathbb{Z}/100$, then $x = 10$ has order 10. If $G \cong \mathbb{Z}/10 \times \mathbb{Z}/10$, then $x = (1,1)$ has order 10. If $G \cong \mathbb{Z}/2 \times \mathbb{Z}/50$, then $x = (0,5)$ has order 10. If $G \cong \mathbb{Z}/5 \times \mathbb{Z}/20$, then $x = (0,2)$ has order 10.

If no element has order > 10, then $G \cong \mathbb{Z}/10 \times \mathbb{Z}/10$, so $d_1 = d_2 = 10$.

Example 7.2.16. Let G be a finite Abelian group, such that $|G|$ is not divisible by a square (not equal to 1). Show that G is cyclic.

We want to show that if $G \cong \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_r$, with $1 < d_1 < \cdots < d_r$ and $d_1 \mid d_2, \ldots, d_i \mid d_{i+1}$ then $r = 1$.

Assume that opposite, that $r \geq 2$. We have $|G| = d_1 \cdots d_r$ and $d_1 \mid d_2$, $d_1 \mid d_3, \ldots, d_1 \mid d_r$. Hence $d_1^r \mid d_1 d_2 \cdots d_r$, so $d_1^r \mid |G|$. By assumption, $r \geq 2$, so $d_1^2 \mid d_1^r$ so $d_1^2 \mid |G|$. But $d_1 > 1$ so $d_1^2 > 1$ so $|G|$ is divisible by a square (not equal to 1) so we have a contradiction.

Hence $r \geq 1$, so G is cyclic.

Example 7.2.17. (Problems class) Let G be a finite group such that $\forall x \in G - \{e_G\}$, $\mathrm{ord}_G(x) = 2$. Then $G \cong (\mathbb{Z}/2)$ for some $k \geq 0$.

G only has elements of order 2, so if $xy \in G$, then $e_G = (xy)^2 = xyxy = xyx^{-1}y^{-1}$ since $x = x^{-1}$, $y = y^{-1}$, so G is Abelian. By the structure theorem for finite Abelian groups, for some $r \geq 1$, and $1 < d_1 \leq \cdots \leq d_r$, with $d_1 \mid d_2, \ldots, d_i \mid d_{i+1}$, $G \cong \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_r =: H$.

Suppose for the sake of contradiction that for some $1 \leq i \leq r$, $d_i \geq 3$. Let $y = (0, \ldots, 0, 1, 0 \ldots, 0)$ with 1 in the i position and let $x \in G$ correspond to y, so let $\phi : G \to H$ be an isomorphism, then $x = \phi^{-1}(y)$. So $\mathrm{ord}_G(x) = \mathrm{ord}_H(y) = d_i \geq 3$, but this is a contradiction.

Hence $d_1 = \cdots = d_r = 2$.

Example 7.2.18. (Problems class) Classify all Abelian groups of order 60 and 144.

$60 = 2^2 \cdot 3 \cdot 5$, so if $G \cong \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_r$, with $1 < d_1 < \cdots < d_r$ and $d_1 \mid d_2, \ldots, d_i \mid d_{i+1}$, $1 \leq r \leq 2$ as the highest multiplicity of a prime factor of 60 is 2. If $r = 1$, then $d_1 = 60$, so $G \cong \mathbb{Z}/60$.

If $r = 2$, then let $d_1 = 2^{a_i} \cdot 3^{b_i} \cdot 5^{c_i}$ so $(a_1, b_1, c_1) = (1, 0, 0)$ and $(a_2, b_2, c_2) = (1, 1, 1)$. So $d_1 = 2$ and $d_2 = 30$, so $G \cong \mathbb{Z}/2 \times \mathbb{Z}/30$.

$144 = 2^4 \cdot 3^2$ so $1 \leq r \leq 4$. Look at the partitions of the multiplicity of 2 (4 in this case).

$$
\begin{aligned}
&r = 1 : 4 \text{ for } a_i, 2 \text{ for } b_i \\
&r = 2 : 1 + 3, 2 + 2 \text{ for } a_i, 0 + 2, 1 + 1 \text{ for } b_i \\
&r = 3 : 1 + 1 + 2 \text{ for } a_i, 0 + 1 + 1, 0 + 0 + 2 \text{ for } b_i \\
&r = 4 : 1 + 1 + 1 + 1 \text{ for } a_i, 0 + 0 + 0 + 2, 0 + 0 + 1 + 1 \text{ for } b_i
\end{aligned}
$$

So G is isomorphic to $\mathbb{Z}/144$, $\mathbb{Z}/2 \times \mathbb{Z}/72$, $\mathbb{Z}/6 \times \mathbb{Z}/24$, $\mathbb{Z}/4 \times \mathbb{Z}/36$, $\mathbb{Z}/3 \times \mathbb{Z}/48$, $\mathbb{Z}/12 \times \mathbb{Z}/12$, $\mathbb{Z}/2 \times \mathbb{Z}/6 \times \mathbb{Z}/12$, $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/36$, $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/18$, or $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/6 \times \mathbb{Z}/6$.