Higher Algebra

Jeremy Le — UNSW MATH3711 25T1

Contents

Part I
Group Theory

1 The Mathematical Language of Symmetry

Definition 1.1 (Isometry)**.** A function $f : \mathbb{R}^n \to \mathbb{R}^n$ is an isometry if $\|f(x) - f(y)\| = \|x - y\|$ for all $x, y \in \mathbb{R}^n$. i.e. preserves distances.

Definition 1.2 (Symmetry)**.** Let $F \subseteq \mathbb{R}^n$, a symmetry of F is a (surjective) isometry $T : \mathbb{R}^n \to \mathbb{R}^n$ such that $T(F) = F$.

Properties 1.3. Let S, T be symmetries of $F \subseteq \mathbb{R}^n$. Then $S \cdot T : \mathbb{R}^n \to \mathbb{R}^n$ is also a symmetry of F.

Proof. Given $x, y \in \mathbb{R}^n$.

$$\begin{aligned} \|STx - STy\| &= \|Tx - Ty\| && (S \text{ is an isometry}) \\ &= \|x - y\|. && (T \text{ is an isometry}) \end{aligned}$$

Therefore ST is an isometry. Clearly ST is surjective as both S and T are surjective. Also,

$$\begin{aligned} ST(F) &= S(F) && (T(F) = F) \\ &= F. && (S(F) = F) \end{aligned}$$

So ST is a symmetry of F.

Properties 1.4. If G = set of symmetries of $F \subseteq \mathbb{R}^n$, then G satisfies:

i) Composition is associative, $ST(R) = S(TR)$ for all $S, T, R \in G$.

ii) $\mathrm{id}_{\mathbb{R}^n} \in G \quad (\mathrm{id}_{\mathbb{R}^n}(x) = x \quad \text{for all } x \in \mathbb{R}^n)$. Also, $\mathrm{id}_G T = T$ and $T \,\mathrm{id}_G = T$ for all $T \in G$.

iii) If $T \in G$, then T is bijective and $T^{-1} \in G$.

Proof. If $Tx = Ty$, then $\|Tx - Ty\| = 0$. So $\|x - y\| = 0, x = y$, therefore T is injective. By definition T is surjective, hence, T is bijective and therefore T^{-1} is surjective.

To prove T^{-1} is an isometry.

$$\begin{aligned} \left\|T^{-1}x - T^{-1}y\right\| &= \left\|TT^{-1}x - TT^{-1}y\right\| \\ &= \|\mathrm{id}\, x - \mathrm{id}\, y\| \\ &= \|x - y\|. \end{aligned}$$

To prove symmetry, $T^{-1}F = F$:

$$T^{-1}F = T^{-1}(T(F)) = F.$$

Thus $T^{-1} \in G$.

Definition 1.5 (Group)**.** A group is a set G equipped with a "multiplication map" $\mu : G \times G \to G$ such that

1) Associativity: $(gh)k = g(hk)$ for all $g, h, j \in G$.

2) Existence of identity: There exists $1 \in G$ such that $1g = g$ and $g1 = g$ for all $g \in G$.

3) Existence of inverses: $\forall g \in G,$ there exists $h \in G$ such that $gh = 1$ and $hg = 1$. Denoted by g^{-1}.

Properties 1.6. Basic facts about groups.

- "**Generalised Associativity**". When multiplying three or more elements, the bracketing does not matter. E.g. $(a(b(cd)))e = (ab)(c(de))$.

  Proof. Mathematical Induction as for matrix multiplication.

- **Cancellation Law**. If $gh = gk$ then $h = k$ for all $g, h, k \in G$.

  Proof. $gh = gk \implies g^{-1}(gh) = g^{-1}(gk) \implies (g^{-1}g)h = (g^{-1}g)k \implies 1h = 1k \implies h = k.$

2 Matrix Groups and Subgroups

Recall $\mathrm{GL}_n(\mathbb{R})$ and $GL_n(\mathbb{C})$ which represent the set of real/complex invertible $n \times n$ matrices.

Proposition 2.1. $\mathrm{GL}_n(\mathbb{R})$ and $GL_n(\mathbb{C})$ are groups when endowed with matrix multiplication.

Proof. Product of real invertible matrices is in $\mathrm{GL}_n(\mathbb{R})$.

i) matrix multiplication is associative.

ii) identity matrix $I_n : I_n m = m$ and $mI_n = m$ for all $m \in \mathrm{GL}_n(\mathbb{R})$

iii) if $m \in \mathrm{GL}_n(\mathbb{R})$ then m^{-1}. $mm^{-1} = I$ and $m^{-1}m = I$.

Proposition 2.2. Let G = group.

1) Identity is unique i.e. suppose $1, e$ are both identities then $1 = e$.

   Proof. $1 = 1 \cdot e = e$.

2) Inverses are unique.

   Proof. If $g \in G, gh = hg = 1$ and $gk = kg = 1$ then $h = k$.

3) For $g, h \in G$ we have $(gh)^{-1} = h^{-1}g^{-1}$.

   Proof. $(gh)(h^{-1}g^{-1}) = ghh^{-1}g^{-1} = g1g^{-1} = gg^{-1} = 1$. Similarly, $(h^{-1}g^{-1}(gh) = 1)$.

Definition 2.3 (Subgroup)**.** Let G be a group with multiplication μ. A subset $H \subseteq G$ is called a subgroup of G (denoted $H \leq G$) if it satisfies:

i) $1_G \in H$ (contains identity),

ii) if $g, h \in H$ then $gh \in H$ (closed under multiplication),

iii) if $g \in H$ then $g^{-1} \in H$ (closed under inverse).

Proposition 2.4. H is a group with the induced multiplication map $\mu_H : H \times H \to H$ by $\mu_H(g, h) = \mu(g, h)$.

Proof. (ii) tells us that μ_H makes sense. μ_H is associative because μ is. H has an identity from (i). H has inverses from (iii).

Proposition 2.5. Set of orthogonal matrices $O_n(\mathbb{R}) = \{M \in \mathrm{GL}_n(\mathbb{R}) : M^T = M^{-1}\} \leq \mathrm{GL}_n(\mathbb{R})$ forms a group. Namely the set of symmetries of an $n-1$ sphere, i.e. an n dimensional circle.

Proof. Check axioms.

i) $I_n \in O_n(\mathbb{R})$

ii) If $M, N \in O_n(\mathbb{R})$ then $(MN)^T = N^T M^T = N^{-1}M^{-1} = (MN)^{-1}$, so $MN \in O_n(\mathbb{R})$.

iii) If $M \in O_n(\mathbb{R})$ then $(M^{-1})^T = (M^T)^{-1} = (M^{-1})^{-1}$ so $M^{-1} \in O_n(\mathbb{R})$.

Proposition 2.6. Basic subgroup facts.

i) Any group G has two trivial subgroups: itself and $1 = \{1_G\}$.

ii) If $J \leq H$ and $H \leq G$ then $J \leq G$.

Here are some notations. For $g \in G$ where G is a group.

i) If n positive integer, define $g^n = g \cdot g \cdots g$ (n times)

ii) $g^0 = 1$

iii) n positive: $g^{-n} = (g^{-1})^n$ or $(g^n)^{-1}$.

iv) For $m, n \in \mathbb{Z}$, $g^m \cdot g^n = g^{m+n}$ and $(g^m)^n = g^{mn}$.

Definition 2.7. The order of a group G, denoted $|G|$ is the cardinality of G. For $g \in G$, the order of g is the smallest positive integer n such that $g^n = 1$. If no such integer exists, order is ∞.

3 Permutation Groups

Definition 3.1 (Permutations)**.** Let S be a set. Let $\mathrm{Perm}(S)$ be the set of permutations of S. This is the set of bijections of form $\sigma : S \to S$.

Proposition 3.2. $\mathrm{Perm}(S)$ is a group when endowed with composition of functions.

Proof. Composition of bijections is a bijection. The identity is id_S and group inverse is the inverse function.

Definition 3.3 (Symmetric Group)**.** Let $S = \{1, \ldots, n\}$. The symmetric group S_n is $\mathrm{Perm}(S)$.

Two notations are used. With the two line notation, represent $\sigma \in S_n$ by

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

($\sigma(i)$'s are all distinct, hence σ is one to one and bijective). Note this shows $|S_n| = n!$.

With the cyclic notation, let $s_1, s_2, \ldots, s_k \in S$ be distinct. We define a new permutation $\sigma \in \mathrm{Perm}(S)$ by $\sigma(s_i) = s_{i+1}$ for $i = 1, 2, \ldots, k-1, \sigma(s_k) = \sigma(s_1)$ and $\sigma(s) = s$ for $s \notin \{s_1, s_2, \ldots, s_k\}$. Denoted $(s_1 s_2 \ldots s_k)$ and called a k-cycle.

Example 3.4. For $n = 4$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \in S_4 \quad \text{means} \quad \begin{matrix} \sigma(1) = 2, & \sigma(2) = 3 \\ \sigma(3) = 1, & \sigma(4) = 4. \end{matrix}$$

In cyclic notation this is $(123)(4)$ or (123) where the cycle is $1 \to 2 \to 3 \to 1$.

Note that a 1-cycle is the identity and the order of a k-cycle is k. So $\sigma^k = 1$ and $\sigma^{-1} = \sigma^{k-1}$.

Definition 3.5 (Disjoint Cycles)**.** Cycles $s_1 \ldots s_k$ and $t_1 \ldots t_k$ are disjoint if $\{s_1, \ldots, s_k\} \cup \{t_1, \ldots, t_k\} = \emptyset$.

Definition 3.6 (Commuativity)**.** In any group, two elements g, h commute if $gh = hg$.

Proposition 3.7. Disjoint cycles commute.

Proposition 3.8. Any permutation σ of a finite set S is a product of disjoint cycles.

Example 3.9. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 5 & 3 \end{pmatrix} \in S_6$ does $1 \to 2 \to 4 \to 1$, $3 \to 6 \to 3$ and $5 \to 5$.
Thus $\sigma = (124)(36)$ since (5) is the identity.

Proposition 3.10. Let σ be a permutation of a finite set S. Then S is a disjoint union of subsets, say $S_1, \ldots, S_r$, such that σ permutes the elements of each S_i cyclically.

Definition 3.11 (Transposition)**.** A transposition is a $2-$cycle i.e. (ab).

Proposition 3.12. i) The k-cycle $(s_1 s_2 \ldots s_k) = (s_1 s_k)(s_1 s_{k-1}) \ldots (s_1 s_3)(s_1 s_2)$

Example 3.13. $(3625) = (35)(32)(36) = (36)(62)(25)$

Proof. The RHS produces the mapping below which is equivalent to the LHS.

$$\begin{aligned} s_1 &\to s_2 \\ s_2 &\to s_1 \to s_3 \\ s_3 &\to s_1 \to s_4 \\ &\vdots \\ s_{k-1} &\to s_1 \to s_k \\ s_k &\to s_1. \end{aligned}$$

ii) Any permutations in S_n is a product of transpositions.

Proof. We can write any $\sigma \in S_n$ as product of (disjoint) cycles. By part i), each cycle is a product of transpositions. So we can write σ as product of transpositions.

4 Generators and Dihedral Groups

Lemma 4.1. Let $\{H_i\}_{i\in I}$ be a (non-empty) collection of subgroups of G. Then $\bigcap_{i\in I} H_i \leq G$.

Proof.

1) Why is $1 \in \bigcap_{i\in I} H_i$? Because $1 \in H_i$ for all i.

2) Closed under multiplication? If $g, h \in \bigcap_{i\in I} H_i$, then $g, h \in H_i$ for all $i \implies gh \in H_i$ for all $i \implies gh \in_{i\in I} H_i$.

3) Closed under taking inverse? If $g \in \bigcap_{i\in I} H_i$ then $g \in H_i$ for all i as H_i are subgroups, every element has an inverse. So an inverse exists for all elements in H_i for all i.

Proposition - Definition 4.2. Let G be a group and $S \subseteq G$. Let $\mathcal{J}$ be the set of subgroups $J \leq G$ containing S.

i) [Definition] The subgroup generated by S, $\langle S \rangle$ is $\bigcap J \in \mathcal{J} \leq J \leq G$. i.e. it's the intersection of all subgroups of G containing S.

Proof. Lemma 4.1 implies $\langle S \rangle$ is a subgroup of G.

ii) [Proposition] $\langle S \rangle$ is the set of elements of the form $g = s_1 s_2 \dots s_n$ where $n \geq 0$ and $s_i \in S \cup S^{-1}$. Define $g = 1$ when $n = 0$.

Proof. Let $H = \{s_1 \dots s_n : s_i \in S \cup S^{-1}\}$. First, $H \subseteq \langle S \rangle$. Need to prove that $s_i \cdots s_n \in$ every J. Each $s_i \in J$ because $s_i = s$ or s^{-1} for some $s \in S \leq J$ and J closed under inversion. Therefore, $s_1 \dots s_n \in J$ by closure under multiplication. Hence $s_1 \dots s_n \in \bigcap_{J\in\mathcal{J}} J = \langle S \rangle$.

Second, $\langle S \rangle \subseteq H$. Need to prove H is a subgroup containing S. Closure under multiplication: $(s_1 \dots s_n)(t_1 \dots t_m) = s_1 \dots s_n t_1 \dots t_m$ also closure under inversion: $(s_1 \dots s_n)^{-1} = s_1^{-1} \dots s_n^{-1} \in H$ since $s_i^{-1} \in S$ for all i. Identity: $s, s^{-1} \in S \neq \emptyset \implies ss^{-1} = 1 \in H$.

Definition 4.3 (Finitely Generated)**.** A group G is finitely generated $f.g.$ if $G = \langle S \rangle$ for a finite subset $S \subseteq G$. G is cyclie if we can take $|S| = 1$.

Example 4.4. Take $G \in \mathrm{GL}_2(\mathbb{R})$ with $\sigma = \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & -\cos\left(\frac{2\pi}{n}\right) \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Find the subgroup generated by $\{\sigma, \tau\}$.

Notice both σ, τ are symmetries of any n-gon. Any element of $\langle \sigma, \tau \rangle$ has form

$$\sigma^{i_1}\tau^{j_1}\sigma^{i_2}\tau^{j_2} \dots \sigma^{i_r}\tau^{j_r} \quad \text{for } i_1, \dots, i_r, j_1, \dots, j_r \in \mathbb{Z}.$$

We have relations: $\sigma^n = 1, \tau^2 = 1$ and $\tau\sigma\tau^{-1} = \sigma^{-1}$. We use these relations to push all σ's to the left and all τ's to the right to achieve the form $\sigma^i \tau^j$ where $0 \leq i < n$ and $j = 0, 1$.

Proposition - Definition 4.5. $\langle \sigma, \tau \rangle$ = dihedral group of $2n$, denoted D_n (sometimes D_{2n}).

$$D_n = \{1, \sigma, \dots, \sigma^{n-1}, \tau, \sigma\tau, \sigma^2\tau, \dots, \sigma^{n-1}\tau\} \text{ and } |D_n| = 2n.$$

Proof. Need to show $2n$ elements are all distinct. $\det(\sigma^i) = 1$ (because $\det(\sigma) = 1$), $\det(\tau) = -1$ and $\det(\sigma^i\tau) = -1$. We conclude, $\{1, \sigma, \dots, \sigma^{n-1}\} \cap \{\tau, \sigma\tau, \dots, \sigma^{n-1}\tau\} = \emptyset$ because $\sigma^k = \begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) & -\sin\left(\frac{2k\pi}{n}\right) \\ \sin\left(\frac{2k\pi}{n}\right) & \cos\left(\frac{2k\pi}{n}\right) \end{pmatrix}$ are distinct. If $\sigma^i\tau = \sigma^j\tau$ then $\sigma^i = \sigma^j$ then $i = j$.

5 Alternating and Abelian Groups

Definition 5.1 (Symmetric Functions)**.** Let $f(x_1, \dots, x_n)$ be a function of n variables. Let $\sigma \in S_n$. We define function $(\sigma f)(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$. We say that f is symmetric if $\sigma f = f$ for all $\sigma \in S_n$.

Example 5.2. Suppose $f(x_1, x_2, x_3) = x_1^3 x_2^2 x_3$ and $\sigma = (12)$ then $\sigma f(x_1, x_2, x_3) = x_2^3, x_1^2 x_3$. Not symmetric because $x_1^3 x_2^2 x_3 \neq x_2^3 x_1^2 x_3$. But $f(x_1, x_2) = x_1^2 x_2^2$ is symmetric in two variables.

Definition 5.3 (Difference Product)**.** The difference product in (n variables) is

$$\Delta(x_1, \dots, x_n) = \Pi_{i<j}(x_i - x_j).$$

Lemma 5.4. Let $f(x_1, \dots, x_n)$ be a function in n variables. Let $\sigma, \tau \in S_n$, then $(\sigma\tau) \cdot f = \sigma \cdot (\tau f)$.

Proof.

$$\begin{aligned}
(\sigma \cdot (\tau f))(x_1, \dots, x_n) &= (\tau f)(x_{\sigma(1)}, \dots, x_{\sigma(n)}) && \text{(by definition)} \\
&= f(y_{\tau(1)}, \dots, y_{\tau(n)}) && \text{(where } y_i = x_\sigma(i)) \\
&= f(x_{\sigma(\tau(1))}, \dots, x_{\sigma(\tau(n))}) \\
&= f(x_{(\sigma\tau)(1)}, \dots, x_{(\sigma\tau)(n)}) \\
&= ((\sigma\tau) \cdot f)(x_1, \dots, x_n).
\end{aligned}$$

Note, the second and third step follows because $x_{\sigma(1)}$ is not necessarily x_1, so τ is applied to x_1 first, then σ can be applied.

Proposition - Definition 5.5. For $\sigma \in S_n$ write $\sigma = \tau_1\tau_2 \dots \tau_m$ where τ_i are transpositions. Then

$$\sigma \cdot \Delta = \begin{cases} \Delta & \text{if } m \text{ even (call } \sigma \text{ an even permutation)} \\ -\Delta & \text{if } m \text{ odd (call } \sigma \text{ an odd permutation)} \end{cases}$$

Proof. Sufficent to prove for a single transposition (i.e. $m = 1$) because by the above Lemma,

$$\sigma\Delta = \tau_1(\tau_2 \dots (\tau_{m-1}(\tau_m\Delta)) \dots) = \tau_1((-1)^{m-1}\Delta) = (-1)^m\Delta.$$

Let's assume $\sigma = (ij), i < j$. There are 3 cases:

i) $x_i - x_j \implies x_j - x_i$ (factor of -1).

ii) $x_r - x_s$ where i, j, r, s all distinct $\implies x_r - x_s$ (factor of +1).

iii) $x_r - x_s$ where one of r, s is equal to i or j. There are several subcases:

(a) $r < i < j$: $x_r - x_i \implies x_r - x_j$ but also $x_r - x_j \implies x_r - x_i$, no change (factor of $+1$).

(b) $i < r < j$: $(x_i - x_r)(x_r - x_j) \implies (x_j - x_r)(x_r - x_i)$ (factor of $+1$).

(c) $i < j < r$: similar to (a) (factor of $+1$).

So only change in i). Multiplying the three cases together yields $\sigma \cdot \Delta = -\Delta$.

Corollary - Definition 5.6 (Alternating Group)**.** The alternating group (on n symbols) is

$$A_n = \{\sigma \in S_n : \sigma \text{ is even}\}.$$

This is a subgroup of S_n. Also A_n is generated by $\{\tau_1\tau_2 : \tau_1, \tau_2 \text{ are transposition}\}$.

Example 5.7. $A_3 = \{1, (123), (132)\}, S_3 \setminus A_3 = \{(12), (13), (23)\}.|A_n| = n!/2$ except for $n = 1, A_1 = S_1 = \{1\}$.

Definition 5.8 (Abelian Group)**.** A group G is abelian if any two elements commute.

In abelian groups, often switch to additive notation:

i) product $gh \implies g + h$

ii) identity $1 \implies 0$

iii) power $g^n \implies ng$

iv) inverse $g^-1 \implies -g$

This notation follows from $\mathbb{Z}$ endowed with addition which forms an abelian group.

6 Cosets and Lagrange's Theorem

Let $H \leq G$ be a subgroup. This will apply to all statements in this section unless mentioned otherwise.

Definition 6.1 (Coset)**.** A left coset of H in G is a set of the form $gH = \{gh : h \in H\} \subseteq G$ for some $g \in G$. The set of left cosets is denoted byt G/H.

Example 6.2. Let $H = A_n \leq S_n = G$ for $n \geq 2$. Let τ be any transposition. We claim that $\tau A_n = \{\text{odd permutations}\}$.

$\subseteq$: $\tau A_n = \{\tau\sigma : \sigma \text{ even}\}$, they are all odd.

$\supseteq$: Suppose σ is odd, then $\sigma = \tau \cdot (\tau^{-1}\sigma) \in \tau A_n$.

Theorem 6.3. Define a relation on $G : g \equiv g'$ if and only if $g \in g'H$. Then $\equiv$ is an equivalence relation, the equivalence classes are the left cosets. Therefore $G = \dot{\bigcup}_{i \in I} g_i H$ (disjoint union).

Proof.

i) Reflexive. i.e. $g \in gH$ for all $g \in G$. True because $1 \in H$.

ii) Symmetry. Suppose $g \in g'H$, need to prove $g' \in gH$. Since $g \in g'H$ we have $g = g'H$ for some $h \in H$. $g' = gh^{-1}$ so $g' \in gH$ (as $h^{-1} \in H$).

iii) Transitivity. Suppose $g \in g'H$ and $g' \in g''H$. Then $g = g'h$ and $g' = g''h'$ for $h, h' \in H$. Therefore $g = (g''h)h = g''(h'h) \in g''H$ from associativity and $h'h \in H$.

Thus $\equiv$ is an equivalence relation and G is a disjoint union of equivalence classes.

Note $1H = H$ is always a coset of G and the coset containing $g \in G$ is gH.

Example 6.4. $H = A_n \leq S_n = G$ cosets are exactly S_n and τS_n where $S_n = A_n \dot{\bigcup} \tau A_n$.

Definition 6.5 (Index)**.** The index of H in G is the number of left cosets, i.e. $|G/H|$. Denoted by $[G : H]$.

Lemma 6.6. Let $g \in G$. Then H and gH have the same cardinality.

Proof. Bijection, $H \to gH, h \mapsto gh$. Surjective and injective (multiply on lefy by g^{-1}).

Theorem 6.7 (Lagrange's Theorem)**.** Assume G finite. Then $|G| = |H|[G : H]$ i.e. $|G/H| = |G|/|H|$.

Proof. Using Lemma 6.6, we have:

$$G = \bigcup_{i=1}^{[G:H]} g_i H \quad \text{(disjoint union)} \implies |G| = \sum_{i=1}^{[G:H]} |g_i H| = \sum_{i=1}^{[G:H]} |H| = [G : H]|H|.$$

Example 6.8. $A_n \leq S_n$. $[S_n : A_n] = 2 \implies |S_n| = 2|A_n| \implies n! = 2 * n!/2$.

All above statements hold for right cosets which have form $Hg = \{hg : h \in H\}$ denoted $H\backslash G$. The number of left cosets are equal the number of right cosets.

7 Normal Subgroups and Quotient Groups

Let $G =$ group and $J, K \subseteq G$. Define the subset product $JK = \{jk : j \in J, k \in K\}$.

Proposition 7.1. Let $G =$ group.

i) If $J' \subseteq J \subseteq G$ and $K \subseteq G$ then $KJ' \subseteq KJ$.

ii) If $H \leq G$, then $HH = H(= H^2)$.

iii) For $J, K, L \subseteq G$ then $(JK)L = J(KL) = \{jkl : j \in J, k \in K, \ell \in L\}$

Proposition - Definition 7.2 (Normal Subgroup)**.** Let $N \leq G$. We say N is a normal subgroup of G and write $N \trianglelefteq G$ if any of the following equivalent conditions hold:

i) $gN = Ng$ for all $g \in G$.

ii) $g^{-1}Ng = N$ for all $g \in G$.

iii) $g^{-1}Ng \subseteq N$ for all $g \in G$

Proof. (i) $\iff$ (ii), multiply both sides on the left by g^{-1}. (ii) $\implies$ (iii) by definition. (iii) $\implies$ (ii), assume $g^{-1}Ng \subseteq N$ for all $g \in G$, apply this with $g^{-1} : (g^{-1})Ng^{-1} \subseteq N \implies N \subseteq g^{-1}Ng$. Therefore $g^{-1}Ng = N$.

Theorem - Definition 7.3 (Quotient Group)**.** Let $N \trianglelefteq G$. Then subset product is a well-defined multiplication map on G/N which makes G/N into a group, called the quotient group. Also:

i) $(gN)(g'N) = (gg')N$

ii) $1_{G/N} = N$

iii) $(gN)^{-1} = g^{-1}N$.

Proof. Why is this well-defined? Why is the product of 2 cosets another coset?

Take cosets $gN = \{g\}N$ and $g'N$. Calculate

$$\begin{aligned}(gN)(g'N) &= g(Ng')N && \text{(associative)}\\ &= g(g'N)N && (N \trianglelefteq G)\\ &= (gg')(NN) && \text{(associative)}\\ &= gg'N && (N^2 = N)\end{aligned}$$

This is a coset. Also proves (i). For (ii), $(gN)N = g(NN) = gN \implies N(gN) = (Ng)N = (gN)N = gN$, N is an identity. For (iii), $(g^{-1}N)(gN) = g^{-1}(Ng)N = g^{-1}(gN)N = (g^{-1}g)(NN) = 1 \cdot N = N$.

8 Group Homomorphisms

Definition 8.1 (Homomorphism)**.** Given groups G, H. A function $\phi : H \to G$ is a homomorphism of groups if $\phi(hh') = \phi(h)\phi(h')$ for all $h, h' \in H$.

Proposition - Definition 8.2 (Isomorphisms and Automorphisms)**.** Let $\phi : H \to G$ be a group homomorphism. The following are equivalent:

- There exists a group homomorphism, $\psi : G \to H$ such that $\psi\phi = \mathrm{id}_H$ and $\phi\psi = \mathrm{id}_G$
- ϕ is bijective.

We call ϕ is a group isomorphism. If $H = G$, ϕ is an automorphism.

Proposition 8.3. If $\phi : H \to G, \psi : K \to H$ are group homomorphism then $\phi \cdot \psi : K \to G$ is a homomorphism.

Proof. $(\phi \cdot \psi)(kk') = \phi(\psi(kk')) = \phi(\psi(k)\psi(k')) = \phi(\psi(k))\phi(\psi(k'))$

Proposition 8.4. Let $\phi : H \to G$ be a group homomorphism.

i) $\phi(1_H) = 1_G$.

ii) $\phi(h^{-1}) = \phi(h)^{-1}$ for all $h \in H$.

iii) if $H' \leq H$ then $\phi(H') \leq G$.

Proposition - Definition 8.5. Let G be a group with $g \in G$. Conjugation by g is the map $C_g : G \to G; h \mapsto ghg^{-1}$. Then C_g is an automorphism with inverse $C_{g^{-1}}$.

Proof. C_g is a homomorphism: $C_g(h_1h_2) = C_g(h_1)C_g(h_2)$. Check: $C_g(h_1h_2) = gh_1h_2g^{-1} = gh_1g^{-1}gh_2g^{-1} = C_g(h_1)C_g(h_2)$. Now check $C_{g^{-1}}$ is an inverse. $C_{g^{-1}}(C_g(h)) = C_{g^{-1}}(ghg^{-1}) = g^{-1}ghg^{-1}g = h$. Similarly $C_g(C_{g^{-1}})(h) = h$, therefore $(C_g)^{-1} = C_{g^{-1}}$.

Corollary - Definition 8.6. For $H \leq G$, a conjugate of H (in G) is a subgroup of G of the form $gHg^{-1} := c_g(H)$.

Definition 8.7 (Epimorphism and Monomorphism)**.** Let $\phi : H \to G$ be a group homomorphism. ϕ is an epimorphism if ϕ is surjective. ϕ is a monomorphism if ϕ is injective.

Example 8.8. Linear map $T : V \to W$ where V and W are vector spaces. Suppose T is a projection onto some subspace. What does $T^{-1}(w) = \{v \in V : T(v) = w\}$ looks like, for a given $w \in W$?

If $w \in L$, $T^{-1}(w) = \emptyset$
If $w \in L, T^{-1}(w) =$ plane containing w, orthogonal to $L = w + K$ where $K =$ kernel of $T = T^{-1}(0)$.

Definition 8.9. Let $\phi : H \to G$ be a group homomorphism. The kernel of ϕ is

$$\ker \phi = \phi^{-1}(1_G) = \{h \in H : \phi(h) = 1_G\}$$

Proposition 8.10. Let $\phi : H \to G$ be a group homomorphism.

i) If $G' \leq G$ then $\phi^{-1}(G') \leq H$.

ii) If $G' \trianglelefteq G$ then $\phi^{-1}(G') \trianglelefteq H$.

Proof. (Normality) Given $h \in \phi^{-1}(G')$ and$g \in H$. We need to prove $ghg^{-1} \in \phi^{-1}(G') \implies \phi(ghg^{-1}) \in G \implies \phi(g)\phi(h)\phi(g)^{-1} \in G$ true because $\phi(h) \in G'$ and $G' \trianglelefteq G$.

iii) $K = \ker \phi \trianglelefteq H$.

Proof. Follows from (ii) because $K = \phi^{-1}(\{1\})$ and $\{1\} \trianglelefteq G$.

iv) The non-empty fibres of ϕ, i.e. $\phi^{-1}(g)$ for all $g \in G$, are exactly the cosets of H.

Proof. Suppose $g \in G$, consider $\phi^{-1}(g)$. Assume $\phi^{-1}(g) \neq \phi$. Let $h \in \phi^{-1}(g)$.

Claim. $\phi^{-1}(g) = hK$.
Proof. $hK \subseteq \phi^{-1}(g)$ because $\phi(hK) = \phi(h)\phi(j) = g \cdot 1 = g$.
Converse: $\phi^{-1}(g) \subseteq hK$. Let $h' \in \phi^{-1}(g)$. Then $\phi(h') = g$, also $\phi(h) = g$. Therefore $\phi(h'h^{-1}) = \phi(gg^{-1}) = \phi(1) = 1$. So $h'h^{-1} \in K, h' \in Kh = hK$, thus $\phi^{-1}(g) = hK$.

v) ϕ is one to one if and only if $K = \{1\}$.

Proof. ($\implies$) trivial. ($\impliedby$) Assume $K = \{1\}$. By part (iv) fibres $\phi^{-1}(g)$ are cosets of $\{1\}$ hence contain single element.

Proposition - Definition 8.11. Let $N \trianglelefteq G$. The quotient monomorphism (of G by N) is the map $\pi : G \to G/N; g \mapsto gN$. Its an epimorphism with kernel N.

9 First Group Isomorphism Theorem

Theorem 9.1. Let $N \trianglelefteq G$ and $\pi : G \to G/N$ be quotient map. Suppose $\phi : G \to H$ is a homomorphism such that $N \leq \ker \phi$.

i) If $g, g' \in G$ lie in the same coset of N, i.e. $gN = g'N$, then $\phi(g) = \phi(g')$.

ii) The map $\psi : G/N \to H; gN \mapsto \phi(g)$ is a homomorphism (the induced homomorphism).

iii) ψ is the unique homomorphism $G/N \to H$ such that $\phi = \psi \circ \pi$.

iv) $\ker \psi = (\ker \phi)/N = \{gN : g \in \ker \phi\}$.

Lemma 9.2 (Universal Property of Quotient Morphism)**.** If $N \trianglelefteq \mathbb{Z}$ then $N = m\mathbb{Z}$ for some $m \in \mathbb{N}$.

Proof. If $N = 0 (= \{0\})$ then can take $m = 0$. Suppose $N \neq 0$. Must contain at least one nonzero element. Take $m =$ smallest positive element in N. $m\mathbb{Z} \subseteq N$ easy. $N \subseteq m\mathbb{Z}$. Let $n \in N$, we write $n = mq + r$ where $0 \leq r < m$. We know $n \in N, mq \in N$. Therefore $r = n - mq \in N$ but $r < m \implies r = 0$. Thus, $n = mq \in m\mathbb{Z}$.

Proposition 9.3. Let $H = \langle h \rangle$ be a cyclic group. Then there exists an isomorphism: $\phi : \mathbb{Z}/m\mathbb{Z} \to H$ where m is the order of $h$if this is finite and 0 if h has infinite order.

Proof. Define $\phi : \mathbb{Z} \to H; i \mapsto h^i$. ϕ is an epimorphism (because $h^{i+j} = h^i \cdot h^j and H = \langle h \rangle$ gives surjective.) Let $N = \ker \phi$. By lemma, $N = m\mathbb{Z}$ for some $m \geq 0$. Apply Universal Property Theorem, gives $\psi : \mathbb{Z}/m\mathbb{Z} \to H$. ψ surjective because ϕ is surjective. Injective if $i + m\mathbb{Z} \in \ker \psi$, then $\phi(i) = 1 \in H$ so $i \in \ker \phi = N = m\mathbb{Z}$. So $H \cong \mathbb{Z}/m\mathbb{Z}$. Check m gives correct order.

Theorem 9.4 (First isomorphism Theorem)**.** Let $\phi : G \to H$ be a homomorphism. The isomorphism π given by $G \to H$ induces $G/\ker \phi \to H$ (by Universal Property) induces $G/\ker \phi \to \operatorname{Im} \phi$.

10 Second and Third Isomorphism Theorems

Proposition 10.1 (Subgroups of Quotient Groups)**.** Let $N \trianglelefteq G$ and $\pi : G \to G/N$ be the quotient map.

i) If $N \leq H \leq G$ then $N \trianglelefteq H$.

ii) There is a bijection between subgroups $H \leq G$ that contain N and subgroups $\bar{H} \leq G/N$. $H \mapsto \pi(H) = \{nH : h \in H\} = H/N$ and $\bar{H} \leftarrow\!\shortmid \pi^{-1}(\bar{H})$.

Proof. Images and image images of subgroups are subgroups. If $\bar{H} \leq G/N$, then $\pi^{-1}(\bar{H})$ contains N (because $1_{G/N} \in \bar{H}$). Surjective: $\pi(\pi^{-1}(\bar{H})) = \bar{H}$ because π surjective. Injective: If $\pi(H_1) = \pi(H_2)$ then $H_1 = H_2$. This follows from $H_1 = \cup_{g \in H_1} gN$ (disjoint union of cosets).

iii) Normal subgroups correspond i.e. $H \trianglelefteq G$ iff $\bar{H} \trianglelefteq G/N$.

Theorem 10.2 (Second Isomorphism Theorem)**.** Suppose $N \trianglelefteq G$ and $N \leq H \trianglelefteq G$. Then $\frac{G/N}{H/N} \cong G/H$.

Proof. Since $\pi_N, \pi_{H/N}$ are both onto, $\phi = \pi_{H/N} \circ \pi_N$ is also onto. $\ker(\phi) = \{g \in G : \pi_N(g) \in \ker(\pi_{H/N} : G/N \to \frac{G/N}{H/N}\} = \{g \in G : \pi_N(g) \in H/N\} = \pi^{-1}(H/N) = H$ by Proposition 10.1. First

Isomorphism Theorem says $G/\ker(\phi) \cong \mathrm{Im}(\phi) \implies G/N \cong \frac{G/N}{H/N}$ which proves the theorem.

Theorem 10.3. Suppose $H \leq G, N \trianglelefteq G$. Then

i) $H \cap N \trianglelefteq H$, $HN \leq G$.

ii) $\frac{H}{H \cap N} \cong \frac{HN}{N}$.

11 Products of Groups

Recall given groups $G_1, \ldots, G_n$, the set $G_1 \times G_2 \times \ldots G_n = \{(g_1, \ldots, g_n) : g_1 \in G_1, \ldots g_n \in G_n\}$. More generally if $G_i, i \in I$ are groups then $\prod_{i \in I} G_i = \{(g_i)_{i \in I} : g_i \in G_i\}$.

Proposition - Definition 11.1 (Product)**.** The set $\prod_{i \in I} G_i$ is called the (direct) product of the G_i's, it is a group when endowed with co-ordinatewise multiplication. $(g_i)(g_i') = (g_i g_i')$

i) $1_G = (1_{G_i}) = (1_{G_1}, 1_{G_2}, 1_{G_3}, \ldots)$

ii) $(g_i)^{-1} = (g_i^{-1})$

Example 11.2. Consider $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$. $(a, b) + (a', b') = (a + a', b + b')$, group law in each coordinate. $\mathbb{Z}^2 = \langle (1, 0), (0, 1) \rangle$ is finitely generated.

Proposition 11.3 (Canonical Injections and Projections)**.** Let $G_i, i \in I$ be groups and $r \in I$.

i) The canonical injection $\iota_r : G_n \to \prod_{i \in I} G_i; g \mapsto (g_i)_{i \in I}$ where $g_i = 1$ if $i \neq r$ or $g_i = g$ if $i = r$.

ii) The canonical project $\pi_r : \prod_{i \in I} G_i \to G_r; (g_i)_{i \in I} \mapsto g_r$.

iii) $\frac{G_1 \times G_2}{G_1 \times \{1\}} \cong G_2$ (Note: $G_n \times \{1\} \trianglelefteq G_1 \times G_2$).

Proof. $\pi_2 : G_1 \times G_2 \to G_2$. Apply First Isomorphism Theorem

Proposition 11.4 (Internal Characterisation of Product)**.** Let $G_1, \ldots, G_n \leq G$. Assume $G = \langle G_1, \ldots, G_n \rangle$. Assume:

i) If $i \neq j$ then elements of G_i and G_j commute

ii) For any i, $G_i \cap \langle U_{\ell \neq i} G_\ell \rangle = 1$.

Then there is an isomorphism $\phi : G_1 \times \ldots G_n \to G; (g_1, \ldots, g_n) \mapsto g_1 g_2 \cdots g_n$.

Proof. Check homomorphism:

$$\begin{aligned}
\phi((g_1, \ldots, g_n)(h_1, \ldots, h_n)) &= \phi((g_1 h_1, \ldots g_n h_n)) \\
&= g_1 h_1 g_2 h_2 \cdots g_n h_n \\
&= g_1 \cdots g_n h_1 \cdots h_n && \text{(using (i))} \\
&= \phi(g_1 \ldots g_n) \phi(h_1 \ldots h_n)
\end{aligned}$$

Surjective? Yes because G is generated by $G_1, \ldots, G_n$. Injective? Suppose $\phi((g_1, \ldots, g_n)) = 1$, then

$g_1 \cdots g_n = 1 \implies g_1^{-1} \in G_1 = g_2 \cdots g_n \in \langle G_2 \cdots G_n \rangle$ by (ii) must be id. So $g_1 = 1$ and $g_2 \cdots g_n = 1$. Repeat the same argument to get all $g_i = 1$.

Corollary 11.5. Let G = finite group of exponent 2. i.e. LCM of all orders of group element is 2. Then $G \cong \mathbb{Z}/2\mathbb{Z} \times \cdots \mathbb{Z}/2\mathbb{Z}$.

Proof. G is finitely genereqated. Choose minimal generating set $\{g_1, \ldots, g_n\}$, each $\langle g_i \rangle \cong \mathbb{Z}/2\mathbb{Z}$. Want to prove that $G \cong \langle g_1 \rangle \times \ldots \langle g_n \rangle$. Condition (i): Need $g_i g_j = g_j g_i$ for $i \neq j$. $\operatorname{ord}(g_i g_j) = 2$, so $g_i g_j g_i g_j = 1 \implies g_i g_j = g_j^{-1} g_i^{-1} = g_j g_i$. Condition (ii): e.g. $\langle g_1 \rangle \cap \langle g_2, \ldots, g_n \rangle = \{1\}$. If false, then $g_1 \in \langle g_2, \ldots, g_n \rangle$ but then our generating set is not minimal. By proposition $G \cong \langle g_1 \rangle \times \cdots \times \langle g_n \rangle$.

Theorem 11.6. Let G be a finitely generated abelian group. Then $G \cong$ product of cyclic groups. In fact $G \cong \mathbb{Z}/h_1\mathbb{Z} \times \mathbb{Z}/g_2\mathbb{Z} \times \cdots \times \mathbb{Z}/h_n\mathbb{Z} \times \mathbb{Z}^s$ where $h_1 \mid h_2 \mid h_3 \mid \cdots \mid h_n$ for some $n, r \in \mathbb{N}$.

12 Symmetries of Regular Polygons

AO_n, the set of surjective symmetries $T : \mathbb{R}^n \to \mathbb{R}^n$ forms a subgroup of $\operatorname{Perm}(\mathbb{R}^n)$.

Proposition 12.1. Let $T \in AO_n$, then $T = T_{\mathbf{v}} \circ T'$, where $\mathbf{v} = T(\mathbf{0})$ and T' is an isometry with $T'(\mathbf{0}) = \mathbf{0}$.

Proof. Set $T' = T_{\mathbf{v}}^{-1} \circ T = T_{-\mathbf{v}} \circ T$ where $\mathbf{v} = T(\mathbf{0})$. T' is an isometry because T and $T_{\mathbf{v}}$ are isometries. Also $T'(\mathbf{0}) = T_{-\mathbf{v}}(T(\mathbf{0})) = T_{-\mathbf{v}}(\mathbf{v}) = \mathbf{v} - \mathbf{v} = 0$.

Theorem 12.2. Let $T : \mathbb{R}^n \to \mathbb{R}^n$ be an isometry such that $T(\mathbf{0}) = \mathbf{0}$. Then T is linear.

The centre of mass $V = \{\mathbf{v}^1, \ldots, \mathbf{v}^m\} \subseteq \mathbb{R}^n$ is $\mathbf{c}_V = \frac{1}{m}(\mathbf{v}^1 + \cdots + \mathbf{v}^m)$.

Corollary 12.3. Let $V = \{\mathbf{v}^1, \ldots, \mathbf{v}^m\}$ and let $T : \mathbb{R}^n \to \mathbb{R}^n$ be an isometry such that $T(V) = V$. Then $T(\mathbf{c}_V) = \mathbf{c}_V$.

Proof. Decomposte $T = T_{\mathbf{w}} \circ T'$ for some $\mathbf{w} \in \mathbb{R}^n$ and isometry T' with $T'(\mathbf{0}) = \mathbf{0}$. So T' is linear. Then

$$\begin{aligned}
T(\mathbf{c}_V) &= \mathbf{w} + T'(\mathbf{c}_V) = \mathbf{w} + T'\left(\frac{1}{m}\sum_i \mathbf{v}^i\right) \\
&= \mathbf{w} + \frac{1}{m}\sum_i T'(\mathbf{v}^i) && \text{(using linearity)} \\
&= \frac{1}{m}\sum_i \big(T'(\mathbf{v}^i) + \mathbf{w}\big) = \frac{1}{m}\sum_i T(\mathbf{v}^i) \\
&= \frac{1}{m}\sum_i \mathbf{v}^i && \text{(since } T(\mathbf{v}) = \mathbf{v}) \\
&= \mathbf{c}_V
\end{aligned}$$

Corollary 12.4. Let $G \leq AO_n$ be finite. Then there exists $\mathbf{c} \in \mathbb{R}^n$ such that $T\mathbf{c} = \mathbf{c}$ for any $T \in G$. If we translate to change coordinates so $\mathbf{c} = \mathbf{0}$, then $G < O_n$.

Proof. Pick any $\mathbf{w} \in \mathbb{R}^n$ and let $V = \{S\mathbf{w} : S \in G\} \subseteq \mathbb{R}^n$. V is finite because G is finite. Also $T(V) = \{TS\mathbf{w} : S \in G\} = \{S\mathbf{w} : S \in G\} = V$. Take $\mathbf{c} = \mathbf{c}_V$ then by the previous corollary $T(\mathbf{c}) = \mathbf{c}$ for all $T \in G$.

Proposition 12.5 (Symmetries of Regular Polygons)**.** The group of symmetries of a regular n-gon is in fact D_n.

13 Abstract Symmetry and Group Actions

Definition 13.1 (G-set, Group Action)**.** A G-set is a set S equipped with a map $\alpha : G \times S \to S; (g, s) \mapsto \alpha(g, s) = g.s$ is called a group action and satisfies the following axioms:

i) $g.(h.s) = (g.h).s$ for all $g, h \in G, s \in S$.

ii) $1_G.s = s$ for all $s \in S$.

Definition 13.2 (Permutation Representation)**.** A permutation representation of a group G on a set S is a homomorphism $\phi : G \to \text{Perm}(S)$. This gives a G-set structure on S. Action is $g.s = (\phi(g))(s)$.

Proposition 13.3. Every G-set S arises from some permutation representation. Given G-set S, need to define homomorphism $\phi : G \to \text{Perm}(S)$, take $\phi(g)(s) = g.s$.

Definition 13.4. Let S_1, S_2 be G-sets. A morphism of G-sets is a function $\psi : S_1 \to S_2$ such that $g.\psi(S) = \psi(g.s)$ for all $g \in G, s \in S_1$. Say that ψ is G-equivalent or that ψ is compatible with the G-action.

14 Orbits and Stabilisers

Let $G =$ group, $S = G-$set. Define relation $\sim$ on S by $s \sim t \iff$ there exists $g \in G$ such that $t = g.s$.

Proposition 14.1. This $\sim$ is an equivalence relation.

Proof. Reflexive: $1 \in G$. Symmetric: if $t = g.s$ then $s = g^{-1}.t$. Transitive: if $t = g.s$ and $u = g'.t$ then $u = g'.(g.s) = (g'g).s$.

Corollary - Definition 14.2 (Orbits)**.** The equivalence classes of $\sim$ are called G-orbits. Also, S is a disjoint union of orbits. The G-orbit containing $s \in S$ is denoted $G.s = \{g.s : g \in G\}$. S/G denotes the set of G-orbits of S.

Proposition - Definition 14.3 (G-stable)**.** Let S be a G-set. A subset $T \subseteq S$ is called G-stable if $g.t \in T$ for all $g \in G, t \in T$.

Proposition 14.4. Let $S = G$-set and $s \in S$. The orbit $G.s$ is the smallest G-stable subset of S containing s.

Proof. $G.s$ is G-stable. If T is a G-stable subset containing s then $G.s \subseteq T$. Check these.

Definition 14.5. We say G acts transitively on G-set S, if S consists of a single orbit. i.e. for all $t, s \in S$, there exists $g : g.s = t$.

Example 14.6. Let $G = \mathrm{GL}_n(\mathbb{R})_n(\mathbb{C})$. G acts on $S = M_n(\mathbb{C})$, the set of $n \times n$ matrices over $\mathbb{C}$, by conjugation, i.e. for all $A \in G = \mathrm{GL}_n(\mathbb{C}), M \in S, A.M = AMA^{-1}$. Let us check indeed this gives a group action. Check axioms. $(i) I_n.M = I_nMI^{-1} = M.(ii)A.(B.M) = A.(BMB^{-1}) = ABMB^{-1}A_1 = (AB)M(AB)^{-1} = (AB).M$. What are the orbits? $GM = \{AMA^{-1} : A \in \mathrm{GL}_n(\mathbb{C})\}$.

Definition 14.7 (Stabilisers)**.** Let $s \in S$. Then the stabiliser of s is $\mathrm{stab}_G(s) = \{g \in G : g.s = s\} \subseteq G$

Proposition 14.8. Let S be a G-set and let $s \in S$. Then $\mathrm{stab}_G(s) \leq G$.

15 Structure of G-orbits

Proposition 15.1. Let $H \leq G$. Then G/H is a G-set with the action $g'.(gH) = (g'g)H$ for all $g, g' \in G$

Proof. Checking axioms to show G/H is a G-set.

(i) $1.(gH) = gH$

(ii) $g''.(g'.(gH)) = (g''g')(gH)$. LHS $= g''.(g'gH) = g''g'g'H = (g''g')gH =$ RHS.

Theorem 15.2 (Structure of G-orbits)**.** Suppose G acts transitively on S. Let $s \in S$ and $H = \mathrm{stab}_G(s) \leq G$. Then there is an isomorphism of G-sets: $\psi : G/H \to S; gH \mapsto g.s$.

Proof. Well-defined: if $gH = g'H$ then $g' = gh$ for $h \in H$. So we need to check $g.s = g'.s$. RHS $= g'.s = (gh).s = g.(h.s) = g.s =$ LHS, for $h \in \mathrm{stab}(s)$.

Next we need to check its a morphism of G-sets. i.e. $\psi(g'(gH)) = g'.\psi(gH) \implies (g'g).s = g'.(g.s)$. Next surjective because action is transitive. Injective: if $\psi(gH) = \psi(g'H) \implies g.s = g'.s \implies s = (g^{-1}g').s$. So $g^{-1}g' \in \mathrm{stab}(s) = H$ so $g' \in gH, gH = g'H$.

Corollary 15.3. If G is finite then, $|G.s|$ divides $|G|$ by Lagrange's theorem.

Proposition 15.4. Let $S = G$-set, $s \in S, g \in G$. Then $\mathrm{stab}_G(g.s) = g.\mathrm{stab}_G(s).g^{-1}$.

Corollary 15.5. Let $H_1, H_2 \leq G$ be conjugate. (i.e. $H_2 = gH_1g^{-1}$ for some $g \in G$). Then $G/H_1 \cong G/H_2$ as G-sets.

Definition 15.6. If $S =$ a platonic solid (all faces same, and all regular polygons, and same number of faces at each vertex) and $G =$ group of rotation symmetries $=$ symmetries $\cap SO_3$.

Proposition 15.7. With notation as above, then $|G| =$ number of faces $\times$ number of edges on each face.

Proof. Let $F =$ set of faces, G acts on F. Gives a G-set structure to F. Let $f \in F$ be a face, then $G.f = F$ (i.e. action is transitive). By the theorem, $F \cong G/\mathrm{stab}_G(f)$. But $\mathrm{stab}_G(f) =$ rotations around axis through face. $\mathrm{stab}_G(f) =$ number of edges on each face which implies $|G| = |F||\mathrm{stab}_G(f)|$.

16 Counting Orbits and Cayley's Theorem

Let G be a group and S be a G-set.

Definition 16.1 (Fixed Point Set)**.** The fixed point set of a subset $J \subseteq G$ is $S^J = \{s \in S : j.s = s \text{ for all } j \in J\}$.

Proposition 16.2. Let S be a G-set

i) If $J_1 \subseteq J_2 \subseteq G$ then $S^{J_2} \subseteq S^{j_1}$

ii) If $J \subseteq G$ then $S^J = S^{\langle J \rangle}$

Example 16.3. $G = \text{Perm}(\mathbb{R}^2)$ acts naturally on $S = \mathbb{R}^2$. Let $\tau_1, \tau_2 \in G$ be reflections about lines L_1, L_2. Then $S^{\tau_i} = L_i$, $S^{\{\tau_1, \tau 2_2\}} = L_1 \cap L_2$ and $S^{\langle \tau_1, \tau_2 \rangle} = L_1 \cap L_2$.

Theorem 16.4. Let G be a finite group and S be a finite G-set. Let $|X|$ denote the cardinality of X. Then

$$\text{number of orbits of } S = \frac{1}{|G|} \sum_{g \in G} |S^g| = \text{average size of the fixed point set}$$

Proof. Let $S = \dot{\bigcup}_i S_i$ where S_i are G-orbits. Then $S^g = \dot{\bigcup}_i S_i^g$. LHS $= \sum_i$ number of orbits of S_i (since S_i's are union of G-orbits and S_i's are disjoint) while RHS $= \sum_i \frac{1}{|G|} \sum_{g \in G} |S_i^g|$. Thus it suffices to prove theorem for $S = S_i$ and then just sum over i. But S are disjoint union of G-orbits, so can assume $S = S_i = G$-orbit which by (Theorem 15.2), means $S \cong G/H$ for some $H \leq G$. So in this case

$$\begin{aligned}
\text{RHS} &= \frac{1}{|G|} \sum_{g \in G} |S^g| \\
&= \frac{1}{|G|} \times \text{number of } (g, s) \in G \times S : g.s = s \text{ by letting } g \text{ vary all over } G \\
&= \frac{1}{|G|} \sum_{s \in S = G/H} |\operatorname{stab}_G(s)|
\end{aligned}$$

Note by proposition 15.4, these stabilisers are all conjugates, and hence all have the same size. Since $|\operatorname{stab}_G(1.H)| = |H|, |\operatorname{stab}_G(s)| = |H|$ for all $s \in S$. Hence RHS $= \frac{1}{G}|G/H||H| = \frac{|H|}{|G|}\frac{|G|}{|H|} = 1$ and LHS $=$ number of orbits of $S = 1$ as S is assumed to be a G-orbit.

Example 16.5. Birthday cake with 8 slices. Red/green candle on each slide. How many ways? Notice that: two arrangments are the same if you can rotate one to get the other.

$S = \{0, 1\}^8, |S| = 2^8 = 256$. $\sigma \in \text{Perm}(S)$ acts by $\sigma(x_1, \ldots, x_8) = (x_2, x_3, \ldots, x_8, x_1)$. $G = \langle \sigma \rangle, |G| = 8$. We want to find number of G-orbits. By the theorem above, this is equal to $\frac{1}{8} \sum_{g \in G} |S^g|$. Trying each g:

$$
\begin{aligned}
g &= 1 &&\implies |S^1| = 2^8 & g &= \sigma^4 &&\implies |S^{\sigma^4}| = 2^4\\
g &= \sigma &&\implies |S^\sigma| = 2 & g &= \sigma^5 &&\implies |S^{\sigma^5}| = 2\\
g &= \sigma^2 &&\implies |S^{\sigma^2}| = 2^2 & g &= \sigma^6 &&\implies |S^{\sigma^6}| = 2^2\\
g &= \sigma^3 &&\implies |S^{\sigma^3}| = 2 & g &= \sigma^7 &&\implies |S^{\sigma^7}| = 2
\end{aligned}
$$

$$\text{Final Answer: } \frac{1}{8}(256 + 16 + 4 + 4 + 4 + 4 \cdot 2) = \frac{1}{8}(288) = 36.$$

Definition 16.6 (Faithful Permutation Representation)**.** A permutation representation $\phi : G \to \operatorname{Perm} S$ is faithful if $\ker \phi = 1$.

Theorem 16.7 (Cayley)**.** Let G be a group. Then G is isomorphic to a subgroup of $\operatorname{Perm}(G)$. In particular, if $|G| = n < \infty$, then G is isomorphic to a subgroup of S_n.

Proof. Let G act oon itself: $g.h = gh$. This gives $\phi : G \to \operatorname{Perm}(G)$. If $g \in G$ has property that $gh = h$ for all $h \in G$ then $g = 1$. Clear, take $h = 1$.

Part II
Ring Theory

17 Rings

Definition 17.1 (Ring)**.** A ring is an abelian group R, with group addition together with ring multiplication map ($\mu : R \times R \to R$) satisfying:

i) associativity: $(rs)t = r(st)$ for all $r, s, t \in R$.

ii) there exists $1_R \in R$ such that $1r = r$ and $r1 = r$ for all $r \in R$.

iii) distributive law: $r(s+t) = rs + rt$ and $(r+s)t = rt + st$ for all $r, s, t \in R$.

Similar to a group, 1 is unique and $0r = 0$.

Example 17.2. $\mathbb{C}, \mathbb{Z}, \mathbb{R}, \mathbb{Q}$ are all rings.

Example 17.3. Let V be a vector space over $\mathbb{C}$. Define $\mathrm{End}_{\mathbb{C}}(V)$ be the set of linear maps $T : V \to V$. Then $\mathrm{End}_{\mathbb{C}}(V)$is a ring when endowed with ring additional equal to sum of linear maps, ring multiplication equal to composition of linear maps. $0 =$ constant map to $\mathbf{0}$ and $1 = \mathrm{id}_V$.

Proposition - Definition 17.4 (Subrings)**.** A subset of $S \subseteq R$ is a subring if:

i) $s + s' \in S$ for all $s, s' \in S$

ii) $ss' \in S$ for all $s, s' \in S$

iii) $-s \in S$ for all $s \in S$

iv) $0_R \in S$

v) $1_R \in S$.

Then S becomes a ring with restricted $+, \cdot, 0, 1$. Note the identity 1_R is the identity from R.

Example 17.5. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are all substrings of $\mathbb{C}$. Also the set of Gaussian integers $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ is a subring.

Example 17.6. Matrices $M_n(\mathbb{R})$ and $N_n(\mathbb{C})$ both form rings. The set of upper triangular matrices form a subring.

Proposition 17.7. i) subrings of subrings are subrings

ii) intersection of subrings is a subring

Proposition - Definition 17.8 (Units)**.** Let $R =$ ring. An element $u \in R$ is called a unit or invertible if there exists $v \in R$ such that $uv = 1$ and $vu = 1$. Define $R^* = \{$ set of units in R$\}$ as a group (with multiplicative structure).

Example 17.9. $\mathbb{Z}^* = \{1, -1\}, \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$

Definition 17.10 (Commutative Ring)**.** A ring R is commutative if $rs = sr$ for all $r, s \in R$.

Definition 17.11 (Fields)**.** A commutative ring R is a field if $R^* = R - 0$. i.e. Every non-zero element is invertible.

18 Ideals and Quotient Rings

Let $R =$ ring.

Definition 18.1 (Ideals)**.** A subgroup I of the underlying abelian group R is called an ideal of R if

$$\text{for all } r \in R, x \in I, \text{ we have } rx \in I \text{ and } xr \in I.$$

Then we write $I \trianglelefteq R$.

Example 18.2. $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ is an ideal of $\mathbb{Z}$. It is a subgroup as if $m \in n\mathbb{Z}$ then $rm \in n\mathbb{Z}$ for any integer r.

Lemma 18.3. If $\{I_i\}_{i \in A}$ ideals in R then $\bigcap_{i \in A} I_i$is an ideal of R.

Corollary 18.4. Let $R =$ ring, $S \subseteq R$ any subset. Let $J =$ set of all ideals $I \trianglelefteq R$ such that $S \subseteq I$. Define $\langle S \rangle = \bigcap_{I \in J} J$ as the ideal generated by S. (i.e. smallest ideal containing S).

Proposition 18.5.

i) If $I, J \trianglelefteq R$ then ideal generated by $I \cup J$ is $I + J = \{i + j : i \in I, j \in J\}$.

ii) Assume R is commutative and $x \in R$. Then $\langle x \rangle = Rx = \{rx : r \in R\} \subseteq R$.

iii) R commutative, $x_1, \ldots, x_n \in R$. Then $\langle x_1, \ldots, x_n \rangle = Rx_1 + \ldots Rx_n = \{r_1 x_! + \ldots r_n x_n : r_1, \ldots, r_n \in R\}$. Set of R-linear combinations of $x_1, \ldots, x_n$.

Proposition - Definition 18.6 (Quotient Ringa)**.** Let $I \trianglelefteq R$. The abelian group R/I has a well-defined multiplication map $\mu : R/I \times R/I \to R/I; (r + I, s + I) \mapsto rs + I$ which makes R/Iinto a ring, called the quotient ring of R by I.

Proof. Check multiplication is well defined, given $x, y \in I$, we need $rs + I = (r + x)(s + y) + I$. RHS $= rs + xs + ry + xy + I = rs + I$ as $xs, ry, xy \in I$. Note that the ring axioms for R/I follow from ring axioms for R.

Example 18.7. Again $\mathbb{Z}/n\mathbb{Z}$ is essentially modulo n arithmetic, i.e. $(i + n\mathbb{Z})(j + n\mathbb{Z}) = ij + n\mathbb{Z}$. Thus $\mathbb{Z}/n\mathbb{Z}$ represents not only the addition but also the multiplication in modulo n.

19 Ring Homomorphisms

Proposition - Definition 19.1 (Homomorphism)**.** Let R, S be rings. A ring homomorphism is a group homomorphism $\phi : R \to S$ such that:

i) $\phi(1_R) = 1_S$

ii) $\phi(rr') = \phi(r)\phi(r')$ for all $r, r' \in R$.

Definition 19.2 (Isomorphism)**.** A ring isomorphism is a bijective ring homomorphism $\phi : R \to S$. In this case ϕ^{-1} is also a ring homomorphism. We write $R \cong S$ as rings.

Proposition 19.3. Let $\phi : R \to S$ be a ring homomorphism.

i) If R' is a subring of R then $\phi(R')$ is a subring of S.

ii) If S' is a subring of S then $\phi^{-1}(S')$ is a subring of R.

iii) If $I \trianglelefteq S$ then $\phi^{-1}(I) \trianglelefteq R$

Corollary 19.4. In particular, $\operatorname{Im} \phi = \phi(R)$ is a subring of S and $\ker \phi = \phi^{-1}(0) \trianglelefteq R$.

Theorem 19.5. Let $R =$ ring, $I =$ ideal with $\pi : R \to R/I$ be a quotient map. Suppose $\phi : R \to S$ is a ring homomorphism such that $I \subseteq \ker \phi$. Recall group situation gives a map $\psi : R/I \to S$ then ψ is also a ring homomorphism. Special case for $I = \ker \phi$: $R/\ker \phi \cong \operatorname{Im} \phi$ (as rings).

Proposition 19.6. Let $J \trianglelefteq R$ and let $\pi : R \to R/J$ be quotient map. Then there is a 1-1 correspondence:

$$\{I \trianglelefteq R \text{ such that } J \subseteq I\} \leftrightarrow \{\text{ideals } \bar{I} \trianglelefteq R/J\}$$

Definition 19.7. An ideal $I \trianglelefteq R$, with $I \neq R$, is called maximal if it is not contained in any strictly larger ideal $J \neq R$.

Example 19.8. $10\mathbb{Z} \trianglelefteq \mathbb{Z}$ is not maximal as $10\mathbb{Z} \subsetneq 2\mathbb{Z} \triangle \mathbb{Z}$. However $2\mathbb{Z} \trianglelefteq \mathbb{Z}$ is maximal.

Proposition 19.9. Let $R \neq 0$ be a commutative ring.

i) R is a field $\iff$ every proper ideal is maximal

ii) if $I \trianglelefteq R$, with $I \neq R$, I is maximal $\iff$ R/I is a field

Proof. Assume R is a field. Let $I \trianglelefteq R$, adn assume $I \neq 0$. Then can choose $x \in I, x \neq 0$. Then x is invertible, let $y = x^{-1}$ then $1 = yx \in I$ therefore $I = R$.

Converse: assume only ideals of R are 0 and R. Take any $x \in R, x \neq 0$. Consider $I = \langle x \rangle$, cannot be 0, since $x \in I$ then $I = R$ so $xy = 1$ for some y. This proves x is invertible so R is a field.

Theorem 19.10 (Second Isomorphism Theorem)**.** R is a ring. $I \trianglelefteq R, J \trianglelefteq$ with $J \subseteq I$. Then $\frac{R/J}{I/J} \cong R/I$.

Proof. Consider $R \to R/J \to \frac{R/J}{I/J}$, show kernel is I. Then follows from First Isomorphism Theorem.

Theorem 19.11 (Third Isomorphism Theorem)**.** Let $S \subseteq R$ be a subring and $I \trianglelefteq R$. Then $S + I$ is a subring of R and $S \cap I \trianglelefteq S$.

$$\frac{S}{S \cap I} \cong \frac{S + I}{I}.$$

Example 19.12. $S = \mathbb{C}[x]$ subring of $R = \mathbb{C}[x, y]$. Let $I = \langle y \rangle = y\mathbb{C}[x, y]$.

- $S \cap I = \mathbb{C}[x] \cap \langle y \rangle = 0.$
- $S + I = \mathbb{C}[x, y] = R$

Then by the Third Isomorphism Theorem,

$$\frac{S}{S \cap I} = \frac{\mathbb{C}[x]}{0} = \mathbb{C}[x] \quad \text{and} \quad \frac{S+I}{I} = \frac{\mathbb{C}[x,y]}{\langle y \rangle},$$

$$\mathbb{C}[x, y]/\langle y \rangle \cong \mathbb{C}[x].$$

20 Polynomial Rings

Definition 20.1 (Polynomials)**.** Let R be a ring. A polynomial in x with coefficients in R is a formal expression of the form

$$\begin{aligned} p &= \sum_{i \geq 0} r_i x^i \quad \text{ where } r_i \in R \text{ and } r_i = 0 \text{ for all sufficiently large } i. \\ &= r_0 x^0 + r_1 x^1 + \cdots + r_n x^n. \end{aligned}$$

Let $R[x]$ denote the set of all such polynomials.

Proposition - Definition 20.2 (Polynomial Ring)**.** $R[x]$ is a ring. called the (univariate) polynomial ring with coefficients in R, when equipped with:

- Addition: $\sum_{i\geq 0} r_i x^i + \sum_{i \geq 0} r_i' x^i = \sum_{i \geq 0} (r_i + r_i')x^i$.
- Multiplication: $\left(\sum_{i\geq 0} r_i x^i\right) + \left(\sum_{i\geq 0} r_i' x^i\right) = \sum_{i\geq 0} \left(\sum_{j+k=i} r_j r_k'\right) x^i$.
- Zero: $r_i = 0$ for all i.
- One: $r_0 = 1$ and $r_i = 0$ for all $i \geq 1$.

Proposition 20.3. Let $\phi : R \to S$ be a ring homomorphism

i) R is a subring of $R[x]$ under $r \mapsto r + 0x + 0x^2 + \dots$

ii) ϕ induces $\phi[x] : R[x] \to S[x]$ where $\phi\left(\sum_{i\geq} r_i x^i\right) = \sum_{i\geq 0} \phi(r_i) x^i$ and this is a ring homomorphism.

Definition 20.4 (Evaluation Homomorphism)**.** Let $S \subset R$ be a subring. Let $r \in R$ such that $rs = sr$ for all $s \in S$. Define evaluation map:

$$\epsilon_r : S[x] \to R; \quad p = \sum_{i\geq 0} s_i x^i \mapsto \sum_{i \geq 0} s_i r^i = p(r).$$

Proposition 20.5. ϵ_r is a ring homomorphism from $S[x] \to R$.

Corollary 20.6. Assume R is commutative. Consider the map $c : S[x] \to \mathrm{Fun}(R, R); p \mapsto (r \mapsto p(r))$. Then$c$ is a ring homomorphism.

Example 20.7. $p(x) := x^2 + x \in (\mathbb{Z}/2\mathbb{Z})[x]$. Trying values

$$p(0) = 0^2 + 0 = 0 \qquad p(1) = 1^2 + 1 = 0$$

$p(\alpha) = 0$ for all α in domain $(\mathbb{Z}/2\mathbb{Z})$. We have $p \neq 0$ in $(\mathbb{Z}/2\mathbb{Z})[x]$ but $c(p) = 0$. That is, p defines a zero function.

Polynomials in Several Variables A possible definition is that

$$R[x_1, x_2, \ldots, x_n] = (\ldots((R[x_1])[x_2])[x_3]\ldots[x_n]) = R[x_1][x_2]\cdots[x_n]$$

.
Another definition is that $R[x_1, \ldots, x_n] = \left\{\sum_{i \in \mathbb{N}^n} r_i x^i : \text{ only finitely many non-zero } r_i\text{'s.}\right\}$. Defined similarly to $i = (i_1, \ldots, i_n) : x^i = x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$. This definition then requires you to define suitable ring operations.

Proposition - Definition 20.8. Let S be a subring of commutative ring R and $r_1, \ldots, r_n \in R$. Then $S[r_1, \ldots, r_n]$ is the subring of R generated by $S \cup \{r_1, \ldots, r_n\}$. Equivalently it is the image of $S[x_1, \ldots, x_n]$ under the evaluation map $x_i \mapsto r_i$ for all i.

Example 20.9. $R = \mathbb{C}, S = \mathbb{Z}$. Then $\mathbb{Z}[i]$ is the subring generated by $\mathbb{Z}$ and i. That is,

$$\mathbb{Z}[i] = \mathrm{Im}(\epsilon_i : \mathbb{Z}[x] \mapsto \mathbb{C}) = \left\{\sum_{j \geq 0} a_j i^j : a_j \in \mathbb{Z}\right\} = \{a + ib : a, b \in \mathbb{Z}\}$$

21 Matrix Rings

Let R be a ring. Then $M_n(R)$ is the set of $n \times n$ matrices with entries in R. Denoted,

$$(r_{ij}) = \begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nn} \end{pmatrix} \quad r_{ij} \in R.$$

Proposition 21.1. $M_n(R)$is a ring with operations

- $(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$
- $(a_{ij})(b_{ij}) = (c_{ij})$ where $c_{ij} = \sum_{k=1}^n a_{ik} b_{kj}$. Here order of multiplication is significant.
- $1_{M_n(R)} = \begin{pmatrix} 1_R & 0 & \cdots & 0 \\ 0 & 1_R & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1_R \end{pmatrix}$

Note R not necessarily commutative. e.g. $M_3(M_2(\mathbb{R}))$.

Example 21.2. In $M_2(\mathbb{C}[x])$, $\begin{pmatrix} 1 & x \\ 0 & 2 \end{pmatrix} \begin{pmatrix} x^3 & 0 \\ 4 & -x^5 \end{pmatrix} = \begin{pmatrix} 4x + x^3 & -x^6 \\ 8 & -2x^5 \end{pmatrix}$

22 Direct Products

Proposition 22.1. Let $R_i, i \in I$ be rings. $\Pi_{i\in I} R_i$ is already an abelian group under addition. It becomes a ring with multiplication: $(r_i)(s_i) = (r_i s_i)$ and identity $(1_R, 1_R, \dots,)$

Example 22.2. For $\mathbb{R} \times \mathbb{R}$, we define

- Addition: $(a, b) + (a', b') = (a + a', b + b')$
- Multiplication: $(a, b)(a', b') = (aa', bb')$
- Identity: $(1, 1)$

Note $\mathbb{R}$ is a field. But $\mathbb{R} \times \mathbb{R}$ is not a field because $(1, 0)$ has no inverse.

Lemma 22.3. Let R be a commutative ring and $I_1, \dots, I_n \trianglelefteq R$ such that $I_i + I_j = R$ for each pair of i, j. Then $I_1 + \cap_{i\geq 2} I_i = R$.

Proof. Choose $a_i \in I_1, b_i \in I_i$ such that $a_i + b_i = 1$ for $i = 2, \dots, n$ since $I_1 + I_i = R$. Then

$$\begin{aligned} 1 &= (a_2 + b_2)(a_3 + b_3) \dots (a_n + b_n) \\ &= [\text{sum of terms involving} a_i] + (b_2 b_3 \dots b_n) \\ &\in I_1 + \cap_{i\geq 2} I_i. \end{aligned}$$

So $R = I_1 + \cap_{i\geq 2} I_i$ as $r \in R, r1 = r \in I_1 + \cap_{i\geq 2} I_i$.

Theorem 22.4 (Chinese Remainder Theorem)**.** Let R be a commutative ring and $I_1, \dots, I_n \trianglelefteq R$ such that $I_i + I_j = R$ for each pair of i, j. Then the natural map

$$\begin{aligned} R/\cap_{i=1}^n I_i &\to R/I_1 \times R/I_2 \times \dots \times R/I_n \\ r + \cap_{i=1}^n I_i &\mapsto (r + I_1, r + I_2, \dots, r + I_n) \end{aligned}$$

is an isomorphism.

Proof. (Missing some details). We prove the result by induction on n. Let $n = 2$. Consider $\psi : R/(I_1 \cap I_2) \to R/I_1 \times R/I_2$ with $r + (I_1 \cap I_2) \mapsto (r + I_1, r + I_2)$. Then ψ is well-defined if $r - s \in I_1 \cap I_2$ then $r + I_1 = s + I_1$ and $r + I_2 = s + I_2$. If $\psi(r + (I_1 \cap I_2)) = 0$ then $r \in I_1$ and $r \in I_2$ so $r \in I_1 \cap I_2$ so ψ is injective. Choose $x_1 \in I_1, x_2 \in I_2$ such that $x_1 + x_2 = 1$. Now given r_1 and r_2, observe $\psi(r_2 x_1 + r_1 x_2) = (r_2 x_1 + r_1 x_2 + I_1, r_2 x_1 + r_1 x_2 + I_2)$. Consider $r_2 x_1 + r_1 x_2 + I_1$. Then $r_2 x_1 \in I_1$ as $x_1 \in I_1$ and $r_1 x_2 = r_1(1 - x_1) = r_1 - r_1 x_1$ with $x_1 \in I_1$ which implies $r_2 x_1 + r_1 x_2 + I_1 = r_1 + I_1$. Similarly $r_2 x_1 + r_1 x_2 + I_2 = r_2 + I_2$. So $\psi(r_2 x_1 + r_1 x_2) = (r_1 + I_1, r_2 + I_2)$ hence ψ is onto. Using the above lemma, we have the $n = 2$ case.

Example 22.5. If $R = \mathbb{Z}$, $I_1 = 3\mathbb{Z}, I_2 = 5\mathbb{Z}$ then $I_1 \cap I_2 = 15\mathbb{Z}$. So we have the following isomorphism,

$$\mathbb{Z}/15\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$
$$n + 15\mathbb{Z} \mapsto (r + 3\mathbb{Z}, r + 5\mathbb{Z})$$

Note $\mathbb{Z}/24\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ is not an isomorphism.

23 Field of Fractions

In this section let R be a commutative ring.

Definition 23.1 (Domain)**.** R is called a domain (or integral domain) if for all $r, s \in R : rs = 0 \implies r = 0$ or $s = 0$. i.e. R does not have non-trivial zer divisors.

Example 23.2. $\mathbb{Z}, \mathbb{C}[x_1, \ldots, x_n]$ are both domains. $\mathbb{Z}/6\mathbb{Z}$ is not a domain as $2 \times 3 = 0$ but neither $2 \neq 0, 3 \neq 0$. However $\mathbb{Z}/p\mathbb{Z}$ for a prime p is a domain. In fact, any field is a domain.

Then we define $\tilde{R} = R \times (R - 0) = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} : a \in R, b \in R - 0 \right\}$. Now define a relation on $\tilde{R}$: $\begin{pmatrix} a \\ b \end{pmatrix} \sim \begin{pmatrix} a' \\ b' \end{pmatrix}$ if $ab' = a'b$.

Lemma 23.3. $\sim$ is an equivalence relation on $\tilde{R}$.

Proof. Reflexive and symmetric are easy. For transitivity, if $ab' = a'b$ and $a'b'' = a''b'$ then the first equation implies $ab'b'' = a'bb'' = a''bb' \implies (ab'' - a''b)b' = 0$. Since R is a domain then $ab'' = a''b$.

Notation Let $\frac{a}{b}$ denote the equivalence class of $\begin{pmatrix} a \\ b \end{pmatrix}$ and $K(R) = \tilde{R}/\sim$, the set of fractions.

Lemma 23.4. The operations $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ and $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ give well-defined addition and multiplication on $K(R)$.

Theorem 23.5. These ring addition/multiplication maps make $K(R)$ into a field, with $0_{K(R)} = \frac{0_R}{1_R}$ and $1_{K(R)} = \frac{1_R}{1_R}$.

Example 23.6. $K(\mathbb{Z}) = \mathbb{Q}$ and $K(\mathbb{R}[x]) =$ set of real rational functions $= \left\{ \frac{f(x)}{g(x)} : f, g \in \mathbb{R}[x], g \neq 0 \right\}$. Similarly, $K(\mathbb{Q}[x]) = \left\{ \frac{f(x)}{g(x)} : f, g \in \mathbb{Q}[x], g \neq 0 \right\} = K(\mathbb{Z}[x])$. Let F be a field, then $K(F[x_1, \ldots, x_n]) = F(x_1, \ldots, x_n)$, where this indicates a field of rational functions in $x_1, \ldots, x_n$ over F.

Proposition 23.7. i) The map $\iota : R \to K(R); \alpha \mapsto \frac{\alpha}{1}$ is an injective ring homomorphism. This allows us to consider R as a subring of $K(R)$.

ii) If S is a subring of R then $K(S)$ is essentially a subring of $K(R)$.

Proposition 23.8. If F is a field, then $K(F) = F$. i.e. the map $\iota : F \to K(F)$ is an isomorphism.

Proof. Injective from above. Surjectivity as given $\frac{a}{b} \in K(F), b \neq 0$, then $\iota(ab^{-1}) = \frac{ab^{-1}}{1} = \frac{a}{b}$ because $(ab^{-1})b = 1a$.

Example 23.9. By the above proposition we have $K(\mathbb{Q}[i]) = \mathbb{Q}[i] = \{r + si : r, s \in \mathbb{Q}\}$. But by Proposition 23.7, $\mathbb{Z}[i] \leq \mathbb{Q}[i] \implies K(Z[i]) \leq K(\mathbb{Q}[i])$ and hence $K(\mathbb{Z}[i]) = \mathbb{Q}[i]$. More generally, $K(R)$ is the smallest field containing R.

24 Introduction to Factorisation Theory

In this section let R be a commutative domain.

Definition 24.1 (Prime Ideal)**.** An ideal $P \trianglelefteq R, P \neq R$ is called prime if R/P is a domain. Equivalently, if $rs \in P$ then either $r \in P$ or $s \in P$ (or both).

Example 24.2. $\mathbb{Z}/p\mathbb{Z}$ for prime p, is a domain, so $p\mathbb{Z} \trianglelefteq \mathbb{Z}$. $(0) \trianglelefteq \mathbb{Z}$ is prime but not maximal.

$\langle y \rangle \trianglelefteq \mathbb{C}[x, y]$ is prime because $\mathbb{C}[x, y]/\langle y \rangle \cong \mathbb{C}[x]$ is a domain.

If $m \trianglelefteq R$ is maximal, then m is prime because R/m is a field which implies R/m is a domain.

Definition 24.3 (Divsibility)**.** Let $r, s \in R$. We say $r \mid s$, "r divides s" if $s = rt$ for some $t \in R$. Equivalently $s \in \langle r \rangle$ or $\langle s \rangle \subseteq \langle r \rangle$.

Example 24.4. $3 \mid 6$ as $6\mathbb{Z} \subseteq 3\mathbb{Z}$.

Definition 24.5 (Associates)**.** Let $r, s \in R - 0$ are associates if one of the following two equivalent conditions hold:

- $\langle r \rangle = \langle s \rangle$ i.e. $r \mid s$ and $s \mid r$.
- There is a unit $u \in R^*$ (u is a unit of R) with $r = us$.

Example 24.6. In $\mathbb{Z} : \langle -2 \rangle = \langle 2 \rangle$ so $2, -2$ are associates. In $\mathbb{Z}[i] : \langle 3i \rangle = \langle 3 \rangle = \langle -3 \ \rangle$.

Definition 24.7 (Primes)**.** An element $p \in R, p \neq 0$ is prime if $\langle p \rangle$ is prime. Equivalently p is not a unit, and $p \mid rs \implies p \mid r$ or $p \mid s$.

Definition 24.8 (Irreducibles)**.** An element $p \in R, p \neq 0, p$ is not a unit, is irreducible whenever $p = rs$, either r or s is a unit.

Example 24.9. $p = 5 = 5 \cdot 1 = (-5)(-1) = 1 \cdot 5 = (-1)(-5)$, so 5 is irreducible. $p = 4 = 2 \cdot 2$ but neither 2 nor 2 are units, so 4 is not irreducible.

Proposition 24.10 (Prime implies Irreducible)**.** Suppose $p \in R$ is prime. Then p is not a unit (otherwise $\langle p \rangle = R$ is not prime). Suppose $p = rs, r, s \in R$ then $p \mid rs$. Without loss of generality say $p \mid r$, so $r = pq$ for some $q \in R$. Then $p = pqs \implies 1 = qs$, so s is a unit.

Definition 24.11 (Unique Factorisation Domains)**.** R is a unique factorisation domain (UFD) if

i) every nonzero non-unit $r \in R$ can be written as $r = p_1 \cdots p_n$ with all p_i irreducible.

ii) if $r = p_1 \cdot p_n = q_1 \cdots q_m$ with all p_i, q_i irreducible, then $n = m$ and we can re-index teh q_i such that p_i and q_i are associates for all i.

Example 24.12. $\mathbb{Z}$ is a UDF. In $\mathbb{Z}, 30 = 2 \cdot 3 \cdot 5 = (-5)(-3)2$. $12 = 2 \cdot 2 \cdot 3 = (-2)2(-3)$.

Lemma 24.13. Assume every irreducible is prime. If r can be factored into irreducible (as in (i)) then the factorisation is unique (i.e. as in (ii)).

Example 24.14. $R = \mathbb{C}[x]$ so $\mathbb{C}[x]^\times = \mathbb{C}^\times$. Any complex polynomial factors into linear factors (Fundamental Theorem of Algebra) so the irreducibls are linear polynomias, i.e. $\alpha(x - \beta)$, $\beta \in \mathbb{C}, \alpha \in \mathbb{C}^\times$. We prove $x - \beta$ is prime as $\mathbb{C}[x]/\langle x - \beta \rangle \cong \mathbb{C}$ is a domain. i.e. every irreducible is prime.

Proof. Suppose $r \in R, r = p_1 \cdots p_n = q_1 \cdots q_m$ (both products of irreducibles). Induction on n. $n = 1, p_1 = q_1 \cdots q_m$. Then by definition of irreducible, $m = 1$ and $p_1 = q_1$.

Now suppose $n > 1$, $p_1 \cdots p_n = q_1 \cdots q_m$. THen $p_1 \mid q_1 \cdots q_m$, but p_1 irreducible which means p_1 is prime. Then p_1 divides some q_i. After permuting q_i's, assume $p_1 \mid q_1$. So $q_1 = p_1 u$ where u is a unit. Cancel out p_1, q_1 from relation, $p_2 \cdots p_n = (uq_2)q_3 \cdots q_m$. By induction, $(p_2 \cdots p_n)$ is a permutation $(uq_2 \cdots q_m)$ up to associates.

25 Principal Ideal Domains

Definition 25.1 (Principal Ideal Domain)**.** Let R be a commutative ring. An ideal I is principal if $I = \langle r \rangle, r \in R$ (generated by a single element). A principal ideal domain (PID) is a domain where every ideal is principal.

Example 25.2. $\mathbb{Z}$ is a PID, every ideal of is of the form $n\mathbb{Z}$.

Proposition 25.3. Let R be a PID. Let $p \in R, p \neq 0$, then p is irreducible if and only if $\langle p \rangle$ is maximal.

Proof. ($\Longleftarrow$) Assume p is not irreducible, so $p = rs$. Neither r, s are units. Then $\langle p \rangle = \langle rs \rangle \subsetneq \langle r \rangle$ so $\langle p \rangle$ is not maximal. (*Alternatively*: $\langle p \rangle$ maximal $\implies$ $\langle p \rangle$ prime $\implies$ p prime $\implies$ p irreducible.)

($\implies$) Suppose $\langle p \rangle \subseteq I$. Since R is a PID, $I = \langle q \rangle$ for some q hence $q \mid p$. Since p irreducible, either $q = up (u \in R^*) \implies I = \langle q \rangle = \langle p \rangle$ or q is a unit so $I = \langle q \rangle = R$.

Corollary 25.4. In a PID, irreducibles are prime.

Proof. p ideal $\implies$ $\langle p \rangle$ maximal $\implies$ $R/\langle p \rangle$ is a field $\implies$ $R/\langle p \rangle$ is a domain $\implies$ $\langle p \rangle$ prime $\implies$ p is prime.

Note, in a PID factorisations are unique if they exist.

Lemma 25.5. Let S be a ring. Let $I_0, I_1, I_2, \ldots$ are ideals of S such that $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$. Then $\bigcup_{i \geq 0} I_i$ is an ideal of S.

Proof. Suppose $x, y \in \cup_{i\geq 0} I_i$ then $x \in I_n$ and $y \in I_m$, so $x, y \in I_k$ where $k = \max(n, m)$ therefore $x + y \in T_k \subseteq \cup_{i\geq 0} T_i$. Then prove other ideal properties.

Theorem 25.6. Any PID is a UFD.

Proof. We need to prove that any $r_0 \in R$, not has a factorisation into ideals. Suppose $r_0 \in R$, not a unit is not a product of irreducibles. In particular r itself is not irreducible, so $r = r_1 q_1$ where r_1, q_1 not units. At least one of r_1, q_1 is not a product of irreducibles. Repeat this argument for $r_1 = r_2 q_2$ where without loss of generality, r_2 is not a product of irreducibles. Then we have r_0, r_1, r_2 so $r_1 \mid r_0, r_2 \mid r_1$ etc.. Then $\langle r_0 \rangle \subseteq \langle r_1 \rangle \subseteq \langle r_2 \rangle \subseteq \ldots$.

Let $I = \cup_{i\geq 0} \langle r_i \rangle$. By the previous Lemma, I is an ideal. Since R is a PID, $I = \langle s \rangle$, $s \in R$. So $s \in \langle r_n \rangle$ for some n, $I \subseteq \langle r_n \rangle \subseteq \langle r_{n+1} \rangle \subseteq \cdots \subseteq I$. So in fact, $I = \langle r_n \rangle = \langle r_{n+1} \rangle = \ldots$ but this contradicts $\langle r_n \rangle \subsetneq \langle r_{n+1} \rangle$ because $r_n = r_{n+1} q_{n+1}$ where q_{n+1} is not a unit.

Definition 25.7 (Greatest Common Divisor)**.** Let R be a PID (works for UFD). Let $r, s \in R, r, s \neq 0$. Then a greatest common divisor (gcd) of r and s is an element $d \in R$ such that $d \mid r, d \mid s$ and if $c \in R$ is any element such that $c \mid r, c \mid s$, then $c \mid d$. Write $d = \gcd(r, s)$. d is defined only up to units.

Any 2 gcd's divide each other so are associates.

Proposition 25.8. In a PID, $r, s \in R - \{0\}$ then r, s have a gcd d such that $\langle d \rangle = \langle r, s \rangle$.

Proof. Given r, s. Consider $\langle r, s \rangle = \{ar + bs : a, b \in R\}$. Since R is PID, $\langle r, s \rangle = \langle d \rangle$ for some $d \in R$. $d \mid r$ is clear since $r \in \langle d \rangle$. Similarly $d \mid s$. Now suppose $c \mid r$ and $c \mid s$. Then $r, s \in \langle c \rangle \implies \langle r, s \rangle \subseteq \langle c \rangle \implies \langle d \rangle \subseteq \langle c \rangle \implies c \mid d$.

26 Euclidean Domains

The motivation here is to give a useful criterion for a commutative domain to be a PID and UFD.

Proposition 26.1. $R = \mathbb{C}[x]$ is a PID.

Proof. Let I be a nonzero ideal in $\mathbb{C}[x]$. Let $f \in I$ be a nonzero element of smallest degree. It is clear that $\langle f \rangle \subseteq I$. Now given any $g \in I$, divide g by $f : g = fq + r$, where either $r = 0$ or $\deg r < \deg f$ (This uses the fact that $\mathbb{C}[x]$ has a division algorithm). Thus $f \in I$, so $qf \in I$ also $g \in I \implies r = g - qf \in I$. By choice of f (minimal degree in I) we must have $r = 0$. Therefore $f \mid g$ i.e. $g \in \langle f \rangle$ so $I =\subseteq \langle f \rangle$. This proves $I = \langle f \rangle$.

Definition 26.2 (Euclidean Domain)**.** Let R be a commutative domain. A function $\nu : R - \{0\} \to \mathbb{N}$ is called a Euclidean function on R if:

i) for all $f, p \in R, p \neq 0$, there exists $q, r \in R$ such that $f = pq + r$ where either $r = 0$ or $\nu(r) < \nu(p)$.

ii) if $f, g \in R - \{0\}$ then $\nu(f) \leq \nu(fg)$.

If R has such a function, we call it an Euclidean domain.

Example 26.3. If $R = F[x]$ where F is a field. Then $\nu(f) = \deg f$. If $R = \mathbb{Z}$, then $\nu(n) = |n|$.

Theorem 26.4. Let R be a Euclidean domain with ν. Then R is a PID and hence a UFD.

Proof. Let $I \trianglelefteq R$ be nonzero ideal. Choose $f \in I$ with minimal $\nu(f)$. Clearly $\langle f \rangle \subseteq I$. Given $g \in I$ write $g = qf + r$ with $r = 0$ or $\nu(r) < \nu(f)$ as before (previous proof) $r \in I$. So $r = 0$ then $f \mid g$ so $I \subseteq \langle g \rangle$.

Lemma 26.5. Let R be one of $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}], \mathbb{Z}[\sqrt{-2}], \mathbb{Z}[\frac{1+\sqrt{-3}}{2}], \mathbb{Z}[\frac{1+\sqrt{-7}}{2}], \mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$. Define $\nu : R \to \mathbb{R}$ by $\nu(z) = |z|^2$. Then

i) ν takes integer values on R

ii) for any $z \in \mathbb{C}$, there is some $s \in R$ such that $\nu(z - s) < 1$.

Proof. We prove this for $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} : a, b \in \mathbb{Z}\}$. Then $\nu(a + b\sqrt{-2}) = |a + b\sqrt{-2}|^2 = a^2 + 2b^2 \in \mathbb{N}$. Let $z = x + iy \in \mathbb{C}$. Choose s to be closest $a + b\sqrt{-2}$ to z. Then $|a - x| \leq \frac{1}{2}$ and $|b\sqrt{2} - y| \leq \frac{\sqrt{2}}{2}$. Then

$$|s - z|^2 = |(a + b\sqrt{-2}) - (x + iy)^2 \leq (\frac{1}{2})^2 + (\frac{\sqrt{2}}{2})^2 = \frac{3}{4} < 1.$$

So $\nu(s - z) < 1$. We can repeat this argument for the other cases with simple modification of the argument.

Theorem 26.6. Let R be one of the rings from the previous lemma. Then ν is a Euclidean norm on R.

Note For the remainder of this section, denote R to be a Euclidean domain and $\nu : R \to \mathbb{Z}_+$ the Euclidean norm.

Proposition 26.7. Let $I \trianglelefteq R$ be an ideal. Let $p \in I, p \neq 0$. Then p generates $I \iff \nu(p)$ is minimal (on I). In particular, $p \in R^* \iff \nu(p) = \nu(1)$.

Proof. If $\nu(p)$ minimal then by the results prior $I = \langle p \rangle$. Conversely, if $I = \langle p \rangle$ and $f = gp \in I$ for some g then $\nu(f) = \nu(gp) \geq \nu(p)$.

Example 26.8. In $\mathbb{Z}[i] : \nu(z) = |z|^2$. $u \in \mathbb{Z}[i]^* \implies |u|^2 = 1 \implies u = \pm 1, \pm i$. Also, $\mathbb{Z}[\sqrt{-2}]^* = \{\pm 1\}$ for $\nu(z) = |z|^2$.

Theorem 26.9 (Euclidean Algorithm)**.** To find the gcd of two elements f and g we can use the following algorithm. Assume $\nu(f) \geq \nu(g)$. Find $q, r \in R$ such that $f = qg + r$ with either $r = 0$or $\nu(r) < \nu(g)$. If $r = 0$, then $\langle f, g \rangle = \langle g \rangle$ because $f \in \langle f \rangle$ so the gcd is g. If $r \neq 0$, then $\langle f, g \rangle = \langle g, r \rangle$ since $f \in \langle g, r \rangle (f = qg + r), r \in \langle f, g \rangle (r = f - qg)$. So $\gcd(f, g) = \gcd(g, r)$. In this case, repeat first step with g, r instead of f, g. The algorithm terminates because $\nu(r) < \nu(g)$ and $\mathbb{N}$ has minimum at 0.

Example 26.10. In $R = \mathbb{Z}[\sqrt{-2}]$, find $\gcd(y + \sqrt{-2}, 2\sqrt{-2})$ for y odd. Answer is 1, see course notes for computation.

Theorem 26.11. The only integer solutions to $y^2 + 2 = x^3$ are $y = \pm 5, x = 3$.

Proof. If y is even, then x^3 is even, then x is even. So $x^3 = 0 \mod 8$. But LHS can only be 2 or $6 \mod 8$, hence $y$must be odd.

Let's work in $\mathbb{Z}[\sqrt{-2}]$. The equation becomes $(y+\sqrt{-2})(y-\sqrt{-2}) = x^3$.

$$\begin{aligned}
\gcd(y+\sqrt{-2}, y-\sqrt{-2}) &= \gcd(y+\sqrt{-2}, (y-\sqrt{-2}) - (y+\sqrt{-2})) \\
&= \gcd(y+\sqrt{-2}, 2\sqrt{-2}) \\
&= 1.
\end{aligned}$$

Now have: $(y+\sqrt{-2})(y-\sqrt{-2}) = x^3$. By UFD, $y+\sqrt{-2} = u\alpha^3$ where $u \in \mathbb{Z}[\sqrt{-2}]^*, \alpha \in \mathbb{Z}[\sqrt{-2}]$.

> More detail: consider prime factorisation of $y+\sqrt{-2}, y-\sqrt{-2}, x^3$. Any prime must occur as p^{3e} on RHS for some $e \in \mathbb{Z}$. If $e \geq 1$, then $p \mid$ either $y+\sqrt{-2}$ or $y-\sqrt{-2}$ but not both. So p^{3e} is the exact power of p divides either $y+\sqrt{-2}$ or $y-\sqrt{-2}$.

Possible units: $u \pm 1$ which are both cubes. So

$$\begin{aligned}
y+\sqrt{-2} &= \beta^3 = (a+b\sqrt{-2})^3 \\
&= a^3 + 3a^2b\sqrt{-2} - 6ab^2 - 2b^3\sqrt{-2} \\
&= (a^3 - 6ab^2) + \sqrt{-2}(3a^2b - 2b^3) \\
y-\sqrt{-2} &= (a^3 - 6ab^2) - \sqrt{-2}(3a^2b - 2b^3).
\end{aligned}$$

Subtract both sides

$$\begin{aligned}
2\sqrt{-2} &= 2\sqrt{-2}(3a^2b - 2b^3) \\
1 &= 3a^2b - 2b^3 = b(3a^2 - 2b^2) \\
b &= \pm 1
\end{aligned}$$

Then you can find a, deduce y which then gives x.

27 Gauss's Lemma

Proposition 27.1. In a UFD, any irreducibles are primes.

Proof. Follows from observation that $q_1 \mid rt \implies q_1 = up_j$ or $q_1 = vr_l, u, v \in R^*$ by unique factorisation. Therefore $q_1 \mid p_j \mid r$ or $q_1 \mid r_l \mid t$.

Definition 27.2 (Primitive Polynomials)**.** $f \in R[x], f \neq 0$ is primitive if the gcd of its coefficients is 1.

Example 27.3. $3x^2 + 2 \in \mathbb{Z}[x]$ is primitive, but $6x^2 + 4$ is not.

Proposition 27.4. Let R be a UFD and $K = K(R)$.

i) if $f \in K[x], f \neq 0$, then there exists $\alpha \in K^*$ such that $\alpha f \in R[x]$ and αf primitive

ii) if $f \in R[x], f \neq 0$ is primitive, and $\alpha \in K^*$ such that $\alpha f \in R[x]$ then $\alpha \in R$.

Proof.

i) Choose $d =$ common denominator, then $df \in R[x]$. Now choose $e = \gcd(\text{coefficients of } df) \in R$. Then $\frac{df}{e} \in R[x]$ and primitive so take $\alpha = \frac{d}{e}$.

ii) Let $\alpha = \frac{n}{d}$ with $n \in R, d \in R, d \neq 0$. Then $\gcd(\text{coefficients of } nf) = n \gcd(\text{coefficients of } f) = n \times 1 = n = d \gcd(\text{coefficients of } (\frac{b}{d})f) = d \gcd(\text{coefficients of } \alpha f) \implies n = \text{multiple of } d \implies \alpha \in R$.

Lemma 27.5 (Gauss's Lemma)**.** Let R be a UFD and $f = f_0 + \cdots + f_m x^m, g = g_0 + \cdots + g_n x^n \in R[x]$ be primitive polynomials. Then fg is primitive.

Proof. We need to show that for any prime p, p does not divide all coefficients of fg. Consider $\bar{f} =$ image of f in $(R/p)[x]$ and similarly for $\bar{g}$ where R/p is a domain. Neither $\bar{f}$ nor $\bar{g}$ are 0 as they are primitive so $\bar{f}\bar{g} = \bar{f}g$ is not the zero polynomial.

Corollary 27.6. Let R be a UFD and $K = K(R)$. Let $f \in R[x]$, assume $f = gh$ with $g, h \in K[x]$. Then $f = \bar{g}\bar{h}$ where $\bar{g}, \bar{h} \in R[x]$ and $\bar{g} = \alpha g$, $\bar{h} = \beta h$ where $\alpha, \beta \in K^*$.

Proof. Write $g = \gamma g', h = \delta h'$ where $\gamma, \delta \in K^*$ and $g', h' \in R[x]$ with both g', h' primitive. Then $f = \gamma\delta g' h'$ then by Gauss' lemma, $g'h'$ is primitive. So $\gamma\delta \in R$ then take $\bar{g} = \gamma\delta g', \bar{h} = h'$.

Theorem 27.7. Let R be a UFD and $K = K(R)$

i) the primes in $R[x]$ are either primes in R or primitive polynomials of positive degree that are irreducible in $K[x]$

ii) $R[x]$ is a UFD.

Corollary 27.8. Let R be a UFD, then $R[x_1, x_2, \ldots, x_n]$ is also a UFD.

Part III
Field Theory

28 Field Extensions

Definition 28.1 (Field Extensions)**.** If F is a subfield of E. We say E is an extension of F, or we say that E/F is a field extension.

Definition 28.2 (Generators of Field Extensions)**.** Let E/F be a field extension, and let $\alpha_1, \ldots, \alpha_n \in E$. Denote $F(\alpha_1, \ldots, \alpha_n)$ the subfield of E generated by $F, \alpha_1, \ldots, \alpha_n$. This is called the subfield generated by $\alpha_1, \ldots, \alpha_n$ over F. If E is of the form $E = F(\alpha_1, \ldots, \alpha_n)$, we say that E/F is a finitely generated extension.

Example 28.3. $\mathbb{Q}(i) \subseteq \mathbb{C}$, $\mathbb{Q}(i) = \{a + ib : a, b \in \mathbb{Q}\} = \mathbb{Q}[i]$. Also, $\mathbb{Q}(\pi) \subseteq \mathbb{R}$, $\mathbb{Q}(\pi) = \left\{\frac{f(\pi)}{g(\pi)} : fg \in \mathbb{Q}[x], g \neq 0\right\} \neq \mathbb{Q}[x]$.

Let E/F be a field extension and $\alpha \in E^{\times}$. Recall the evaluation homomorphism, $\epsilon : F[x] \to E; p \mapsto p(\alpha)$ and $\operatorname{Im} \epsilon = F[\alpha] \subseteq E$.

Theorem - Definition 28.4 (Transcendental and Algebraic)**.** There are two possibilities:

i) $\ker \epsilon = 0$. (ϵ is injective). i.e. α is not a root of any nonzero polynomial in $F[x]$. We say that α is transcendental over F. Hence, $F[\alpha] \cong F[x]$.

ii) $\ker \epsilon \neq 0 = \langle p \rangle$ where p is monic of minimal degree. Then $F[\alpha] \cong F[x]/\langle p \rangle$. We say that α is algebraic over F and $p(x)$ is called the minimal polynomial of α over F. We say that E/F is algebraic if every $\alpha \in E$is algebraic over F.

Example 28.5. i) $\sqrt{2} = 1.414 \cdots \in \mathbb{R}$. Minimal polynomial of $\sqrt{2}$:

- over $\mathbb{Q} : x^2 - 2$
- over $\mathbb{R} : x - \sqrt{2}$

ii) In $\mathbb{R}(x)/\mathbb{R}$, the element $x$is transcendental over $\mathbb{R}$. $\epsilon : \mathbb{R}[x] \to \mathbb{R}(t); x \mapsto t$.

iii) $\mathbb{R}/R$ is algebraic. Let $z = a + ib \in \mathbb{C}$. $(z - a)^2 + b^2 = 0$ then $p(x) = (x - a)^2 b^2 = x^2 - 2ax + (a^2 + b^2) \in R[x]$, $p(z) = 0$.

Proposition 28.6. If $\alpha \in E$ is algebraic over F, then its minimal polynomial in $F[x]$is irreducible.

Proposition 28.7. Let $F(\alpha)$ be a simple extension.

i) If α is transcendental over F, then $F(\alpha) \cong F(x)$ (field of rational functions in 1 variable)

ii) If α is algebraic over F, then $F(\alpha) = F[\alpha] \cong F[x]/\langle p \rangle$ where $p$is the minimal polynomial.

Proof.

i) Know $F[\alpha] \cong F[x]$, take fraction fields gives $F(\alpha) \cong K(F[x]) \cong F(x)$.

ii) Know $F[\alpha] \cong F[x]/\langle p \rangle$. $\langle p \rangle$ is maximal because p is irreducible hence $F[x]/\langle p \rangle$ is a field. Therefore since $F[\alpha]$ is already a field, so $F(\alpha) = F[\alpha]$.

Example 28.8.

- $\mathbb{Q}(i) = \mathbb{Q}[i] \cong \mathbb{Q}[x]/\langle x^2+1 \rangle$
- Let $f(x) = x^3 + x^2 - 1 \in \mathbb{Q}[x]$ which is irreducible. Let α be a root of f. Consider $\mathbb{Q}[\alpha] = \{r + s\alpha + t\alpha^2 : r, s, t \in \mathbb{Q}\}$. E.g. try $\beta = \alpha^2 + 1 \in \mathbb{Q}[\alpha]$. Apply Euclidean algorithm to $f(x)$ and $g(x) = x^2+1$ which gives $\frac{1}{5}(x-2)f(x) + \frac{1}{5}(-x^2+x+3)g(x) = 1$ in $\mathbb{Q}[x]$. Substituting $x = \alpha$: $0 + \frac{1}{5}(-\alpha^2+\alpha+3)\beta = 1$. So $\beta^{-1} = \frac{1}{5}(-\alpha^2+\alpha+3) \in \mathbb{Q}[\alpha]$. This kind of calculation shows that $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$. i.e. $\mathbb{Q}[\alpha]$ is a field.

Definition 28.9 (Degree)**.** Let E/F be a field extension. Then E is a vector space over F. The degree of E/F is $[E : F] = \dim_F E$. We say E/F is a finite extension if $[E : F] < \infty$.

Example 28.10. $[\mathbb{C} : \mathbb{R}] = 2, [\mathbb{R} : \mathbb{Q}] =$ uncountable ∞.

Proposition 28.11. Any finite extension is algebraic.

Proof. Let E/F be finite, say $\dim n \geq 1$. Let $\alpha \in E$. Then $1, \alpha, \alpha^2, \ldots, \alpha^n$ must be linearly dependent over F. i.e. there exists $c_0, \ldots, c_n \in F$ not all 0 such that $c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0$. i.e. $p(\alpha) = 0$ where $p(x) = c_0 + c_1x + \cdots + c_nx^n \in F[x]$. So α is algebric over F.

Theorem 28.12 (The Tower Law)**.** Let K/E and E/F be finite. Then K/F is finite and $[K : F] = [K : E][E : F]$.

Proposition 28.13. Suppose $\alpha \in E$ is algebraic over F. Then $[F(\alpha) : F] = \deg p$ where p is a minimal polynomial of α over F.

Example 28.14. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(2^{1/4})$. What is $[\mathbb{Q}(2^{1/4}) : \mathbb{Q}]$?

- $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ because minimal polynomial of $\sqrt{2}/\mathbb{Q}$ is $x^2 - 2$ has degree 2.
- $[\mathbb{Q}(2^{1/4}) : \mathbb{Q}(\sqrt{2})] = 2$ because minimal polynomial of $2^{1/4}$ over $\mathbb{Q}(\sqrt{2})$ is $x^2 - \sqrt{2}$.

Then by the tower law, $[\mathbb{Q}(2^{1/4}) : \mathbb{Q}] = [\mathbb{Q}(2^{1/4}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$.

Theorem 28.15 (Eisenstein's Criterion)**.** Let R be a UFD, $K = K(R)$. Let $f = f_0 + f_1x + \cdots + f_nx^n \in R[x]$. Suppose there exists a prime $p \in R$ such that $p \mid f_0, \ldots, p \mid f_{n-1}$ but $p \nmid f_n$ and $p^2 \nmid f_0$. Then f is irreducible in $K[x]$.

Theorem 28.16 (Splitting Fields)**.** Let F be a field, $f \in F[x], f \neq 0$. Then there exists a field extension E/F such that $f(x)$ is a product of linear factors in $E[x]$, i.e. $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$ for $\alpha_1, \ldots, \alpha_n \in E$. The subfield $F(\alpha_1, \ldots, \alpha_n)$ generated by F and the α's is called a splitting field for $f(x)$ over F.

Proof. Induction on $n = \deg f$. For $n = 1$, just take $E = F$. Suppose $n > 1$, let $p \in F[x]$ be an irreducible factor of f. Let $K = F[x]/\langle p \rangle$. Then K is a field (since p is irreducible), K contains a root of p namely $\alpha = x + \langle p \rangle \in K$. Also F is a subfield of K. In $K[x]$ we have $f(x) = (x-\alpha)g(x)$ for $g \in K[x], \deg g < \deg f$. By induction, there is an extension E of K such that g factors into linear factors in $E[x]$. So does f.

Example 28.17. Splitting field of $x^3 - 2$ over $\mathbb{Q}$.

We already know in $\mathbb{C}$: $x^3 - 2 = (x - 2^{1/3})(x - 2^{1/3}\omega)(x - 2^{1/3}\omega^2)$ where $\omega = e^{2\pi i/3}$ so splitting field is $\mathbb{Q}(2^{1/3}, \omega)$.

$x^3 - 2$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein's Criterion. Let $K = \mathbb{Q}[x]/\langle x^3 - 2\rangle$ and $\alpha = x + \langle x^3 - 2\rangle \in K$. So $\alpha^3 = (x + \langle x^3 - 2\rangle)^3 = x^3 + \langle x^3 - 2\rangle = x^3 - 2 + 2 + \langle x^3 - 2\rangle = 2 + \langle x^3 - 2\rangle = 2$. Then $x^3 - 2 = (x - \alpha)(x^2 + \alpha x + \alpha^2)$ in $K[x]$.

Q: is $x^2 + \alpha x + \alpha^2$ irreducible in $K[x]$.

Proof. Suppose not. Say β is a root in K. i.e. $\beta^2 + \alpha\beta + \alpha^2 = 0$. Let $\omega = \beta/\alpha$. Then $\omega^2 + \omega + 1 = 0$, but $x^2 + x + 1$ is irreducible over $\mathbb{Q}$. Thus $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ but $\omega \in K$ and $[K : \mathbb{Q}] = 3 (= \deg(x^3 - 2))$ but this is a contradiction by the Tower Law, $[K : \mathbb{Q}] = [K : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}]$.

Now define $E = K[x]/\langle x^2 + \alpha x + \alpha^2\rangle$, then E is a field. Let $\beta = x + \langle x^2 + \alpha x + \alpha^2\rangle$. so $\beta \in E$ is a root of $x^2 + \alpha x + \alpha^2$ get $x^-3 = (x - \alpha)(x - \beta)(x - \alpha^2/\beta) = (x - \alpha)(x - \omega)(x - \omega^2\alpha)$ with $\omega = \beta/\alpha$.

Proposition - Definition 28.18 (Algebraically Closed)**.** A field F is algebraically closed if one of the following equivalent conditions hold:

i) Any non-constant $p \in F[x]$ has a root in F.

ii) There are no non-trivial algebraic extensions of F.

Theorem 28.19. Let F be a field. There exists a "smallest" extension $\tilde{F}/F$ which is algebraically closed, called the algebraic closure of F. It is unique up to isomorphism.

29 Finite Fields

Definition 29.1 (Characteristic of a Ring)**.** Let R be a ring. Consider the homomorphism $\phi : \mathbb{Z} \to R; n \mapsto 1 + 1 + \cdots + 1 (n \text{times})$. Then $\ker \phi \trianglelefteq \mathbb{Z} = \langle n\rangle$ for some n. This is called the characteristic of R, $\operatorname{char} R$.

Example 29.2. $\operatorname{char} \mathbb{R} = 0, \operatorname{char} \mathbb{Z} = 0, \operatorname{char}(\mathbb{Z}/n\mathbb{Z}) = n$.

Definition 29.3. A finite field is a field with only finitely many elements.

Example 29.4. $\mathbb{Z}/p\mathbb{Z}$ if $p$is prime is a finite field.

Proposition 29.5. Let F be a finite field. Then $|F| = p^n$ for some prime p, integer $n \geq 1$. p is the characteristic of F. F contains $\mathbb{Z}/a/bZ$ as a subfield.

Proof. Let $n = \operatorname{char} F$. Since F finite, $n \neq 0$.

Claim. n is prime.

Proof. If $n = n_1 n_2$ then $0 = \phi(n) = \phi(n_1)(n_2)$. Since F is a field, either $\phi(n_1) = 0$ or $\phi(n_2) = 0$.

Call $p = n$. $\mathrm{Im}(\phi) = \{0, 1, 1+1, \ldots, p-1\}$. By First Isomorphism Theorem, $\mathrm{Im}\,\phi \cong \mathbb{Z}/\ker\phi = \mathbb{Z}/p\mathbb{Z}$. i.e. F contains $\mathbb{Z}/p\mathbb{Z}$ as a subfield. Also F is a vector space over $\mathbb{Z}/p\mathbb{Z}$ of finite dimension say t, so $|F| = p^t$, i.e. can write elements uniquely in form $c_1b_+ \cdots + c_nb_n$ where $c_i \in \mathbb{Z}/p\mathbb{Z}$ and b_i forms a basis for F over $\mathbb{Z}/p\mathbb{Z}$.

Theorem 29.6 (Existence of Finite Fields)**.** Let $p \geq 2$ be a prime, let $n \geq 1$. Then there exists a field F with $|F| = p^n$.

Proof. Let $q = p^n$. Let $g(x) = x^q - x \in \mathbb{F}_p[x]$. From the previous chapter, there eixsts a field extension $E/\mathbb{F}_p$ such that $g(x)$ splits into linear factors in $E[x]$. Define $F = \{\alpha \in E : g(\alpha) = 0\} = \{\alpha \in E : \alpha^q = \alpha\}$. Know $|F| \leq q$, since $g(x)$ has at most q roots.

Claim. $g(x)$ has no repeated roots.

Proof. If $g(x) = (x-a)^2h(x)$ for some $\alpha \in E, h \in E[x]$. Then $g'(x) = 2(x-\alpha)h(x) + (x-\alpha)2h(x)$. So $g'(\alpha) = 0$. But $g'(x) = qx^{q-1} - 1 = -1$, contradiction.

Therefore $|F| = q$. Need to show F is a subfield of E. If $\alpha, \beta \in F$ then $(\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta$ so $\alpha\beta \in F$.

$$\begin{aligned}
(\alpha+\beta)^p &= \alpha^p + \beta^p \\
(\alpha+\beta)^{p^2} &= \alpha^{p^2} + \beta^{p^2} \\
&\vdots \\
(\alpha+\beta)^q &= \alpha^q + \beta^q = \alpha + \beta
\end{aligned}$$

so $\alpha + \beta \in F$ and closed under addition and multiplication. Inverses $\alpha^{-1} = \alpha^{q-2}$ because $\alpha^{q-1} = 1$ if $\alpha \neq 0$.

Theorem 29.7 (Existence of Generators)**.** Let F = finite field order $q = p^n$. Then $F^*$is cyclic of order $q-1$.

Example 29.8. $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ with $\alpha^2 + \alpha + 1 = 0$. We have $\alpha^0 = 1, \alpha^1 = \alpha, \alpha^2 = \alpha + 1$ so $\mathbb{F}_4^* = \langle\alpha\rangle$.

Lemma 29.9. Let $m \in \mathbb{F}_p[x]$ be irreducible with $\deg n \geq 1$. Let $q = p^n$ then $m \mid x^q - x$.

Theorem 29.10. Let F, F' be finite fields. $|F| = |F'|$ then $F \cong F'$.

30 Ruler and Compass Constructions

Definition 30.1 (Admissible Towers)**.** Let $F = \mathbb{Q}(S_0) = \mathbb{Q}($ all x, y coordinates of points in $S_0)$ ($= \mathbb{Q}$ for some S_0). An admissible tower is a tower of extensions: $F = E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_n$ where $E_j \subseteq \mathbb{R}$, $[E_j : E_{j-1}] = 2$ for all j.

Theorem 30.2. Let $(x, y) \in S_i$. Then there exists an admissible tower $E_0 \subseteq \cdots \subseteq E_n$ such that $x, y \in E_n$.

Lemma 30.3. If $F_0 \subseteq \cdots F_n$ and $E_0 \subseteq \ldots E_n$ are admissible then there exists admissible $K_0 \subseteq \cdots \subseteq K_r$ such that $F_n \subseteq K_r$ and $E_m \subseteq K_r$.

Corollary 30.4. Let $(x, y) \in \mathbb{R}^2$ be constructible from S_0. Then $[F(x, y) : F] = 2^k$ for some k.