MATH3711 Lecture Notes*

typed by Charles Qin

June 2006

1 How Mathematicians Study Symmetry

Example 1.1. Consider an equilateral triangle with six symmetries. Rotations about O through angles 0, $\frac{2\pi}{3}$, $\frac{4\pi}{3}$ and three reflections about axial lines l_1, l_2, and l_3.

Definition 1.1 (Isometry). A function $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ is called an isometry if it preserves distance, i.e. $\|\mathbf{x} - \mathbf{y}\| = \|f(\mathbf{x}) - f(\mathbf{y})\|$ for any $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$.

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

Proposition 1.1. Let S, T be symmetries of some $F \subseteq \mathbb{R}^n$. The composite $ST : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ is also a symmetry of F.

Proof. Let us check that ST is an isometry for $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$. $\|ST\mathbf{x} - ST\mathbf{y}\| = \|T\mathbf{x} - T\mathbf{y}\|$ (S is an isometry) $= \|\mathbf{x}-\mathbf{y}\|$ (T is an isometry). So ST is an isometry. Also $ST(F) = S(F)$ (T is onto) $= F$ (S is onto). So ST is indeed a symmetry of F.

Let G be the set of symmetries of $F \subseteq \mathbb{R}^n$.

Proposition 1.2. G possesses the following properties:

(i) Composition of functions is associative, i.e. $(ST)R = S(TR)$

(ii) $\mathrm{id}_{\mathbb{R}^n} \in G$, recall $\mathrm{id}_{\mathbb{R}^n} T = T = T\mathrm{id}_{\mathbb{R}^n}$ for any $T \in G$

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

Proof. (i) and (ii) are fairly easy exercises. For (iii), we have that $T \in G$ is surjective by definition, so only need to check one to one. For $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, $T\mathbf{x} = T\mathbf{y} \Longrightarrow 0 = \|T\mathbf{x}-T\mathbf{y}\| = \|\mathbf{x}-\mathbf{y}\| \Longrightarrow \mathbf{x} = \mathbf{y}$. So T is bijective, and T^{-1} is surjective. T^{-1} is an isometry since for $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, $\|T^{-1}\mathbf{x} - T^{-1}\mathbf{y}\| = \|TT^{-1}\mathbf{x} - TT^{-1}\mathbf{y}\| = \|\mathbf{x} - \mathbf{y}\|$. Lastly $T^{-1}(F) = T^{-1}(T(F)) = F$. So $T^{-1} \in G$.

*The following notes were based on Dr Daniel Chan's MATH3711 lectures in semester 1, 2006

The proposition is used to motivate abstract definition of a group.

Definition 1.3 (Group). A group is a set G equipped with a map $\mu : G \times G \longrightarrow G$, where for $g, h \in G$, $\mu(g, h)$ is abbreviated to gh, called the multiplication map, satisfying the following axioms

(i) Associativity, i.e. $g, h, k \in G$, then $(gh)k = g(hk)$

(ii) Existence of identity, i.e. there is an element denoted by 1_G in F called identity of G such that $1_G g = g = g1_G$ for any $g \in G$

(iii) Existence of inverse, i.e. for any $g \in G$, there is an element denoted by $g^{-1} \in G$ called inverse of g such that $gg^{-1} = g^{-1}g = 1$

Example 1.2. For $F \subseteq \mathbb{R}^n$, the set G of symmetries of F, equipped with multiplication map equal to composition of functions is a group by Proposition 1.2. It has identity $1_G = \mathrm{id}_{\mathbb{R}^n}$ and the inverse in group is just the inverse function.

Proposition 1.3. Here are some properties of a group.

(i) When you multiply three or more elements in a group, it does not matter how you bracket the expression

(ii) Cancellation law, i.e. for elements g, h, k in a group, $gh = gk \Longrightarrow h = k$

Proof. (i) Mathematical induction as for matrix multiplication. (ii) By associative law, $gh = gk \Longrightarrow g^{-1}gh = g^{-1}gk \Longrightarrow h = k$.

2 Matrix Groups

Let $GL_n(\mathbb{R})$ and $GL_n(\mathbb{C})$ be the set of real and complex invertible $n \times n$ matrices respectively. Note that we will often identify matrices with the linear transformations they represent.

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

Proof. Note that product of invertible matrices is an invertible matrix. Just check axioms. (i) Matrix multiplication is associative. (ii) Identity matrix I_n satisfies $I_n M = M = M I_n$ for any $M \in GL_n(\mathbb{R})$. So $GL_n(\mathbb{R})$ has identity $1 = I_n$. (iii) For $M \in GL_n(\mathbb{R})$, $M^{-1} \in GL_n(\mathbb{R})$ satisfies $MM^{-1} = I_n = M^{-1}M$ where $I_n \in G$. So inverses exist too and $GL_n(\mathbb{R})$ is a group.

As for matrix multiplication, we have ...

Proposition 2.2. In a group G

(i) The identity is unique, i.e. if $1, e \in G$ satisfy $1g = g = g1$ and $eg = g = ge$ for all $g \in G$, then $1 = e$

(ii) Inverses are unique

(iii) For $g, h \in G$, $(gh)^{-1} = h^{-1}g^{-1}$

Proof. (i) By definition, $1 = 1e = e$. (ii) Suppose a, b are inverses of h, then using associative law, $a = a1_G = a(hb) = (ah)b = 1_G b = b$. (iii) Also using associative law, $(h^{-1}g^{-1})(gh) = h^{-1}(g^{-1}g)h = h^{-1}1h = 1 = g1g^{-1} = ghh^{-1}g^{-1} = (gh)(h^{-1}g^{-1})$. Thus by uniqueness of inverse in (ii), $(gh)^{-1} = h^{-1}g^{-1}$.

Definition 2.1 (Subgroup). Let G be a group. A subset $H \subseteq G$ is said to be a subgroup of G, denoted by $H \leq G$, if it satisfies the following axioms.

(i) Existence of identity, $1_G \in H$

(ii) Closure under multiplication, i.e. if $h, k \in H$, then $hk \in H$

(iii) Closure under inverse, i.e. if $h \in H$, then $h^{-1} \in H$

Proposition 2.3. In this case, we have an induced multiplication map $\mu_H : H \times H \longrightarrow H$, such that $(h, k) \in H \times H \Longrightarrow hk \in H$ by Definition 2.1 (ii), which makes H into a group.

Proof. Just check axioms. (i) μ_H is associative since μ is, i.e. $(gh)k = g(hk)$. (ii) For any $h \in H$, $1_G h = h = h1_G$, so $1_G = 1_H$, i.e. identity exists. (iii) For $h \in H$, its inverse h^{-1} in G lies in H by Definition 2.1 (iii). Since $hh^{-1} = 1_G = 1_H = h^{-1}h$, the inverse in H is inverse in G. Hence the inverse exists and the result is proved.

Proposition - Definition 2.1. Set of orthogonal matrices $O_n(\mathbb{R}) = \{M \in GL_n(\mathbb{R}) : M^T = M^{-1}\} \lneqq GL_n(\mathbb{R})$ forms a group, namely the set of symmetries of an $n-1$ sphere, i.e. an n dimensional circle.

Proof. Check axioms. (i) Know $I_n \in O_n(\mathbb{R})$. (ii) For $M, N \in O_n(\mathbb{R})$, have $(MN)^T = N^T M^T = N^{-1}M^{-1} = (MN)^{-1}$. So have closure under multiplication. (iii) For $M \in O_n(\mathbb{R})$, $(M^{-1})^T = (M^T)^T = M = (M^{-1})^{-1}$. So closed under inverses. Since $O_n(\mathbb{R}) \subsetneqq GL_n(\mathbb{R})$, we have a subgroup.

Proposition 2.4. Other basic observations include

(i) Any group G has two trivial subgroups, namely G and $1 = \{1_G\}$

(ii) If $H \leq G$ and $J \leq H$, then $J \leq G$

Proof. Similarly check axioms ...

Here are some notations. Given group G and $g \in G$, write

(i) $g^n = gg \dots g$ (n times), $n \in \mathbb{Z}^+$

(ii) $g^0 = 1_G$

(iii) $g^{-n} = (g^{-1})^n = (g^n)^{-1}$ (proof by mathematical induction)

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

Definition 2.2. The order of a group G, denoted $|G|$, is the number of elements in G. For $g \in G$, the order of g is the smallest integer n such that $g^n = 1$. Say infinite order if no such n exists.

Example 2.1. $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in GL_2(\mathbb{R})$ has order 2. More generally any reflection has order 2.

3 Permutation Groups

Definition 3.1 (Permutation). Let S be a set. The set of permutations on S, $\mathrm{Perm}(S)$ is the set of bijections of the form $\sigma : S \longrightarrow S$.

Proposition 3.1. $\mathrm{Perm}(S)$ is a group when endowed with composition of functions for multiplication.

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

Definition 3.2. If $S = \{1, 2, \ldots, n\}$, then the symmetric group (set of symmetries) on the n symbols is $\mathrm{Perm}(S)$ and is denoted by S_n.

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

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

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

Example 3.1. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \in S_4$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} \in S_4$. We have $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$ and $\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$. Note that $\sigma\tau(1) = \sigma(4) = 4$, $\sigma\tau(2) = \sigma(2) = 3$, $\sigma\tau(3) = \sigma(3) = 1$, $\sigma\tau(4) = \sigma(1) = 2$.

With the cyclic notation, let $s_1, s_2, \ldots, s_k \in S$ be distinct. We will 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 $s \notin \{s_1, s_2, \ldots, s_k\}$. This permutation is denoted by $(s_1 s_2 \ldots s_k)$ and is called a k-cycle.

Example 3.2. For Example 3.1, σ does $1 \longmapsto 2 \longmapsto 3 \longmapsto 1$ and 4 fixed. So we have 3-cycle $\sigma = (123)$. τ does $1 \longmapsto 4 \longmapsto 1$ and 2, 3 fixed. So we have 2-cycle $\tau = (14)$.

Note that an 1-cycle is the identity. The order of a k-cycle σ is k, i.e. rotate k times before getting back to the original position. So $\sigma^k = 1$ and $\sigma^{-1} = \sigma^{k-1}$.

Definition 3.3 (Disjoint Cycles). Cycles $(s_1 s_2 \ldots s_k)$ and $(t_1 t_2 \ldots t_l)$ are disjoint if $\{s_1, s_2, \ldots, s_k\} \cap \{t_1, t_2, \ldots, t_l\} = \emptyset$.

Definition 3.4 (Commutativity). Two elements g, h in a group are said to commute if $gh = hg$.

Proposition 3.2. Disjoint cycles commute.

Proof. Clear from any example such as $g = (12)$, $h = (34)$. Then gh and hg both do $1 \longmapsto 2 \longmapsto 1$, $3 \longmapsto 4 \longmapsto 3$, i.e. swaps irrelevant of order. So $gh = hg$.

Proposition 3.3. For S, a finite set, any $\sigma \in \text{Perm}(S)$ is a product of disjoint cycles.

Example 3.3. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 5 & 3 \end{pmatrix}$ does $1 \longmapsto 2 \longmapsto 4 \longmapsto 1$, $3 \longmapsto 6 \longmapsto 3$ and 5 fixed. $\therefore$ $\sigma = (124)(36)$ since (5) is the identity.

Proposition 3.4. Let S be a finite set and $\sigma \in \text{Perm}(S)$ then S is a disjoint union of certain subsets $S_1, S_2, \ldots, S_n$ such that σ permutes elements of S_i cyclically for each i, i.e. $\sigma = (s_1\sigma(s_1)\sigma^2(s_1)\ldots)(s_2\sigma(s_2)\sigma^2(s_2)\ldots)\ldots(s_r\sigma(s_r)\sigma^2(s_r)\ldots)$ for s_i being an element of S_i.

Definition 3.5 (Transposition). A transposition is a 2-cycle.

Proposition 3.5. Two important observations

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

(ii) Any permutation of a finite set is a product of transpositions

Proof. (i) The right hand side does the following: $s_1 \longmapsto s_2$ (consider the first transposition); $s_2 \longmapsto s_1 \longmapsto s_3$ (the first two transpositions); $s_3 \longmapsto s_1 \longmapsto s_4$ (the second two transpositions); $\ldots$; $s_k \longmapsto s_1$ (the last transposition). This is the same as $(s_1 s_2 \ldots s_k)$ as desired. (ii) By Proposition 3.4, $\sigma \in \text{Perm}(S)$ has form $\sigma = \sigma_1\sigma_2\ldots\sigma_r$ with σ_i cycles. But by (i), each cycle is a product of transpositions, and so can rewrite each σ_i as product of transpositions, hence giving (ii).

4 Generators & Dihedral Groups

Lemma 4.1. Let $\{H_i\}_{i\in I}$ be a set of subgroups of a group G. Then $\bigcap_{i\in I} H_i \leq G$.

Proof. Same as for subspaces. Just check axioms. For example, with closure under multiplication, if $h, h' \in \bigcap_{i\in I} H_i$, then $h, h' \in H_i$ for every i. But $H_i \leq G \implies hh' \in H_i$ for every i by closure under groups. Hence $hh' \in \bigcap_{i\in I} H_i$ as desired.

Proposition - Definition 4.1. Let G be a group and $S \subseteq G$. Let J be the set of subgroups $j \leq G$ containing S.

(i) The subgroup generated by S is $\langle S\rangle = \bigcap_{j\in J} \leq G$, i.e. it is the unique smallest subgroup of G containing S.

(ii) $\langle S\rangle$ is the set of elements of the form $g = s_1 s_2 \ldots s_n$ where $s_i \in S$ and $n \geq 0$; define $g = 1$ when $n = 0$.

Proof. (i) Follows from Lemma 4.1 that $\bigcap_{j\in J} j \leq G$. (ii) Let H be the set of elements of form $g = s_1 s_2 \ldots s_n$. Closure axioms $\implies H \leq j$, $\forall j \in J$. $\therefore H \subseteq \langle S\rangle = \bigcap_{j\in J} j$. Suffice to show that $H \supseteq \langle S\rangle$, or by part (i) that H is a subgroup containing S. $H \supseteq S$ by definition. So only need to check $H \leq G$ by checking axioms. For example, suppose $s_1, s_2, \ldots, s_n$ as in $g = s_1 s_2 \ldots s_n$, then $(s_1 s_2 \ldots s_n)^{-1} = s_n^{-1} s_{n-1}^{-1} \ldots s_1^{-1} \in H$ since $s_i^{-1} \in S\ \forall\ i$. So H is closed under inverses. H is closed under multiplication by the associative law, i.e. $s_1 s_2 \ldots s_m, t_1 t_2 \ldots t_n \in H \implies (s_1 s_2 \ldots s_m)(t_1 t_2 \ldots t_n) = s_1 s_2 \ldots s_m t_1 t_2 \ldots t_n \in H$. Finally, $s, s^{-1} \in S \neq \emptyset \implies ss^{-1} = 1_G \in H$. So we have the identity.

Definition 4.1 (Finitely Generated & Cyclic Groups). A group G is finitely generated if there is a finite set $S \subseteq G$ such that $G = \langle S \rangle$. We say G is cyclic if furthermore we can take S to be an one element set, i.e. generated by one element.

Example 4.1. Find the subgroup generated by $\sigma = \begin{pmatrix} \cos(\frac{2\pi}{n}) & -\sin(\frac{2\pi}{n}) \\ \sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{pmatrix} \in GL_2(\mathbb{R})$ and $\tau = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ for integers $n \geq 2$. These are both symmetries of a regular n-gon. Note symmetries of regular n-gon are either rotations or reflections. Any element of $\langle \sigma, \tau \rangle$ has form $\sigma^{i_1}\tau^{j_1}\sigma^{i_2}\tau^{j_2}\ldots\sigma^{i_r}\tau^{j_r}$. Note it must be finite. But we have relations $\sigma^n = 1 = \tau^2$. So we may as well assume $i_1, i_2, \ldots, i_r \in \{0, 1, \ldots, n-1\}$ and $j_1, j_2, \ldots, j_r \in \{0, 1\}$ through multiplications of appropriate numbers $\sigma^n, \sigma^{-n}, \tau^2, \tau^{-2}$. Also it is easily checked that $\tau\sigma\tau^{-1} = \sigma^{-1}$. Thus we get skew commutativity $\tau\sigma = \sigma^{-1}\tau$. Hence we have

$$\begin{aligned} \tau\sigma^i &= \tau\underbrace{\sigma\sigma\ldots\sigma}_{i} \\ &= \sigma^{-1}\tau\underbrace{\sigma\sigma\ldots\sigma}_{i-1} \\ &= \sigma^{-2}\tau\underbrace{\sigma\sigma\ldots\sigma}_{i-2} \\ &= \ldots \\ &= \sigma^{-i}\tau \end{aligned}$$

Proposition - Definition 4.2. $\langle \sigma, \tau \rangle$ is the dihedral group. It is denoted by D_n. Its elements are $D_n = \{1, \sigma, \ldots, \sigma^{n-1}, \tau, \sigma\tau, \ldots, \sigma^{n-1}\tau\}$ and $|D_n| = 2n$.

Proof. Note $\tau\sigma^i = \sigma^{-i}\tau$ allows us to put all τ's to the right without changing the number of total τ's in the expression. So push all the τ's in $\sigma^{i_1}\tau^{j_1}\sigma^{i_2}\tau^{j_2}\ldots\sigma^{i_r}\tau^{j_r}$ to the right. This shows that elements in D_n have form above. It remains only to show that they are distinct. Now $\det(\sigma^i) = 1$ and $\det(\sigma^i\tau) = -1$ for all i. By cancellation law, to show $\sigma^i\tau$'s are distinct is same as showing σ^i, $i = 0, 1, 2, \ldots, n-1$ are distinct. But these are easily seen to be distinct rotations through matrix multiplication.

We will see D_n is the complete group of symmetries of a regular n-gon.

5 Alternating & Abelian Groups

Let f be a real valued function in n real variables.

Definition 5.1 (Symmetric Function). Let $\sigma \in S_n$. We define a new function $\sigma.f$ as follow: $\sigma.f(x_1, x_2, \ldots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$. We say f is symmetric if $\sigma.f = f$ for any $\sigma \in S_n$.

Example 5.1. $f(x_1, x_2, x_3) = x_1^3x_2^2x_3$ and $(12).f(x_1, x_2, x_3) = x_2^3x_1^2x_3$. $\therefore f$ is not symmetric. But $f(x_1, x_2) = x_1^2x_2^2$ is symmetric in two variables.

Definition 5.2 (Difference Product). The difference product in n variables is $\Delta(x_1, x_2, \ldots, x_n) = \prod_{i<j}(x_i - x_j)$.

Example 5.2. For $n = 2$, $\Delta = x_1 - x_2$ is not symmetric. But what symmetries does it have?

Lemma 5.1. Let $f(x_1, x_2, \ldots, x_n)$ be a real valued function in n real values. If $\sigma, \tau \in S_n$, then $(\sigma\tau).f = \sigma.(\tau.f)$.

Proof.

$$\begin{aligned}
(\sigma.(\tau.f))(x_1, x_2, \ldots, x_n) &= (\tau.f)(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) \quad \text{(by definition)} \\
&= f(y_{\tau(1)}, y_{\tau(2)}, \ldots, y_{\tau(n)}) \quad (\text{where } y_i = x_{\sigma(i)}) \\
&= f(x_{\sigma(\tau(1))}, x_{\sigma(\tau(2))}, \ldots, x_{\sigma(\tau(n))}) \\
&= f(x_{(\sigma\tau)(1)}, x_{(\sigma\tau)(2)}, \ldots, x_{(\sigma\tau)(n)}) \\
&= ((\sigma\tau).f)(x_1, x_2, \ldots, x_n)
\end{aligned}$$

Proposition - Definition 5.1 (Odd & Even Permutations). Let $\sigma \in S_n$. Write $\sigma = \tau_1\tau_2 \ldots \tau_m$, with τ_i's transpositions. Then

$$\sigma.\Delta = \begin{cases} \Delta & \text{if } m \text{ is even (say that } \sigma \text{ is an even permutation)} \\ -\Delta & \text{if } m \text{ is odd (say that } \sigma \text{ is an odd permutation)} \end{cases}$$

Proof. Need only to prove $m = 1$ case, for then Lemma 5.1 implies that

$$\sigma.\Delta = \tau_1(\tau_2(\tau_3 \ldots (\tau_{m-1}(\tau_m.\Delta)) \ldots)) = \tau_1((-1)^{m-1}\Delta) = (-1)^m\Delta \quad \text{(by induction)}$$

So we mat assume $\sigma = (ij)$ with $i < j$. Examine three cases. (1) $\sigma(x_i - x_j) = x_j - x_i = -(x_i - x_j)$. (2) For i, j, r, s distinct, $\sigma(x_r - x_s) = x_r - x_s$. (3) For i, j, r distinct, we have three more cases. (i) $r < i < j$, $\sigma.(x_r - x_i)(x_r - x_j) = (x_r - x_j)(x_r - x_i)$, i.e. no change. (ii) $i < r < j$, $\sigma.(x_i - x_r)(x_r - x_j) = (x_j - x_r)(x_r - x_i) = (x_i - x_r)(x_r - x_j)$. (iii) $i < j < r$, $\sigma.(x_i - x_r)(x_j - x_r) = (x_j - x_r)(x_i - x_r)$. So no changes in (i), (ii) and (iii). Multiply (1), (2) and (3) together to find $\sigma.\Delta = -\Delta$.

Corollary 5.1. Even permutations are products of even number of transpositions and odd permutations are products of odd number of permutations.

Proposition - Definition 5.2 (Alternating Group). The alternating group is $A_n = \{\sigma \in S_n : \sigma.\Delta = \Delta\}$ which is the subgroup of S_n generated by $\{\tau_1\tau_2 : \tau_1, \tau_2 \text{ transpositions}\}$.

Proof. Just note $(\tau_1\tau_2)^{-1} = \tau_2^{-1}\tau_1^{-1} = \tau_2\tau_1$ since inverse of a transposition is itself. Since the inverses do not add anything new to the generating set, we have $\{\tau_1\tau_2 : \tau_1, \tau_2 \text{ transpositions}\}$ generates all functions of the form $\tau_1\tau_2 \ldots \tau_m$ where m is even.

Proposition 5.1. Group of symmetries of anti-symmetric functions is A_n.

Definition 5.3 (Abelian Group). A group G is abelian or commutative if any two elements commute.

Example 5.3. $G = \mathbb{Z}$ is an abelian group when endowed with group multiplication equal to addition. The identity is 0 and the group inverse of m is $-m$.

Often for abelian groups, we switch notation and terminology as below.

(i) Product gh to sum $g + h$

(ii) Identity 1 to zero 0

(iii) g^n to ng

(iv) Inverse g^{-1} to negative $-g$

Example 5.4. Let V be a vector space. it is an abelian group under its additive structure. Also any subspace is a subgroup.

Example 5.5. Let F be a field, e.g. $\mathbb{C}, \mathbb{R}, \mathbb{Q}$, then $F^* = F - \{0\}$ is an abelian group with multiplication in the group equal to usual multiplication in the field.

Example 5.6. For $\{1, -1\} \leq \mathbb{R}^*$, the multiplication table is

$\times$	1	-1
1	1	-1
-1	-1	1

6 Cosets & Lagrange's Theorem

Let $H \leq G$ be a subgroup.

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

Example 6.1. Let $H = A_n \leq S_n = G$ for the alternating group for $n \geq 2$. Let τ be a transposition. We claim that τA_n is the set of odd permutations. To prove this, we see that elements of τA_n have form $\tau\sigma$ where σ is a product of an even number of transpositions. So $\tau\sigma$ is an odd number of transpositions. Suppose conversely, $\rho \in S_n$ is odd. Then $\rho = \tau^2\rho = \tau(\tau\rho)$ since $\tau^2 = 1$ for transposition τ. But $\tau\rho$ is product of even number of transpositions. Hence $\rho = \tau(\tau\rho) \in \tau A_n$ and this proves the claim.

Example 6.2. Let $G = \mathbb{Z}$. The set of multiples of m, $m\mathbb{Z}$, is a subgroup of $\mathbb{Z}$. Using addition notation, the left cosets are $r + m\mathbb{Z} = \{r + mq : q \in \mathbb{Z}\}$, the set of integers whose remainder on dividing by m is r. Using this notation, $2\mathbb{Z}$ is the set of even integers and $1 + 2\mathbb{Z}$ is the set of odd integers.

Theorem 6.1. Let $H \leq G$. We define a relation on G by $g \equiv g'$ if and only if $g \in g'H$. Then $\equiv$ is an equivalent relation with equivalence classes, the left cosets of H. Hence $G = \dot{\bigcup}_{i \in I} g_i H$ (disjoint union) for some $g_i \in G$.

Proof. Let us check reflexivity. $g = g1 \in gH$ since $1 \in H$ for subgroup H. $\therefore g \equiv g$. Symmetry, suppose $g \equiv g'$, so $g = g'h$ for some $h \in H$. Now $g' = gh^{-1} \in gH$ as a subgroup is closed under inverses, thus $g' \equiv g$. For transitivity, suppose $g \equiv g'$, $g' \equiv g''$. Say $g = g'h$, $g' = g''h'$ where $h, h' \in H$. $\therefore g = g'h = g''h'h \in g''H$ due to closure under multiplication of a subgroup, i.e. $g \equiv g''$. This completes the proof of the theorem. Note that subgroup properties of existence of identity, closures under inverses and products give the respective properties of reflexivity, symmetry and transitivity.

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

Example 6.3. $H = A_n \leq S_n = G$. $S_n = A_n \dot{\cup} \tau A_n$, ,i.e. union of the set of even and odd permutations, where τ is an odd permutation, e.g. a transposition.

Lemma 6.1. Let $H \leq G$. Then for any $g \in G$, H and gH have the same cardinality.

Proof. Cancellation laws implies that map $\pi : H \longrightarrow gH$; $h \longmapsto gh$ is injective, i.e. $gh = gh' \Longrightarrow h = h'$. It is clearly surjective by definition. So it is bijective and we see that any two cosets of H have the same cardinality.

Definition 6.2 (Index Of Subgroup). Let $H \leq G$. The index of H in G is the number of left of cosets of H in G. It is denoted by $[G : H]$.

Theorem 6.2 (Lagrange's Theorem). Let $H \leq G$, where G is finite. Then $|G| = |H|[G : H]$, i.e. $[G : H] = |G/H| = \frac{|G|}{|H|}$. So in particular, $|H|$ divides $|G|$.

Proof. By Theorem 6.1 and Lemma 6.1, we have

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

Example 6.4. Again $A_n \leq S_n$. $[S_n : A_n] = 2$. $\therefore |A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$, i.e. half of the permutations are odd, the half even.

In the problem sheets, there is a right handed version of everything above. Right cosets have form $Hg = \{hg : h \in H\}$. Set of these is denoted by $H \backslash G$. All theorems and lemmas hold for these right cosets. Also the number of left cosets equal the number of right cosets always.

7 Normal Subgroups & Quotient Groups

Study of a group G may be done by studying some $H \leq G$ and G/H. This however requires G/H to be a group also. Suppose G is some group and $J, K \leq G$. Then the subset product is $JK = \{jk : j \in J, k \in K\} \subseteq G$.

Proposition 7.1. Let G be a group.

(i) If $J' \subseteq J \subseteq G$, $K \subseteq G$, then $KJ' \subseteq KJ$

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

(iii) For $J, K, L \subseteq G$, we have $(JK)L = J(KL)$

Proof. (i) is clear. (ii) $H = 1H \subseteq HH$ by (i), since $1 \subseteq H$ and $HH \subseteq H$ by closure under products for $H \leq G$. (iii) Using associativity of products in G, $(JK)L = J(KL) = \{jkl : j \in J, k \in K, l \in L\}$.

Proposition - Definition 7.1 (Normal Subgroup). Let $N \leq G$. The following conditions on N are equivalent.

(i) $gN = Ng$ for all $g \in G$, i.e. left coset equals right coset

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

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

(iv) We say N is a normal subgroup of G and denote this by $N \trianglelefteq G$

Proof. (i) $\implies$ (ii) $gN = Ng \implies g^{-1}gN = g^{-1}Ng \implies N = 1N = g^{-1}Ng$. (ii) $\implies$ (i) is similar by reversing the steps. It only remains to show (iii) $\implies$ (ii) since (ii) $\implies$ (iii) is obvious. Suppose $g^{-1}Ng \subseteq N$ then $gg^{-1}Ngg^{-1} \subseteq gNg^{-1} \implies N \subseteq gNg^{-1} = (g^{-1})^{-1}Ng^{-1}$. But as g runs through all of G, g^{-1} also runs through all of G. Hence $N \subseteq g^{-1}Ng$ for all g too and so (iii) $\implies$ (ii).

Example 7.1. If G is abelian, then any subgroup N is normal since $gH = Hg$ is always true due to commutativity.

Example 7.2. Matrix computation. Consider $\begin{pmatrix} a_1 & * & * & \dots & * \\ 0 & a_2 & * & \dots & * \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & a_n \end{pmatrix} \begin{pmatrix} b_1 & * & * & \dots & * \\ 0 & b_2 & * & \dots & * \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & b_n \end{pmatrix} = \begin{pmatrix} a_1b_1 & * & * & \dots & * \\ 0 & a_2b_2 & * & \dots & * \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & a_nb_n \end{pmatrix}$ and $\begin{pmatrix} a_1 & * & * & \dots & * \\ 0 & a_2 & * & \dots & * \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & a_n \end{pmatrix}^{-1} = \begin{pmatrix} a_1^{-1} & * & * & \dots & * \\ 0 & a_2^{-1} & * & \dots & * \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & a_n^{-1} \end{pmatrix}$ We have $B = \{M \in GL_n(\mathbb{C}) : M \text{ is upper triangular}\} \leq GL_n(\mathbb{C})$ (check axioms). The set of unipotent matrices, $U = \{M \in B : \text{generalised eigenvalues are all 1, i.e. only 1's on the diagonal of } M\} \leq B$

(check axioms). Now we have $\begin{pmatrix} a_1 & 0 & 0 & \dots & 0 \\ 0 & a_2 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & a_n \end{pmatrix} U =$ set of $\begin{pmatrix} a_1 & * & * & \dots & * \\ 0 & a_2 & * & \dots & * \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & a_n \end{pmatrix}$, where $\begin{pmatrix} a_1 & 0 & 0 & \dots & 0 \\ 0 & a_2 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & a_n \end{pmatrix} \in GL_n(\mathbb{C})$ multiplies row i of matrices of U by a_i. We also have that $U \begin{pmatrix} a_1 & 0 & 0 & \dots & 0 \\ 0 & a_2 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & a_n \end{pmatrix} =$ set of $\begin{pmatrix} a_1 & * & * & \dots & * \\ 0 & a_2 & * & \dots & * \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & a_n \end{pmatrix}$, where $\begin{pmatrix} a_1 & 0 & 0 & \dots & 0 \\ 0 & a_2 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & a_n \end{pmatrix} \in GL_n(\mathbb{C})$ multiplies column i of matrices of U by a_i. Hence all left and right cosets of U in B coincide, and $U \trianglelefteq B$. Note that $U \not\trianglelefteq GL_n(\mathbb{C})$.

Proposition - Definition 7.2 (Quotient Group). Let $N \trianglelefteq G$ then subset multiplication is a well defined multiplication map on G/N which makes G/N a group. It is called the quotient group. Furthermore, for $g, g' \in G$, we have

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

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

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

Proof. (i) By Proposition 7.1, we have both closure and associativity of multiplication, i.e. subset product of cosets is a coset and multiplication is well defined. $(gN)(g'N) = g(Ng')N = gg'NN = gg'N$. (ii) Using (i), $NgN = 1NgN = (1g)N = gN \implies N = 1_{G/N}$. (iii) $(gN)(g^{-1}N) = gg^{-1}N = 1N = N = 1_{G/N}$ and $(g^{-1}N)(gN) = g^{-1}gN = 1N = N = 1_{G/N}$. So inverse exist with $(gN)^{-1} = g^{-1}N$. Hence G/N is a group.

Example 7.3. Multiplication in B/U. Cosets of U are of the form $\{\begin{pmatrix} a_1 & * & * & \dots & * \\ 0 & a_2 & * & \dots & * \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & a_n \end{pmatrix}\} \implies \{\begin{pmatrix} a_1 & * & * & \dots & * \\ 0 & a_2 & * & \dots & * \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & a_n \end{pmatrix}\}\{\begin{pmatrix} b_1 & * & * & \dots & * \\ 0 & b_2 & * & \dots & * \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & b_n \end{pmatrix}\} = \{\begin{pmatrix} a_1b_1 & * & * & \dots & * \\ 0 & a_2b_2 & * & \dots & * \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & a_nb_n \end{pmatrix}\}$, i.e. closure under multiplication.

Example 7.4. Let $m \in \mathbb{Z}^+$. $\mathbb{Z} \trianglerighteq m\mathbb{Z}$ since $\mathbb{Z}$ is abelian. $\mathbb{Z}/m\mathbb{Z} = \{m\mathbb{Z}, 1 + m\mathbb{Z}, \dots, (m-1) + m\mathbb{Z}\} = \{\overline{0}, \overline{1}, \dots, \overline{m-1}, \}$. Note G is abelian, so G/N is also an abelian group by Proposition -

Definition 7.2. What is addition in the quotient group $\mathbb{Z}/m\mathbb{Z}$?

$$\begin{aligned}\overline{i}+\overline{j} &= (i+m\mathbb{Z})+(j+m\mathbb{Z}) \\ &= (i+j)+m\mathbb{Z} \\ &= \begin{cases} \overline{i+j} & \text{if } i+j<m \\ \overline{i+j-m} & \text{if } i+j\geq m \end{cases}\end{aligned}$$

This recovers modulo arithmetic.

Example 7.5. Let $G=\mathbb{R}^3$ and $N \trianglelefteq G$, where N is the "$z=0$" plane. Cosets have form $(0,0,a)+N$, i.e. "$z=a$" plane. In G/N, we have partition of "$z=a$" planes. Addition is "$z=a$" plane + "$z=b$" plane = "$z=a+b$" plane.

8 Group Homomorphisms I

Example 8.1. Let $G=\{\sigma \in S_4 : \sigma(4)=4\} \leq S_4$. G looks like S_3, but technically $G \neq S_3$.

Example 8.2. Consider groups $\{1,-1\} \leq \mathbb{R}^*$ and $\mathbb{Z}/2\mathbb{Z}$, with multiplication tables

$\times$	1	-1
1	1	-1
-1	-1	1

and

$+$	$2\mathbb{Z}$	$1+2\mathbb{Z}$
$2\mathbb{Z}$	$2\mathbb{Z}$	$1+2\mathbb{Z}$
$1+2\mathbb{Z}$	$1+2\mathbb{Z}$	$2\mathbb{Z}$

. If we identify $1 \longleftrightarrow 2\mathbb{Z}$ and $-1 \longleftrightarrow 1+2\mathbb{Z}$, then the multiplication tables are the same. We wish to say that the groups are essentially the same. More generally, we want to be able to compare groups.

Definition 8.1 (Homomorphism). For groups H, G, a function $\phi : H \longrightarrow G$ is a group homomorphism if for any $h, h' \in H$, we have $\phi(hh')=\phi(h)\phi(h')$.

Note that group homomorphisms are structure preserving maps like linear transformations of vector spaces.

Example 8.3. $\phi = \det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$ is an homomorphism, i.e. $\det(AB)=\det(A)\det(B)$ for all $A, B \in GL_n(\mathbb{R})$.

Example 8.4. $\exp : \mathbb{R} \longrightarrow \mathbb{R}^*$ is an homomorphism, since $e^{a+b}=e^a e^b \ \forall\ a,b \in \mathbb{R}$. Note that in $\mathbb{R}$, the group multiplication is addition, while in $\mathbb{R}^*$, it is multiplication.

Example 8.5. A linear map $T : U \longrightarrow V$ is an homomorphism of the underlying abelian group, i.e. $T(\mathbf{x}+\mathbf{x})=T(\mathbf{x})+T(\mathbf{y})$.

Example 8.6. $\phi : \{1,-1\} \longrightarrow \mathbb{Z}/2\mathbb{Z}; 1 \longmapsto 2\mathbb{Z}; -1 \longmapsto 1+2\mathbb{Z}$ is an homomorphism in Example 8.2.

Proposition - Definition 8.1 (Isomorphism & Automorphism). Let $\phi : H \longrightarrow G$ be a group homomorphism. The following are equivalent.

(i) There exists an homomorphism $\psi : G \longrightarrow H$ such that $\psi\phi = \mathrm{id}_H$ and $\phi\psi = \mathrm{id}_G$.

(ii) ϕ is bijective.

In this case, we say ϕ is an isomorphism or G and H are isomorphic. Write $G \cong H$. If $H = G$, in this case, we say ϕ is an automorphism.

Proof. (i) $\implies$ (ii) clear due to existence of inverse. (ii) $\implies$ (i), suffice to show $\psi = \phi^{-1}$ is a group homomorphism, i.e for $g, g' \in G$, need to show $\phi^{-1}(gg') = \phi^{-1}(g)\phi^{-1}(g') \iff gg' = \phi(hh')$ (where $h = \phi^{-1}(g), h' = \phi^{-1}(g')) \iff \phi(h)\phi(h') = \phi(hh')$. This is clearly true as ϕ is an homomorphism.

Example 8.7. In Example 8.2, $\phi : \{1, -1\} \longrightarrow \mathbb{Z}/2\mathbb{Z}$ is an isomorphism.

Example 8.8. $\mathrm{id}_G : G \longrightarrow G$ is an automorphism.

Example 8.9. Recall from Example 7.2 that $U = \{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{C}\} \leq GL_2(\mathbb{C})$ (set of unipotent matrices). Claim $\phi : \mathbb{C} \longrightarrow U; a \longmapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ is an isomorphism. Why? Clearly ϕ is bijective. Suffice to check it is an homomorphism, i.e. for any $a, b \in \mathbb{C}$, $\phi(a + b) = \phi(a)\phi(b)$. LHS $= \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$ and RHS $= \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$. So study properties of group U is the same as studying group $\mathbb{C}$.

Proposition 8.1. Let $\phi : H \longrightarrow G$ be a group homomorphism. Then

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

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

(iii) If $H' \leq H$ then $\phi(H') \leq G$

Proof. (i) $1_G\phi(1_H) = \phi(1_H) = \phi(1_H 1_H) = \phi(1_H)\phi(1_H) \implies 1_G = \phi(1_H)$ (cancellation law). (ii) $\phi(h)\phi(h^{-1}) = \phi(hh^{-1}) = \phi(1_H) = 1_G$ from (i). $\therefore \phi(h^{-1}) = (\phi(h))^{-1}$ by uniqueness of inverses. (iii) just check axioms. $1_G = \phi(1_H) \in \phi(H')$ as $1_H \in H'$. Let $h, h' \in H'$. So $\phi(h)\phi(h') = \phi(hh') \in \phi(H')$ as $hh' \in H'$ due to closure of subgroups. Since $\phi(h)$ and $\phi(h')$ are any elements of $\phi(H')$, we have closure under multiplication. Also $(\phi(h))^{-1} = \phi(h^{-1}) \in \phi(H')$ as $h^{-1} \in H'$, i.e. closure under inverses in subgroups. Thus we have closure under inverses and $\phi(H') \leq G$.

Proposition 8.2. If $\psi : I \longrightarrow H$ and $\phi : H \longrightarrow G$ are group homomorphisms then $\phi\psi : I \longrightarrow G$ is also an homomorphism.

Proposition - Definition 8.2 (Conjugate). Let G be a group and $g \in G$. We define conjugate by g to be the function $C_g : G \longrightarrow G; h \longmapsto ghg^{-1}$. Then C_g is an automorphism with inverse $C_{g^{-1}}$. Let $H \leq G$ and $g \in G$. Then $C_g(H) = gHg^{-1} \leq G$ is called the conjugate of H.

Proof. Check first C_g is an homomorphism. For $h, h' \in G$, $C_g(hh') = ghh'g^{-1} = ghg^{-1}gh'g^{-1} = C_g(h)C_g(h')$. Now check $C_{g^{-1}}$ is the inverse. $C_{g^{-1}}C_g(h) = C_{g^{-1}}(ghg^{-1}) = g^{-1}ghg^{-1}(g^{-1})^{-1} = h$. This holds for all g, so we are done.

Proposition 8.3. Let $f : S \longrightarrow T$ be a bijection of sets. Then $\mathrm{Perm}(S) \cong \mathrm{Perm}(T)$.

Proof. Show there is an isomorphism $\phi : \mathrm{Perm}(S) \longrightarrow \mathrm{Perm}(T); \sigma \longmapsto f \circ \sigma \circ f^{-1}$ with inverse $\phi^{-1} : \mathrm{Perm}(T) \longrightarrow \mathrm{Perm}(S); \tau \longmapsto f^{-1} \circ \tau \circ f$.

9 Group Homomorphisms II

Definition 9.1 (Epimorphism & Monomorphism). Let $\phi : H \longrightarrow G$ be an homomorphism, we say ϕ is an epimorphism if ϕ is onto; monomorphism if ϕ is one to one.

Example 9.1. Let G be a group. $\phi : G \longrightarrow \{1\}$ is an epimorphism. Since for $g, g' \in G$, we have $\phi(gg') = 1 = 1^2 = \phi(g)\phi(g')$. This shows ϕ is homomorphism, and it is clearly surjective.

Example 9.2. Let $H \leq G$ then the inclusion map $\eta : H \hookrightarrow G; h \longmapsto h$ is a monomorphism. It is one to one and an homomorphism, i.e. $\eta(h_1h_2) = h_1h_2 = \eta(h_1)\eta(h_2)$.

Definition 9.2 (Kernel). Let $\phi : H \longrightarrow G$ be a group homomorphism. The kernel of ϕ is $\ker(\phi) = \phi^{-1}(1) = \{h \in H : \phi(h) = 1_G\}$.

Proposition 9.1. Let $\phi : H \longrightarrow G$ be a group homomorphism.

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

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

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

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

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

Proof. (i) Just check closure axioms. $\phi(1_H) = 1_G \in G' \implies 1_H \in \phi^{-1}(G')$. If $h, h' \in \phi^{-1}(G')$ then $\phi(hh') = \phi(h)\phi(h') \in G'$ by closure of subgroups. So $hh' \in \phi^{-1}(G')$. By closure under inverses of a subgroup, $\phi(h^{-1}) = (\phi(h))^{-1} \in G' \implies h^{-1} \in \phi^{-1}(G')$. Thus $\phi^{-1}(G') \leq H$. (ii) Suffice to show for any $h \in H$, $h' \in \phi^{-1}(G')$, we have $h^{-1}h'h \in \phi^{-1}(G')$, i.e. $h^{-1}\phi^{-1}(G')h \subseteq \phi^{-1}(G')$. $\phi(h^{-1}h'h) = \phi(h^{-1})\phi(h')\phi(h) = (\phi(h))^{-1}\phi(h')\phi(h) \in (\phi(h))^{-1}G'\phi(h) = G'$ due to normality of G'. $\therefore h^{-1}h'h \in \phi^{-1}(G') \implies \phi^{-1}(G') \trianglelefteq H$. (iii) When you put $G' = 1$ and note $1 \trianglelefteq G$, $\ker(\phi) = \phi^{-1}(1) \trianglelefteq H$. (iv) Let $h \in H$ be such that $g = \phi(h)$. Suffice to show $hK = \phi^{-1}(g)$. Now

$\phi(hK) = \phi(h)\phi(K) = \phi(h) = g$ as $\phi(K) = 1$. $\therefore hK \subseteq \phi^{-1}(g)$. Suppose $h' \in \phi^{-1}(g)$ then $\phi(h^{-1}h') = \phi(h^{-1})\phi(h') = (\phi(h))^{-1}\phi(h') = g^{-1}g = 1$. Thus $h^{-1}h' \in K$. $\therefore h' = h(h^{-1}h') \in hK \implies \phi^{-1}(g) \subseteq hK$. $hK = \phi^{-1}(g)$ and (iv) holds. (v) By (iv), ϕ is one to one if and only if non-empty fibres have one element. But cosets of K has same number of elements, i.e. if and only if K, a coset of K, has one element.

Example 9.3. Let $T : V \longrightarrow W$ be linear, e.g. in $\mathbb{R}^3$, T is the projection onto a line L. Fix $\mathbf{w} \in W$, then the set of solutions to $T(\mathbf{v}) = \mathbf{w}$ is $T^{-1}(\mathbf{w}) = \mathbf{v}_p + K$ (coset of K). K is the kernel and $\mathbf{v}_p$ is any particular solution.

Example 9.4. Special linear group. Consider homomorphism $\det : GL_n(\mathbb{C}) \longrightarrow \mathbb{C}^*$. Define $SL_n(\mathbb{C}) = \ker(\det) = \{M \in GL_n(\mathbb{C}) : \det(M) = 1\} \trianglelefteq GL_n(\mathbb{C})$. Similarly define $SL_n(\mathbb{R})$.

Example 9.5. There is an homomorphism $\phi : S_n \longrightarrow GL_n(\mathbb{R}); \sigma \longmapsto \phi(\sigma)$ defined by $\phi(\sigma) : \mathbb{R}^n \longrightarrow \mathbb{R}^n; \mathbf{e}_i \longmapsto \mathbf{e}_{\sigma(i)}$, e.g. $\sigma(12) = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}$. Consider composite homomorphism $\psi = \det\phi : S_n \xrightarrow{\phi} GL_n(\mathbb{R}) \xrightarrow{\det} \mathbb{R}^*$. Write $\sigma \in S_n$ as $\sigma = \tau_1\tau_2\dots\tau_m$ for transpositions τ_i. $\psi(\sigma) = \psi(\tau_1)\psi(\tau_2)\dots\psi(\tau_m) = (-1)^m$ since ψ of a transposition is the determinant of the identity matrix with two rows swapped. Note $\psi^{-1}(1) = \ker(\psi) = A_n \trianglelefteq S_n$ and $\psi^{-1}(-1) =$ set of odd permutations, which is the other coset of A_n.

Proposition - Definition 9.1 (Quotient Morphism). Let $N \trianglelefteq G$, the quotient morphism of G by N is $\pi : G \longrightarrow G/N; g \longmapsto gN$. π is an epimorphism with kernel N

Proof. Check π is homomorphism, i.e. for $g, g' \in G$, $\pi(gg') = gg'N = gNg'N = \pi(g)\pi(g')$. $\therefore$ it is an homomorphism. Finally, $\ker(\pi) = \pi^{-1}(1_{G/N}) = \pi^{-1}(N) = \{g \in G : gN = N\} = N$.

10 First Group Isomorphism Theorem

How much does an homomorphism deviate from being an isomorphism?

Theorem 10.1 (Universal Property Of Quotient Morphism). Let $N \trianglelefteq G$ and $\pi : G \longrightarrow G/N; g \longmapsto gN$ be the quotient morphism. Let $\phi : G \longrightarrow H$ be an homomorphism such that $\ker(\phi) \geq N$. Then

(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 $\psi : G/N \longrightarrow H; gN \longmapsto \phi(g)$ is an homomorphism, called an induced homomorphism

(iii) $\phi = \psi \circ \pi$ is the unique such function

(iv) $\ker(\psi) = \ker(\phi)/N$

Proof. (i) Suppose $g' = gn$ for some $n \in N$, i.e. $g' \in gN$, then $\phi(g') = \phi(gn) = \phi(g)\phi(n) = \phi(g)$, since $n \in N \leq \ker(\phi)$. (ii) ψ is well defined since if $g'N = gN$ then $\phi(g') = \phi(g)$ by part (i). For $g, g' \in G$, we check $\psi(gNg'N) = \psi(gN)\psi(g'N)$. Now since ϕ is an homomorphism, we have $\psi(gNg'N) = \psi(gg'N) = \phi(gg') = \phi(g)\phi(g') = \psi(gN)\psi(g'N)$. (iii) Clear from the picture. (iv) $\ker(\psi) = \{gN : \psi(gN) = 1_H\} = \{gN : \phi(g) = 1_H\} = \{gN : g \in \ker(\phi)\} = \ker(\phi)/N$ by definition.

$$\begin{array}{ccc} G & \xrightarrow{\quad\phi\quad} & H \\ {\scriptstyle\pi}\searrow & & \nearrow{\scriptstyle\psi} \\ & G/N & \end{array}$$

$$\begin{array}{ccc} g & \longmapsto & \phi(g) \\ & \searrow \quad \nearrow & \\ & gN & \end{array}$$

Lemma 10.1. Any subgroup $N \leq \mathbb{Z}$ has the form $N = m\mathbb{Z}$ for some $m \in \mathbb{Z}$.

Proof. If $N = 0$, can take $m = 0$. Suppose $N \neq 0$, since N is closed under negatives, it has a minimal positive element m. Suffice to show $N = m\mathbb{Z}$. Subgroup closure axioms $\implies m\mathbb{Z} \subseteq N$, as any multiple of m will be in N. To show $N \subseteq m\mathbb{Z}$, let $n \in N$ and write $n = mq + r$, where $q \in \mathbb{Z}$, $r \in \{0, 1, 2, \ldots, m-1\}$. $\therefore r = n - mq \in N$ since $n \in N$ and $mq \in m\mathbb{Z} \subseteq N$. Minimality of $m \implies r = 0$. So $n = mq \in m\mathbb{Z}$. Hence $N = m\mathbb{Z}$ as desired.

Note that $\mathbb{Z}/m\mathbb{Z}$ is a cyclic group generated by $1 + m\mathbb{Z}$, i.e. $k(1 + m\mathbb{Z}) = k + m\mathbb{Z}$ for $k \in \{0, 1, 2, \ldots, m-1\}$. Further, if $m \neq 0$, then $1 + m\mathbb{Z}$ has order m since $m(1 + m\mathbb{Z}) = m\mathbb{Z} = 0_{\mathbb{Z}/m\mathbb{Z}}$ but for $i \in \{1, 2, \ldots, m-1\}$, $i(1 + \ m\mathbb{Z}) = i + m\mathbb{Z} \neq m\mathbb{Z}$.

Proposition 10.1 (Classification Of Cyclic Groups). Let $H = \langle h \rangle$ be a cyclic group. Then there is a well defined isomorphism $\phi : \mathbb{Z}/m\mathbb{Z} \longrightarrow H; i + m\mathbb{Z} \longmapsto h^i$, where m is the order of h if this is finite and is 0 if h has infinite order.

Proof. Define function $\phi : \mathbb{Z} \longrightarrow H; i \longmapsto h^i$. It is an homomorphism since $\phi(i + j) = h^{i+j} = h^i h^j = \phi(i)\phi(j)$. Apply Theorem 10.1 with $N = \ker(\phi)$ to get homomorphism $\psi : \mathbb{Z}/N \longrightarrow H$. By Lemma 10.1, $N = \ker(\phi)$ is a subgroup of $\mathbb{Z}$, so $N = m\mathbb{Z}$ for some $m \in \mathbb{Z}$. Using Theorem 10.1 (iv), $\ker(\psi) = \ker(\phi)/N = \ker(\phi)/\ker(\phi) = 0$, the identity. So ψ is one to one. Note ϕ is surjective. So by Theorem 10.1 (iii), i.e. $\phi = \psi \circ \pi$, ψ must be surjective too. As an exercise, check h infinite order case. See order of h = order of $\phi^{-1}(h)$ = order of $1 + m\mathbb{Z} = m$.

Corollary 10.1. A group H is said to have an exponent $n > 0$ if either of the following equivalent conditions hold.

(i) $h^n = 1$ for all $h \in H$

(ii) For every $h \in H$, n in a multiple of the order of h

Proof. Use isomorphism $\psi : \mathbb{Z}/m\mathbb{Z} \longrightarrow \langle h \rangle$ of Proposition 10.1, to see that $h^n = 1 \iff n \in m\mathbb{Z}$.

Theorem 10.2 (First Isomorphism Theorem). Let $\phi : G \longrightarrow H$ be an homomorphism. Then the Universal Property Of Quotient Morphism $\pi : G \longrightarrow G/\ker(\phi)$ induces a monomorphism $\psi : G/\ker(\phi) \hookrightarrow H$, which induces isomorphism $G/\ker(\phi) \cong \text{Im}(\phi) \leq H$. We can fact ϕ into $\phi : G \xrightarrow{\pi} G/\ker(\phi)$ (quotient morphism) $\cong \text{Im}(\phi) \hookrightarrow H$.

Proof. Same as in Theorem 10.1, The Universal Property Of Quotient Morphism, with $N = \ker(\phi)$.

So to turn an homomorphism into an isomorphism, we need to first factor out the kernel using the quotient morphism, so it is one to one. Then we must restrict the codomain to the range to make it onto.

Example 10.1. $T : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ be the projection onto a line L. Then $\mathbb{R}^3/\ker(T)$ are the planes perpendicular to L. $\therefore \mathbb{R}^3/\ker(T) \cong L$, the bijection from the plane to the corresponding point on L.

11 Subgroups Of Quotient Groups & Other Isomorphism Group Theorems

The idea is that if we know all subgroups of the original group, then we should know all subgroups of the quotient group.

Proposition 11.1 (Subgroups Of Quotient Groups). Let $N \trianglelefteq G$ and $\pi : G \longrightarrow G/N$ be the quotient morphism.

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

(ii) There is a bijection $\{\text{subgroups } H \leq G \text{ such that } N \leq H\} \longrightarrow \{\text{subgroups } \bar{H} \leq G/N\}; H \longmapsto \pi(H) = H/N = \{hN : h \in H\}$ and $\bar{H} \longmapsto \pi^{-1}(\bar{H})$ is the inverse

(iii) Normal subgroups above correspond

Proof. (i) By definition $hN = Nh$ for all $h \in G$, so $hN = Nh \ \forall \ h \in H$, i.e. $N \trianglelefteq H$. For (ii) and (iii), we check that maps are well defined. Homomorphisms takes subgroups to subgroups. So π^{-1} takes subgroups to subgroups, and so does π. Also $\pi^{-1}(\bar{H}) \geq \pi^{-1}(1_{G/N}) = \pi^{-1}(N) = N$. Let us check that it preserves normality. Suppose $N \leq H \trianglelefteq G$, we need to show $H/N \trianglelefteq G/N$. Consider $g \in G$, $h \in H$, $(g^{-1}N)(hN)(gN) = (g^{-1}hg)N$ $(N \trianglelefteq G) \in H/N$ as $g^{-1}hg \in H \trianglelefteq G$. So $H/N \trianglelefteq G/N$. We now check that these two maps are inverses to each other. Firstly π is onto $\implies \pi(\pi^{-1}(\bar{H})) = \bar{H}$. $\pi^{-1}(\pi(H)) = \pi^{-1}(H/N) = \bigcup_{h \in H} hN = H$ as H/N has elements of the form hN. So we obtain a bijection.

Proposition 11.2 (Subgroups Of Cyclic Groups). Let $m \in \mathbb{Z}$ be positive and $\bar{H} \leq \mathbb{Z}/m\mathbb{Z}$. Then $\bar{H} = n\mathbb{Z}/m\mathbb{Z}$ where $n \mid m$ for some n. $\bar{H} = \langle n + m\mathbb{Z} \rangle$ is a cyclic group of order $\frac{m}{n}$.

Proof. By Proposition 11.1, $\bar{H} = H/m\mathbb{Z}$ for some $H \leq \mathbb{Z}$. From Lemma 10.1, we know $H = n\mathbb{Z}$ for some $n \in \mathbb{N}$. Also $n\mathbb{Z} \supseteq m\mathbb{Z} \iff m \in n\mathbb{Z} \iff n \mid m$. The last statement is trivial. Note that $\bar{H}^{\frac{m}{n}} = \frac{m}{n}(n + m\mathbb{Z}) = n \times \frac{m}{n} + m\mathbb{Z} = m\mathbb{Z}$, which is the identity in $\mathbb{Z}/m\mathbb{Z}$.

Suppose $H \leq G$, $N \trianglelefteq G$, we apply First Isomorphism Theorem to the following composite homomorphisms, since composition of homomorphisms is still an homomorphism.

(i) $\phi : H \hookrightarrow G \xrightarrow{\pi_N} G/N$

(ii) $\phi : G \xrightarrow{\pi_N} G/N \xrightarrow{\pi_{H/N}} \frac{G/N}{H/N}$, since by Proposition 11.1, if $N \leq H \trianglelefteq G$, then $H/N \trianglelefteq G/N$.

Theorem 11.1 (Second Isomorphism Theorem). Suppose $N \leq H \trianglelefteq G$ and $N \trianglelefteq G$ as in above. Then $\frac{G/N}{H/N} \cong G/H$.

Proof. Since π_N, $\pi_{H/N}$ are both onto, $\phi = \pi_{H/N} \circ \pi_N$ is onto also. $\ker(\phi) = \{g \in G : \pi_N(g) \in \ker(\pi_{H/N} : G/N \longrightarrow \frac{G/N}{H/N})\} = \{g \in G : \pi_N(g) \in H/N\} = \pi_N^{-1}(H/N) = H$ by Proposition 11.1. First Isomorphism Theorem says $G/\ker(\phi) \cong \mathrm{Im}(\phi) \Longrightarrow G/H \cong \frac{G/N}{H/N}$. This proves the theorem.

Example 11.1. $\frac{\mathbb{Z}/4\mathbb{Z}}{2\mathbb{Z}/4\mathbb{Z}} = \mathbb{Z}/2\mathbb{Z}$.

Theorem 11.2 (Third Isomorphism Theorem). Suppose $H \leq G$, $N \trianglelefteq G$. Then

(i) $H \cap N \trianglelefteq H$, $HN \leq G$ (note if $H, N \leq G$ only, we may not necessarily have $HN \leq G$)

(ii) We have isomorphism $\frac{H}{H \cap N} \cong \frac{HN}{N}$

Proof. By applying First Isomorphism Theorem to $\phi : H \hookrightarrow G \xrightarrow{\pi_N} G/N$ and using Proposition 11.1, it suffices to show (a) $\ker(\phi) = H \cap N$, (b) $\mathrm{Im}(\phi) = HN/N$. Check (a), $\ker(\phi) = \{h \in H : h \in \ker(\pi_N : G \longrightarrow G/N)\} = \{h \in H : h \in N\} = N \cap H$. Check (b), $\mathrm{Im}(\phi) = \{hN : h \in H\} \leq G/N$. By Proposition 11.1, $\bar{H} = \pi_N^{-1}\pi_N(\bar{H}) = \pi_N(\bar{H})/N$. But $\pi_N(\bar{H}) = \bigcup_{h \in H} hN = HN \Longrightarrow \bar{H} = HN/N \leq G/N$ and $HN \leq G$. By First Isomorphism Theorem, $H/\ker(\phi) \cong \mathrm{Im}(\phi) \Longrightarrow \frac{H}{H \cap N} \cong \frac{HN}{N}$. To see $H \cap N \trianglelefteq H$, note $N \trianglelefteq G$ and $H \cap N \leq N \Longrightarrow H \cap N \trianglelefteq G$. Since $H \cap N \leq H \leq G$ and by Proposition 11.1, $H \cap N \trianglelefteq H$.

Example 11.2. $G = S_n \trianglerighteq A_n = N$. $H = \langle \tau \rangle \cong \mathbb{Z}/2\mathbb{Z}$, where τ is a transposition. $H \cap N = \langle \tau \rangle \cap A_n = \{1, \tau\} \cap A_n = 1$. $HN = A_n \cup \tau A_n = S_n$. Hence $\frac{H}{H \cap N} \cong \frac{HN}{N} \iff \langle \tau \rangle \cong S_n/A_n$ with $1 \longleftrightarrow A_n; \tau \longleftrightarrow \tau A_n$.

12 Products

Given groups $G_1, G_2, \ldots, G_n$, recall $G_1 \times G_2 \times \ldots \times G_n = \{(g_1, g_2, \ldots, g_n) : g_i \in G_i \text{ for all } i\}$. More generally, for groups G_i, indexed $i \in I$, we have $\prod_{i \in I} G_i = \{(g_i)_{i \in I} : g_i \in G_i \text{ for all } i\}$.

Proposition - Definition 12.1 (Product). The set $G = \prod_{i \in I} G_i$ is a group called the product of the G_i's, when endowed with coordinatewise multiplication, i.e. $(g_i)(g_i') = (g_i g_i')$.

(i) $1_G = (1_{G_i})$

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

Proof. Check axioms, e.g. $(1_{G_i})(g_i) = (1_{G_i}g_i) = (g_i) = (g_i)(1_{G_i})$.

Example 12.1. $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$. $(2,3) + (1,-1) = (3,2)$ since product of abelian groups is abelian. $\mathbb{Z}^2$ is finitely generated by $(1,0)$ and $(0,1)$ since for all $(m,n) \in \mathbb{Z}^2$, $(m,n) = m(1,0) + n(0,1)$.

Let G_i be groups indexed by $i \in I$. We define two new maps for any $r \in I$.

(i) Canonical projection: $\pi_r : \prod_{i\in I} G_i \longrightarrow G_r; (g_i) \longmapsto g_r$

(ii) Canonical injection: $\iota_r : G_r \longrightarrow \prod_{i\in I} G_i; g_r \longmapsto (g_i)$ where $g_i = 1$ if $i \neq r$; $g_i = g_r$ if $i = r$

Proposition 12.1. With the above notation, we have:

(i) ι_r is a monomorphism

(ii) π_r is an epimorphism

(iii) $\frac{G_1 \times G_2}{G_1 \times 1} \cong G_2$

Proof. (i) is similar to (ii). (ii) π_r is onto, so suffice to check homomorphism, i.e. $\pi_r((g_i)(g_i')) = \pi_r(g_ig_i') = g_rg_r' = \pi_r((g_i))\pi_r((g_i'))$. (iii) For groups G_1, G_2, apply First Isomorphism Theorem to $\pi_2 : G_1 \times G_2 \longrightarrow G_2$ gives the isomorphism.

Note that $G_1 \cong G_1 \times 1$, so we can sort of see G_1, G_2 as subgroups or factors of $G_1 \times G_2$. Can you recognise if subgroups $G_1, G_2, \ldots, G_n \leq G$ are such that $G \cong G_1 \times G_2 \times \ldots \times G_n$ naturally?

Proposition 12.2 (Internal Characterisation Of products). Let $G_1, G_2, \ldots, G_n \leq G$ generate G, i.e. $\langle G_1, G_2, \ldots, G_n\rangle = G$. Suppose that

(i) For i, j distinct, elements of G_i and G_j commute

(ii) For any i, $G_i \cap \langle \bigcup_{l\neq i} G_l\rangle = 1$, i.e. similar to linear independence in vector spaces

Then we have an isomorphism $\phi : G_1 \times G_2 \times \ \ldots \times G_n \longrightarrow G; (g_1, g_2, \ldots, g_n) \longmapsto g_1g_2\ldots g_n$.

Proof. Check ϕ is an homomorphism, i.e. $\phi((g_i)(g_i')) = \phi(g_ig_i') = g_1g_1'g_2g_2'\ldots g_ng_n' = g_1g_2\ldots g_n$ $g_1'g_2'\ldots g_n' = \phi(g_i)\phi(g_i')$ (for $i \neq j$, g_i and g_j commute. Check ϕ is onto. This follows from the commutativity of g_i, g_l for $i \neq j$ (can write in the form $g_1g_2\ldots g_n$, $g_i \in G_i$) and the fact $G_1, G_2, \ldots, G_n$ generate G. Suppose $(g_1, g_2, \ldots, g_n) \in \ker(\phi)$. Then suffice to show $g_i = 1$ for any i. Now $1 = \phi(g_1, g_2, \ldots, g_n) = g_1g_2\ldots g_n \Longrightarrow g_i = g_1^{-1}g_2^{-1}\ldots g_{i-1}^{-1}g_{i+1}^{-1}\ldots g_n^{-1}$ due to commutativity. The left hand side is in G_i and the right hand side in $\langle \bigcup_{l\neq i} G_l\rangle$. Thus $g_i = 1$ since $G_i \cap \langle \bigcup_{l\neq i} G_l\rangle = 1$. This gives the second proposition.

Corollary 12.1. Let G be a finite group of exponent two, then $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \ldots \times \mathbb{Z}/2\mathbb{Z}$ (finite times), where $\mathbb{Z}/2\mathbb{Z}$ is the cyclic group of order two.

Proof. G finite $\Longrightarrow G$ is finitely generated, e.g. generated by G itself. Pick minimal generating set $\{g_1, g_2, \ldots, g_n\}$. Note g_i has order 2. $\Longrightarrow \langle g_i\rangle \cong \mathbb{Z}/2\mathbb{Z}$. It suffices to use Proposition 12.2 to show $G \cong \langle g_1\rangle \times \langle g_2\rangle \times \ldots \times \langle g_n\rangle$. Let us check the conditions (i) and (ii) hold since $\langle g_i\rangle$'s generate G. To check (i), for $g, h \in G$, $1 = (gh)^2 = ghgh \therefore gh = g^2hgh^2 = hg$ as $g^2 = h^2 = 1$. So G is abelian and so is OK. (ii) WLOG, suffice to check $\langle g_1\rangle \cap \langle g_2, g_3, \ldots, g_n\rangle = \{1, g_1\} \cap \langle g_2, g_3, \ldots, g_n\rangle = 1$. If false then $g_1 \in \langle g_2, g_3, \ldots, g_n\rangle$. So g_1 can be omitted from the generating set. This contradicts the minimality assumption.

Proposition 12.3 (Universal Property Of Products). Let H_i, G_i $(i \in I)$ be groups. For $i \in I$, let $\phi_i : H \longrightarrow G_i$ be an homomorphism. Then we have an homomorphism $(\phi_i)_{i\in I} : H \longrightarrow \prod_{i\in I} G_i; h \longmapsto (\phi_i(h))_{i\in I}$.

Proof. Check definitions.

Theorem 12.1 (Structure Theorem For Finitely Generated Abelian Groups). Let G be a finitely generated group. Then $G \cong \mathbb{Z}/h_1\mathbb{Z} \times \mathbb{Z}/h_2\mathbb{Z} \times \ldots \times \mathbb{Z}/h_r\mathbb{Z} \times \mathbb{Z}^s$, where $h_1 \mid h_2 \mid h_3 \mid \ldots \mid h_{r-1} \mid h_r$ for some $r, s \in \mathbb{N}$.

13 Symmetries Of Regular Polygons

Recall an isometry $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ satisfies $\|\mathbf{x} - \mathbf{y}\| = \|T\mathbf{x} - T\mathbf{y}\|$. Also recall that AO_n, the set of surjective symmetries $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ forms a subgroup of $\mathrm{Perm}(\mathbb{R}^n)$.

Example 13.1. Let $\mathbf{x} \in \mathbb{R}^n$. For this lecture, denote translation by $\mathbf{v}$ by $T_\mathbf{v} : \mathbb{R}^n \longrightarrow \mathbb{R}^n; \mathbf{x} \longmapsto \mathbf{x} + \mathbf{v}$. $T_\mathbf{v}$ is an isometry.

Proposition 13.1. 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. Let $\mathbf{v} = T(\mathbf{0})$. Set $T' = T_\mathbf{v}^{-1} \circ T = T_{-\mathbf{v}} \circ T$, which is an isometry, being composite of isometries. $T'(\mathbf{0}) = T_{-\mathbf{v}}(T(\mathbf{0})) = T_\mathbf{v}(\mathbf{v}) = \mathbf{v} - \mathbf{v} = \mathbf{0}$ gives the proposition.

Theorem 13.1. Let $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ be an isometry such that $T(\mathbf{0}) = \mathbf{0}$. Then T is linear. Since T is injective so T is automatically surjective and $T \in O_n$, i.e. T preserves dot product and orthogonality.

Proof. $T\mathbf{x} = T\mathbf{y} \Longrightarrow \|T\mathbf{x} - T\mathbf{y}\| = 0 \Longrightarrow \|\mathbf{x} - \mathbf{y}\| = 0 \Longrightarrow \mathbf{x} = \mathbf{y}$. The following is an heuristic argument that is not examinable. Note that T is continuous ($\|\mathbf{x} - \mathbf{y}\| \to 0 \Longrightarrow \|T\mathbf{x} - T\mathbf{y}\| \to 0$). Check additivity of T. Sides are all equal, i.e. $OA = OA'$, $OB = OB'$, $AB = A'B'$, as T is an isometry. ($\|\mathbf{x} - \mathbf{y}\| = \|T\mathbf{x} - T\mathbf{y}\|$) on $\mathbf{0}$, $T\mathbf{x}$, $T\mathbf{y}$, $T(\mathbf{x} + \mathbf{y})$. $\therefore \triangle OAB \cong \triangle OA'B'$ (SSS). Similarly $\triangle OBC \cong \triangle OB'C'$ (SSS). Now $AC = \|\mathbf{x} - \mathbf{y}\| = \|T\mathbf{x} - T\mathbf{y}\| = A'C'$ also. So points $OA'B'C'$ is a parallelogram congruent to $OABC$. So if $\mathbf{x} \neq \mathbf{y}$, then $T(\mathbf{x}+\mathbf{y}) = T\mathbf{x}+T\mathbf{y}$, using the parallelogram $OA'B'C'$. $\because T$ is continuous $\therefore$ let $\mathbf{x} \to \mathbf{y}$, $T(\mathbf{x} + \mathbf{y}) = T\mathbf{x} + \mathbf{y}$ still holds if $\mathbf{x} = \mathbf{y}$. Thus additivity is true for all $\mathbf{x}$, $\mathbf{y}$ by continuity of T. Let us check scalar multiplication is preserved too. Let $\mathbf{x} \in \mathbb{R}^n$ and $m \in \mathbb{N}$. Then $T(m\mathbf{x}) = T\mathbf{x} + T\mathbf{x} + \ldots + T\mathbf{x} = mT\mathbf{x}$. Put $\frac{1}{m}\mathbf{x}$ for $\mathbf{x}$ in the above gives $T\mathbf{x} = mT(\frac{1}{m}\mathbf{x}) \Longrightarrow T(\frac{1}{m}\mathbf{x}) = \frac{1}{m}T\mathbf{x}$. Note also $\mathbf{0} = T(\mathbf{0}) = T(\mathbf{x}-\mathbf{x}) = T(\mathbf{x})+T(-\mathbf{x}) \Longrightarrow T(-\mathbf{x}) = -T(\mathbf{x})$. $\therefore T(\lambda\mathbf{x}) = \lambda T(\mathbf{x})$ for all $\lambda \in \mathbb{Q}$. Hence true for all $\lambda \in \mathbb{R}$ by continuity of T.

Let $V = \{\mathbf{v}^1, \mathbf{v}^2, \ldots, \mathbf{v}^m\} \subseteq \mathbb{R}^n$. Recall its centre of mass is $\mathbf{c}_V = \frac{1}{m}(\mathbf{v}^1 + \mathbf{v}^2 + \ldots + \mathbf{v}^m)$.

Proposition 13.2. Consider the following function. The function attains a unique minimum when $\mathbf{x} = \mathbf{c}_V$.

$$E_V(\mathbf{x}) = \sum_{i=1}^{m} \|\mathbf{x} - \mathbf{v}^i\|^2$$

Proof. Consider the following. $\therefore$ unique minimum when $x_j = -\frac{b}{2a} = \frac{1}{m}\sum_i v_j^i$, i.e. when $\mathbf{x} = \mathbf{c}_V$.

$$E_V(\mathbf{x}) = \sum_{i,j}(x_j - v_j^i)^2 = \sum_{i,j}(x_j^2 - 2x_j v_j^i + (v_j^i)^2) = \sum_j (mx_j^2 - 2x_j(\sum_i v_j^i) + \sum_i (v_j^i)^2)$$

Corollary 13.1. Let $V = \{\mathbf{v}^1, \mathbf{v}^2, \ldots, \mathbf{v}^m\}$ and $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ be an isometry such that $T(V) = V$. Then $T(\mathbf{c}_V) = \mathbf{c}_V$.

Proof. $T\mathbf{c}_V = \mathbf{c}_V$ since

$$\begin{aligned} E_V(T\mathbf{c}_V) &= \sum_{i=1}^m \|T\mathbf{c}_V - \mathbf{v}^i\|^2 \\ &= \sum_{i=1}^m \|T\mathbf{c}_V - T\mathbf{v}^i\|^2 \quad (T \text{ permutes } \mathbf{v}^i\text{'s}) \\ &= \sum_{i=1}^m \|\mathbf{c}_V - \mathbf{v}^i\|^2 \\ &= E_V(\mathbf{c}_V) \quad (T \in AO_n) \end{aligned}$$

Corollary 13.2. Let $G \leq AO_n$ be finite. There is some vector $\mathbf{c} \in \mathbb{R}^n$ such that $T\mathbf{c} = \mathbf{c}$ for ant $T \in G$.

Proof. Pick $\mathbf{w} \in \mathbb{R}^n$ and let $V = \{S\mathbf{w} : S \in G\} \subseteq \mathbb{R}^n$ be as in Corollary 13.1. Note V is finite as G is finite. Note $T(V) = \{TS\mathbf{w} : S \in G\} \subseteq V$ as $TS \in G$ for all $T \in G$. But T is bijective $\Longrightarrow$ we have $T(V) = V$. Put $\mathbf{c} = \mathbf{c}_V$ in Corollary 13.1 to get this corollary.

Note if $G \leq AO_n$ is finite. Let us translate in $\mathbb{R}^n$ to change the coordinates and make $\mathbf{c}$ in Corollary 13.2 equal to $\mathbf{0}$. By Theorem 13.1, $G \leq O_n$.

Example 13.2. Let $\mathbf{v} \in \mathbb{R}^n - \{\mathbf{0}\}$. Note there is no $\mathbf{c}$ with $T_{\mathbf{v}}(\mathbf{c}) = \mathbf{v} + \mathbf{c} = \mathbf{c}$. However $\langle T_{\mathbf{v}} \rangle = \{T_{\mathbf{v}}^i : i \in \mathbb{Z}\} = \{T_{i\mathbf{v}} : i \in \mathbb{Z}\}$ is infinite. This is a contrapositive example of Corollary 13.2.

Let F be a regular n-gon, V be the set of vertices and G the set of symmetries of F. By Proposition 13.1, any isometry is a composite of linear translation and linear map. $\therefore$ Any $T \in G$ satisfies $T(V) = V$, since T is a linear translation or a linear map, i.e. T takes edges to edges and vertices to vertices. Corollary 13.1 $\Longrightarrow T(\mathbf{c}_V) = \mathbf{c}_V$. We change the coordinates so that $\mathbf{c}_V = \mathbf{0}$. Hence by Theorem 13.1, $G \leq O_2$ ($n = 2$ for a plane). But O_2 consists of rotations and reflections. By symmetry, we get ...

Proposition 13.3 (Symmetries Of Regular Polygons). The group of symmetries of a regular n-gon is in fact D_n.

Note that if T, such that $T(\mathbf{0}) = \mathbf{0}$, preserves distance, then T preserves dot product, i.e. $\|T\mathbf{x} - T\mathbf{y}\|^2 = \|\mathbf{x} - \mathbf{y}\|^2 \Longrightarrow \|T\mathbf{x}\|^2 - 2(T\mathbf{x}) \cdot (T\mathbf{y}) + \|T\mathbf{y}\|^2 = \|\mathbf{x}\|^2 - 2\mathbf{x} \cdot \mathbf{y} + \|\mathbf{y}\|^2 \Longrightarrow (T\mathbf{x}) \cdot (T\mathbf{y}) = \mathbf{x} \cdot \mathbf{y}$ ($\|T(\mathbf{x})\| = \|T(\mathbf{x}) - \mathbf{0}\| = \|T(\mathbf{x}) - T(\mathbf{0})\| = \|\mathbf{x} - \mathbf{0}\| = \|\mathbf{x}\|$).

14 Abstract Symmetry & Group Actions

Example 14.1. (A), (B) and (C) have symmetric groups $\{1, \tau\}$, $\{1, \sigma\}$ and $\{1, \tau\}$ respectively. Thus the symmetry group is $\mathbb{Z}/2\mathbb{Z}$ in all cases but (A) and (B) exhibit very different symmetries while (A) and (C) very similar. So we need more data to distinguish (A) and (B).

Let G be a group.

Definition 14.1 (G-Set). A G-Set S is a set S equipped with a map $\alpha : G \times S \longrightarrow S; (g, s) \longmapsto \alpha(g, s) = g.s$, called the group action or operation satisfying the following axioms:

(i) Associativity, for $g, h \in G$, $s \in S$, we have $g.(h.s) = (gh).s$ (note $h.s \in S$, $gh \in G$)

(ii) For $s \in S$, we have $1.s = s$

We also say that G acts on S or operates on S.

Example 14.2. Let $G = \mathbb{R}^*$ (multiplicative group) and S a vector space over $\mathbb{R}$. Then S is a G-set with group action $\alpha.\mathbf{v} = \alpha\mathbf{v}$ (scalar multiplication, $\alpha \in G = \mathbb{R}^*$, $\mathbf{v} \in S$). In a sense, group actions looks like scalar multiplication in vector spaces.

Example 14.3. let $G = GL_n(\mathbb{C})$ and $S = \mathbb{C}^n$. S is a G-set with G-action $A.\mathbf{v} = A\mathbf{v}$ (matrix multiplication, $A \in GL_n(\mathbb{C})$, $\mathbf{v} \in \mathbb{C}^n$). Why? (i) $(AB)\mathbf{v} = A(B\mathbf{v})$ and (ii) $I_n\mathbf{v} = \mathbf{v}$.

Proposition - Definition 14.1 (Permutation Representation). A permutation representation of a group G on a set S is an homomorphism $\phi : G \longrightarrow \mathrm{Perm}(S)$. This gives rise to a G-set S with G-action $g.s = (\phi(g))(s)$ ($g \in G$, $s \in S$, $\phi(g) \in \mathrm{Perm}(S)$, $(\phi(g))(s) \in S$).

Proof. Check axioms. For $s \in S$, check (ii), i.e. $1.s = s$? $LHS = (\phi(1))(s) = \mathrm{id}(s) = s = RHS$ since ϕ is an homomorphism. And further if $g, h \in G$, we check condition (i), i.e. $g.(h.s) = (gh).s$. $RHS = (\phi(gh))(s) = (\phi(g) \circ \phi(h))(s)$ (multiplication in permutation groups in composition of functions) $= \phi(g)(\phi(h)(s)) = g.(\phi(h)(s)) = g.(h.s) = LHS$. $\therefore S$ is a G-set.

Example 14.4. Back to Example 14.1. $G = \{1, g\} \cong \mathbb{Z}/2\mathbb{Z}$, we have the following representations and G-sets. $S = \mathbb{R}^2$. (A) $\Longrightarrow \phi_A : G \cong \mathbb{Z}/2\mathbb{Z} \longrightarrow \langle\tau\rangle = \langle\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\rangle \hookrightarrow GL_2(\mathbb{R}) \hookrightarrow \mathrm{Perm}(\mathbb{R}^2)$, i.e. permutations of $\mathbb{R}^2$ are matrices, while $\phi_A(g) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. (B) $\Longrightarrow \phi_B : G \longrightarrow \langle\sigma\rangle = \langle\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\rangle \hookrightarrow \mathrm{Perm}(\mathbb{R}^2)$ and (C) $\Longrightarrow \phi_C : G \longrightarrow \langle\sigma\rangle = \langle\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\rangle \hookrightarrow \mathrm{Perm}(\mathbb{R}^2)$.

Proposition 14.1. Every G-set arises from a permutation representation in this fashion, i.e. every G-action can be represented in a permutation form.

Proof. Let S be a G-set. Define function $\phi : G \longrightarrow \text{Perm}(S); g \longmapsto \phi(g)$ and $\phi(g) : S \longrightarrow S; s \longmapsto g.s$. Check well defined, i.e. $\phi(g)$ is bijective by showing $\phi(g^{-1})$ is the inverse. For $s \in S$, $(\phi(g^{-1}) \circ \phi(g))(s) = g^{-1}.(g.s) = (g^{-1}g).s$ (by associativity) $= 1.s = s$. $\therefore \phi(g^{-1}) \circ \phi(g) = \text{id}$ and similarly $\phi(g) \circ \phi(g^{-1}) = \text{id}$. So $\phi(g) \in \text{Perm}(S)$. Now check ϕ is an homomorphism, i.e. $g, h \in G$, $s \in S$, $(\phi(gh))(s) = (\phi(g) \circ \phi(h))(s)$? Note checking functions are equal is equivalent to checking that the functions have the same value for all input. $LHS = (gh).s = g.(h.s) = RHS$. The definition ensures the G-set corresponding to ϕ is S, i.e. $g.s = (\phi(g))(s)$.

Let G be a group and S_1, S_2 be G-sets.

Definition 14.2 (Equivariance). A morphism of G-sets is a function $\psi : S_1 \longrightarrow S_2$ satisfying axiom: for any $g \in G$, $s \in S$, we have $g.\psi(s) = \psi(g.s)$ ($g.s \in S_1$, $\psi(s) \in S_2$). In this case, we also say ψ is G-equivariant or that ψ is compatible with the G-action.

Note that equivariant maps are like linear operators preserving scalar multiplication over vector spaces, i.e. $T(\lambda \mathbf{x}) = \lambda T(\mathbf{x})$.

Example 14.5. Back to Example 14.1 yet again. Let S_A, S_B be G-sets corresponding to ϕ_A and ϕ_B, i.e. $S_A = S_B = \mathbb{R}^2$. Recall $G = \{1, g\}$. Claim $\psi : S_A \longrightarrow S_B; (x, y) \longmapsto (y, x)$ is a morphism of G-sets. Check for $s \in S_A$, the axiom holds. $\psi(1.s) = \psi(s) = 1.\psi(s)$. Also $\psi(g.(x, y)) = \psi(\phi_A(g)(x, y)) = \psi(-x, y) = (y, -x) = \phi_A(g)(y, x) = g.\psi(x, y)$.

Proposition - Definition 14.2 (Isomorphism Of Morphism). A morphism $\psi : S_1 \longrightarrow S_2$ of G-sets is an isomorphism if it is bijective. In this case ψ^{-1} is G-invariant too.

Proof. Same as for isomorphisms of groups.

Example 14.6. $\psi : S_A \longrightarrow S_B$ is bijective as well, so is an isomorphism of G-sets.

15 Orbits & Stabilisers

Example 15.1. We have a permutation representation of $G = O_3$ defined by $G = O_3 \hookrightarrow GL_3(\mathbb{R}) \hookrightarrow \text{Perm}(\mathbb{R}^3)$. $\mathbb{R}^3$ is a G-set in this way, $A.\mathbf{x} = A\mathbf{x}$ for $A \in O_3$, $\mathbf{x} \in \mathbb{R}^3$.

Proposition - Definition 15.1 (G-Stable Subset). Let S be a G-set. A subset $T \subseteq S$ is said to be G-stable if for any $g \in G$, $t \in T$, we have $g.t \in T$. In this case, the group action restricted to T make T a G-set.

Proof. Same as for subgroups.

Example 15.2. $G = O_3$, $S = \mathbb{R}^3$. Let $T = \{\mathbf{v} : \|\mathbf{v}\| < 1\} \subseteq S$, i.e. T is the unit ball. Now T is G-stable, why? If $A \in O_3$, then $\|A\mathbf{v}\| = \|\mathbf{v}\|$. So unit ball T is a G-set.

If $T \subseteq S$ is G-stable then the inclusion $T \hookrightarrow S$ is a morphism of G-sets. Let S be a G-set. We define a relation $\sim$ on S by $s \sim s'$ if there is some $g \in G$ such that $s = g.s'$.

Proposition 15.1. The relation $\sim$ is an equivalence relation.

Proof. Check reflexivity. For $s \in S$, $1.s = s$. $\therefore s \sim s$, as $1 \in G$. Check symmetry. Suppose $s \sim s'$, so $s = g.s'$ for some $g \in G$. Then $s' = 1.s' = (g^{-1}g).s = g^{-1}(g.s') = g^{-1}.s \implies s' \sim s$. Check transitivity. Suppose $s \sim s'$, $s' \sim s''$, so say $g, g' \in G$ are such that $s = g.s'$, $s' = g'.s''$. Then $s = g.s' = g.(g'.s'') = (gg').s''$ (by associativity). Hence $\sim$ is an equivalence relation.

Proposition - Definition 15.2 (G-Orbits). The set of equivalence classes are called the G-orbits. The G-orbit containing $s \in S$ is $G.s = \{g.s : g \in G\}$. Then S is disjoint union of orbits and the set of orbits is denoted by S/G (perhaps $G\backslash S$ is a better notation).

Example 15.3. O_3 acts on $\mathbb{R}^3$ via $O_3 \hookrightarrow \text{Perm}(\mathbb{R})$. Let $\mathbf{v} \in \mathbb{R}^3$ have length d. Let S_d be the sphere of radius d, centred $\mathbf{0}$. Since for $A \in O_3 = G$, $A\mathbf{v} \in S_d$. So $G.\mathbf{v} \subseteq S_d$. But given another $\mathbf{w} \in S_d$, we can rotate $\mathbf{w}$ onto $\mathbf{v}$, i.e. $S_d \subseteq G.\mathbf{v}$. Hence the orbit of $\mathbf{v}$ is $G.\mathbf{v} = S_d$. Also we have that $\mathbb{R}^3 = \dot{\bigcup}_{d \geq 0} S_d$.

Proposition 15.2. Let S be a G-set and $s \in S$. Then $G.s$ is the smallest G-stable subset of S containing s.

Proof. Firstly "closure " axioms imply $G.s$ lies in any G-stable subset containing s. It is suffice now to check $G.s$ is G-stable. Let $g, h \in G$. Then for any $h.s \in G.s$, $g.(h.s) = (gh).s \in G.s$ (by associativity). $\therefore G.s$ is G-stable.

Definition 15.1. We say that G acts transitively on S if S consists of just one orbit.

Example 15.4. Let $G = GL_n(\mathbb{C})$. G acts on $S = M_n(\mathbb{C})$, the set of $n \times n$ matrices over $\mathbb{C}$, by conjugation, i.e. $\forall\ A \in G = GL_n(\mathbb{C})$, $M \in S$, $A.M = AMA^{-1}$. Let us check indeed this gives a group action. Check axioms. (i) $I_n.M = I_n M I_n^{-1} = M$. (ii) $A.(B.M) = A.(BMB^{-1}) = ABMB^{-1}A_1 = (AB)M(AB)^{-1} = (AB).M$. What are the orbits? $G.M = \{AMA^{-1} : A \in GL_n(\mathbb{C})\}$. The theory of Jordan canonical forms aims to find a nice representation in this orbit.

Let S be a G-set.

Definition 15.2 (Stabiliser). The stabiliser of S is $\text{stab}_G(s) = \{g \in G : g.s = s\} \subseteq G$.

Proposition 15.3. Let S be a G-set and $s \in S$. Then $\text{stab}_G(s) \leq G$.

Proof. Check axioms. (i) $1.s = s \implies 1 \in \text{stab}_G(s)$. (ii) Suppose $g, h \in \text{stab}_G(s)$, $(gh).s = g.(h.s) = g.s = s$ (by associativity) $\implies gh \in \text{stab}_G(s)$. (iii) If $g \in \text{stab}_G(s)$ then $g.s = s \implies g^{-1}.s = g^{-1}.(g.s) = (g^{-1}g).s = 1.s = s$. So $g^{-1} \in \text{stab}_G(s)$. $\therefore \text{stab}_G(s) \leq G$.

Example 15.5. Let $G = SO_3 = SL_3 \cap O_3$. It acts on $\mathbb{R}^3$ via permutation representation $SO_3 \hookrightarrow GL_3 \hookrightarrow \text{Perm}(\mathbb{R}^3)$. Let $\mathbf{v} \in \mathbb{R}^3 - \{\mathbf{0}\}$. $\text{stab}_G(\mathbf{v})$ = groups of rotations about axis through $\mathbf{v}$ and $-\mathbf{v} \cong SO_2(\mathbb{R})$.

Note that isomorphic G-sets also have isomorphic orbits and stabilisers of corresponding elements equal.

Example 15.6. Back to Example 14.1. (A) has lots of one point orbits, i.e. on the line of symmetry, while (B) has only a single one point orbit at the centre of mass. Thus they are not isomorphic G-sets.

16 Structure Of Orbits & Platonic Solids

The stereotypical example of a transitive G-action is the G-set G/H. Let $H \leq G$.

Proposition 16.1. The set G/H is a G-set when endowed with group action $g'.(gH) = g'gH$ for $g, g' \in G$, $gH \in G/H$.

Proof. Just check axioms. (i) $1.(gH) = gH$ (ii) Need for any $g, g', g'' \in G$, $g''.(g'.(gH)) = (g''g')(gH)$. $LHS = g''.(g'gH) = g''g'gH = (g''g')gH = RHS$. $\therefore G/H$ is a G-set.

Theorem 16.1 (Structure Of G-Orbits). Let a group G act transitively on a set S. Let $s \in S$ and $H = \text{stab}_G(s) \leq G$. Then we have the following well defined isomorphism of G-sets $\psi : G/H \longrightarrow S; gH \longmapsto g.s$.

Proof. Let us check ψ is well defined, i.e. for $g \in G$, $h \in H$, need to check $g.s = g.(h.s) = (gh).s$ since $h \in \text{stab}_G(s)$. Check ψ is equivariant, i.e. for $g, g' \in G$, $\psi(g'.(gH)) = g'.\psi(gH)$. $LHS = \psi(g'gH) = (g'g).s = g'.(g.s) = RHS$ due to associativity. ψ is surjective as $S = G.s$ (G transitive on $S \implies S$ is an orbit). Check ψ is injective. So suppose $g, g' \in G$ such that $\psi(gH) = \psi(g'H)$ then $g.s = g'.s \implies s = g^{-1}(g'.s) = (g^{-1}g').s$. So $g^{-1}g' \in H$, i.e. a stabiliser of s. $\therefore g' \in gH \implies g'H = gH$, i.e. ψ is injective, completing proof that ψ is an isomorphism of G-sets.

Corollary 16.1. If G is finite then $|G.s| \mid |G|$.

Proof. By Theorem 16.1, $G.s \cong G/H$ and by Lagrange's Theorem, $|G| = |G/H||H| \implies |G.s| \mid |G|$.

Example 16.1. As in Example 15.5, we let $G = SO_3$ act transitively on the unit sphere $S = S^2$. Pick $s \in S$. $H = \text{stab}_G(s) \cong SO_2$ (rotate about s, $-s$ axis). Theorem 16.1 $\implies S^2 \cong G/H = SO_3/SO_2$ as G-sets. Note that the SO_2 changes with choices of s.

Proposition 16.2. Let S be a G-set and $s \in S$ and $g \in G$. Then $\text{stab})_G(g.s) = g\text{stab}_G(s)g^{-1}$.

Proof. Note this is saying that the axis of new points is obtained by changing the coordinates, i.e. conjugation of the original axis. Suffice to prove $\text{stab}_G(g.s) \supseteq g\text{stab}_g(s)g^{-1}$. For this result applied to g^{-1} for g and $g.s$ for s gives $\text{stab}(g^{-1}.(g.s)) \supseteq g^{-1}\text{stab}_G(g.s)g \implies \text{stab}_G(g.s) \subseteq g\text{stab}_G(s)g^{-1}$, which is the reverse inclusion. So we prove that $\text{stab})_G(g.s) \supseteq g\text{stab}_G(s)g^{-1}$. Let $h \in \text{stab}_G(s)$, we need to show $ghg^{-1} \in \text{stab}_G(g.s)$. But $(ghg^{-1}).(g.s) = (gh).s = g.(h.s) = g.s$ ($h \in \text{stab}_G(s)$), i.e. $ghg^{-1} \in \text{stab}_G(s)$ and $\text{stab}_G(g.s) \supseteq g\text{stab}_G(s)g^{-1}$ holds, giving the proposition.

Corollary 16.2. Let $H_1, H_2 \leq G$ be conjugate subgroups. Then $G/H_1 \cong G/H_2$ as G-sets.

Note the converse is also true and is a good exercise, i.e. if two G-sets are isomorphic, then H_1, H_2 must be conjugates.

Platonic solids are solids where all faces are congruent regular polygons and the same number of faces meet at each vertex. There are 5 Platonic solids: tetrahedron (T) ha 4 triangular faces, cube (C) had 6 square faces, octahedron (O) has 8 triangular faces, dodecahedron (D) has 12 pentagonal faces and icosahedron (I) has 20 triangular faces.

Definition 16.1 (Group Of Rotational Symmetries Of Platonic Solids). Let S be a Platonic solid with centre of mass $\mathbf{0}$, its group of symmetries $G \leq O_2$ (since $T \in G \Longrightarrow T(\mathbf{0}) = \mathbf{0}$, i.e. fixed centre of mass). The rotational group of symmetries of S is $H = G \cap SO_3$.

Proposition 16.3. Let S be Platonic solid as defined above and G be its rotational group of symmetries. Then $|G|$ = number of faces of $S \times$ number of edges in each face.

	Tetrahedron	Cube	Octahedron	Dodecahedron	Icosahedron
$\lvert G\rvert$	12	24	24	60	60

Proof. Let F = set of faces of S. G permutes the faces, so get permutation representation $G \hookrightarrow \mathrm{Perm}(F)$, since G is linear. So we get G-set F. Let $f \in F$ be a face. Note $F = G.f$ is an orbit, since we can rotate any faces to any other faces. By Theorem 16.1, $G.f \cong G/\mathrm{stab}_G(f)$. What is $\mathrm{stab}_G(f)$? It is the set of rotations about axis through centre of f and centre of S, i.e $\mathbf{0}$. Hence $|\mathrm{stab}_G(f)|$ = number of edges of f = number of edges in each face. Then $|G.f| = \frac{|G|}{|\mathrm{stab}_G(f)|}$. Hence number of faces of $S = \frac{|G|}{\text{number of edges in each face}}$. This gives the proposition.

17 Counting Orbits & Cayley's Theorem

Let S be a G-set.

Definition 17.1 (Fixed Point Set). Let $J \subseteq G$, the fixed point set of J is $S^J = \{s \in S : j.s = s \text{ for all } j \in J\}$.

Example 17.1. $G = \mathrm{Perm}(\mathbb{R}^2)$ acts naturally on $S = \mathbb{R}^2$. Let $\tau_1, \tau_2 \in G$ be reflections about lines L_1, L_2. Then $S^{\tau_i} = L_i$ and $S^{\{\tau_1,\tau_2\}} = L_1 \cap L_2$.

Proposition 17.1. Let S be a G-set. Then

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

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

Proof. (i) Logically clear. (ii) Exercise.

Example 17.2. In Example 17.1, $S^{\langle \tau_1,\tau_2 \rangle} = L_1 \cap L_2$.

Note that fixed point set are the same for isomorphic G-sets.

Theorem 17.1 (Counting Orbits). 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. Suppose $S = \dot{\bigcup}_i S_i$, where S_i are G-stable, e.g. S_i are G-orbits. Then $S^g = \dot{\bigcup}_i S_i^g$. So $LHS = \sum_i$ number of orbits of S_i (since S_i's are union of G-orbits and S_i's are disjoint) while $RHS = \sum_i \frac{1}{|G|} \sum_{g \in G} |S_i^g|$. $\therefore$ Suffice to prove theorem for $S = S_i$ and then just sum over i. But $S =$ disjoint union of G-orbits, so can assume $S = S_i =$ G-orbit, which by Theorem 16.1, means $S \cong G/H$ for some $H \leq G$. So in this case

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

Note by Proposition 16.2, these stabilisers are all conjugates, and hence all have the same size. Since $|\text{stab}_G(1.H)| = |H|$, $|\text{stab}_G(s)| = |H|$ 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 17.3 (Application To Birthday Cake Problem). Divide the round birthday cake into 8 equal sectors. Place red or green candle in centre of each sector. Question is how many essentially different ways are there of doing this? More precisely, let $S = (\mathbb{Z}/2\mathbb{Z})^8$. Let $\sigma \in \text{Perm}(S)$ be defined by $\sigma(x_0, x_1, \ldots, x_7) = (x_1, x_2, \ldots, x_7, x_0)$. Note σ generates a cyclic subgroup G of order 8. Want to find number of G-orbits in G-set S. Use Theorem 17.1 to compute S^g. $S^1 = S \Longrightarrow |S^1| = 2^8$, $S^\sigma = \{(0, 0, \ldots, 0), (1, 1, \ldots, 1)\} \Longrightarrow |S^\sigma| = 2$, i.e. all colours the same. Similarly $S^{\sigma^2} = \{(0, 0, \ldots, 0), (1, 1, \ldots, 1), (0, 1, 0, \ldots, 0, 1), (1, 0, 1, \ldots, 1, 0)\}$, i.e. when fixed by σ^2, $\mathbf{x} \in S$ is determined by x_0 and x_1. $\therefore |S^{\sigma^2}| = 4$. Using the same idea, $S^{\sigma^3} = S^{\langle \sigma^3 \rangle} = S^{\langle \sigma \rangle} \Longrightarrow |S^{\sigma^3}| = 2$, $|S^{\sigma^4}| = 2^4 = 16$, $|S^{\sigma^5}| = 2$, $|S^{\sigma^6}| = |S^{\sigma^2}| = 4$, $|S^{\sigma^7}| = 2$. By Theorem 17.1, the number of orbits $= \frac{1}{8}(2^8 + 2 + 4 + 2 + 16 + 2 + 4 + 2) = \frac{1}{8}(2^8 + 8 + 8 + 16) = 2^5 + 4 = 36$.

Definition 17.2 (Faithful Permutation Representation). A permutation representation $\phi : G \longrightarrow \text{Perm}(S)$ is faithful if $\ker(\phi) = 1$.

Theorem 17.2 (Cayley's Theorem). Let G be a group. Then G is isomorphic to a subgroup of $\text{Perm}(G)$. In particular, if $|G| = n < \infty$, then G is isomorphic to a subgroup of S_n.

Proof. Consider G-set $G = G/1$. This gives permutation representation $\phi : G \longrightarrow \text{Perm}(G)$. We seek to show this is faithful. So suppose $g \in \ker(\phi)$, so $\phi(g) = 1_{\text{Perm}(G)} = \text{id}_G$. Note $g = g.1 = (\phi(g))(1) = \text{id}_G(1) = 1 \Longrightarrow \ker(\phi) = 1$ and ϕ is faithful. This shows G is isomorphic to $\text{Im}(\phi) \leq \text{Perm}(G)$. We know finally that it $|G| = n$ is finite, then $\text{Perm}(G) \cong \text{Perm}(\{0, 1, \ldots, n-1\}) = S_n$, since G is bijective with $\{0, 1, \ldots, n-1\}$.

18 Finite Groups Of Isometries I

Recall that any finite group G of isometries on $\mathbb{R}^n$ embed in O_n.

Lemma 18.1. Let $H \leq SO_2$ have order n, finite. Then H is cyclic group generated by the rotation σ about angle $\frac{2\pi}{n}$.

Proof. OK if $n = 1$, i.e. $\sigma = \text{id}$. Assume $n > 1$. Pick $\sigma \in H$, rotation anti-clockwise about angle θ where θ is the minimal positive such amongst all possibilities. We first show $\langle\sigma\rangle = H$. We know $\langle\sigma\rangle \subseteq H$ holds by closure. Suppose $h \in H$ is a rotation anticlockwise about angle θ'. Pick integer m so that $m\theta \leq \theta' \leq (m+1)\theta$. Note $\sigma^{-m}h \in H$ is a rotation anticlockwise about angle $0 \leq \theta' - m\theta < \theta$. Minimality of $\theta \implies \theta' - m\theta = 0$ so $\theta' = m\theta \implies h = \sigma^m \in \langle\sigma\rangle$. hence $H = \langle\sigma\rangle$. It remains to check $\theta = \frac{2\pi}{n}$. Pick an integer l, so $l\theta \leq 2\pi < (l+1)\theta$. Since $\sigma^{-l} \in H$ is a rotation anticlockwise about angle $0 \leq 2\pi - l\theta < \theta$, minimality of $\theta \implies 2\pi = l\theta$. We must have $l = n$ so $\theta = \frac{2\pi}{n}$. This proves the lemma.

Theorem 18.1 (Subgroups Of O_2). Any subgroup G of O_2 is cyclic or dihedral.

Proof. The subgroups will be described explicitly in the proof. Note that by dihedral, we always mean isomorphic to the group D_n. If $G \leq O_2$ is finite and is also in SO_2, we just apply Lemma 18.1. Assume $G \not\leq SO_2$ and let $\tau \in G - SO_2$. τ is a reflection about say line L. Rotate to change coordinates so that L is horizontal. This does not change the isomorphic class of G. Then $\tau = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Let $H = G \cap SO_2 \leq SO_2$.By Lemma 18.1, $H = \langle\sigma\rangle$, where σ is the rotation anticlockwise about angle $\frac{2\pi}{n}$ for some n. $\therefore D_n$ satisfies $G \leq D_n$ as $G \subseteq \langle\tau, \sigma\rangle = D_n$. Note $G/H = \frac{G}{G\cap SO_2} \hookrightarrow O_2/SO_2 \cong \{SO_2, \tau SO_2\} \cong \mathbb{Z}/2\mathbb{Z} \implies |G/H| = |\mathbb{Z}/2\mathbb{Z}| = 2$. $\because H \in G/H$, $\tau \in G$, $\tau \notin H$ $\therefore G/H = \{H, \tau H\}$. Hence every element in G has form σ^i or $\tau\sigma^i$, i.e. $G \leq D_n$ too. So G is dihedral.

Theorem 18.2 (Subgroups Of SO_3). Any finite subgroup of SO_3 is either cyclic, dihedral or the rotational symmetry group of a Platonic solid.

Proof. The proof of the theorem requires some new concepts.

Recall any $G \leq SO_3$ acts on the unit sphere $T \subseteq \mathbb{R}^3$.

Definition 18.1 (Pole). A pole of G is some $t \in T$ such that $\text{stab}_G(t) \neq 1$.

Proposition 18.1. The set S of poles of G is G-stable.

Proof. By Proposition 16.2, $\text{stab}_G(g.t) = g\text{stab}_G(t)g^{-1}$.

We can find all poles of a Platonic solid. Let G be the rotational symmetry group of a Platonic solid. It looks like you have face poles corresponding to centres of faces, vertex poles corresponding to vertices, and edge poles to centre of edges. Also it seems like face poles form an orbit, edge poles form an orbit and form vertex poles form an orbit.

Lemma 18.2 (Platonic Triples). An integer triple (n_1, n_2, n_3) ia a Platonic triple if $1 \leq n_1 \leq n_2 \leq n_3$ and $\sum_i \frac{1}{n_i} > 1$. The possibilities are $(n_1, n_2, n_3) = (2, 2, n), (2, 3, 3), (2, 3, 4), (2, 3, 5)$ for $n \geq 2$.

Proof. Suppose $n_1 \geq 3$, then $\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} \leq \frac{1}{3} + \frac{1}{3} + \frac{1}{3} = 1 \Longrightarrow n_1 = 2$. If $n_2 \geq 4$, then $\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} \leq \frac{1}{2} + \frac{1}{4} + \frac{1}{4} = 1 \Longrightarrow n_2 = 2$ or 3. If $n_2 = 2$, then n_3 is anything. Suppose $n_2 = 3$. If $n_3 \geq 6$, then $\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} \leq \frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1$. So the only possibilities are those given above. It is easily checked that they are all indeed Platonic.

Centres of faces of a cube are the vertices of an octahedron. Similarly centres of faces of an octahedron are the vertices of a cube. Hence say octahedron and cube are duals. Similarly icosahedron and dodecahedron are duals. Tetrahedron is self dual. It is clear that if F, F' are dual Platonic solids, their rotational symmetry groups are isomorphic. Why? If T is a symmetry of F, it takes centres of faces of F to centres of faces of F, i.e. vertices of F' to vertices of vertices of F'.

19 Finite Groups Of Isometries II

Theorem 19.1 (Subgroups Of SO_3). Any finite subgroup G of SO_3 is either cyclic, dihedral or the rotational symmetry group of a Platonic solid.

Proof. We consider the G-set S of poles of G and decompose it into G-orbits, i.e. $S = G.s_1 \dot\cup G.s_2 \dot\cup \ldots \dot\cup G.s_r$, we see that each G-orbit is finite later. Apply Theorem 17.1 on counting orbits. For $g \in G$,

$$S^g = \begin{cases} \text{the two poles of rotation} & \text{if } g \neq 1 \\ S & \text{if } g = 1 \end{cases}$$

So by Theorem 17.1, we have

$$\begin{aligned} r &= \text{number of orbits} \\ &= \frac{1}{|G|} \sum_{g \in G} |S^g| \\ &= \frac{1}{|G|}(2 \times (|G| - 1) + |S|) \quad \text{(2 poles of rotation for the non-identity, and everything for the identity)} \\ &= 2 - \frac{2}{|G|} + \sum_{i=1}^{r} \frac{1}{|\text{stab}_G(s_i)|} \quad \text{(since } |S| = \sum_{i=1}^{r} |G.s_i| = \sum_{i=1}^{r} \frac{|G|}{|\text{stab}_G(s_i)|}\text{, due to } G.s_i \cong G/\text{stab}_G(s_i)\text{)} \end{aligned}$$

Hence we can get

$$2 - \frac{2}{|G|} = \sum_{i=1}^{r} \frac{|G|}{\text{stab}_G(s_i)}$$

Since s_i is a pole, i.e. $\text{stab}_G(s_i) \neq 1$, each summand $1 - \frac{1}{|\text{stab}_G(s_i)|} \geq 1 - \frac{1}{2} = \frac{1}{2}$. But $LHS = 2 - \frac{2}{|G|} < 2$. Thus $r \leq 3$. We can also show that $r \neq 1$. Suppose $r = 1$, then $RHS = 1 - \frac{1}{|\text{stab}_G(s_i)|} \in (0, 1)$. But $LHS \in (1, 2)$ as $|G| \geq |\text{stab}_G(s_1)| \geq 2 \Longrightarrow 2 - \frac{2}{|G|} \geq 2 - \frac{2}{2} = 1$. So we have only two case, $r = 2$ and $r = 3$. For $r = 2$ case, $\text{stab}_G(s_i) \leq G \Longrightarrow 1 - \frac{1}{|\text{stab}_G(s_i)|} \leq 1 - \frac{1}{|G|}$ with equality if and only if $G = \text{stab}_G(s_i)$. But we also have

$$\sum_{i=1}^{2}(1 - \frac{1}{|\text{stab}_G(s_i)|}) = 2 - \frac{2}{|G|} = 2(1 - \frac{1}{|G|})$$

We must have equality and so $G = \text{stab}_G(s_i)$. So G must be the cyclic group of rotations about s_i, $-s_i$ axis. And furthermore, we must have $s_1 = -s_2$, i.e. $\{s_1, s_2\} = \{s_i, -s_i\}$. For the $r = 3$ case, we have

$$2 > 2 - \frac{2}{|G|} = \sum_{i=1}^{3}(1 - \frac{1}{|\text{stab}_G(s_i)|})$$

Let $n_i = |\text{stab}_G(s_i)|$ and reorder so $n_1 \leq n_2 \leq n_3$. We have $2 > 3 - \frac{1}{n_1} - \frac{1}{n_2} - \frac{1}{n_3}$ or $\sum_{i=1}^{3} \frac{1}{n_i} > 1$. Hence (n_1, n_2, n_3) is a Platonic triple. Note also $n_1 = |\text{stab}_G(s_1)| \geq 2$. From Lemma 18.2, there are four possibilities for (n_1, n_2, n_3), namely

(i) $(2, 2, n)$ (claim to be dihedral)

(ii) $(2, 3, 3)$ (claim to be a tetrahedron)

(iii) $(2, 3, 4)$ (claim to a cube or an octahedron)

(iv) $(2, 3, 5)$ (claim to be dodecahedron or an icosahedron)

20 Rings

You can add and multiply two integers, polynomials and $n \times n$ matrices. Further, addition and multiplication give similar arithmetic in all three cases. We have abstract common principles in the notion of rings.

Definition 20.1 (Ring). An abelian group R, say with group addition $+$, is called a ring when it is endowed with a ring multiplication map $\mu : R \times R \longrightarrow R; (r, s) \longmapsto \mu(r, s) = rs$ satisfying axioms.

(i) Associativity, for any $r, s, t \in R$, $(rs)t = r(st)$

(ii) Multiplication identity, there is an element $1_R \in R$ such that for any $r \in R$, we have $1_R r = r = r1_R$

(iii) Distributivity, for $r, s, t \in R$, we have $r(s + t) = rs + rt$ and $(s + t)r = sr + tr$

Note that some people do not insist on axiom (ii) and call those rings with (ii) unital. Other things to note is that we have uniqueness of multiplication identity 1_R as usual and for any $r \in R$, $0r = 0 = r0$.

Example 20.1. $\mathbb{C}$ is a ring with ring addition and ring multiplication equal to the usual addition and multiplication of numbers.

Example 20.2. Let X be a set and R be a ring. Let $\text{Fun}(X, R)$ be the set of function from X to R. Then $\text{Fun}(X, R)$ is a ring when endowed with pointwise addition and multiplication, i.e. for $f, g : X \longrightarrow R$, $x \in X$, $(f+g)(x) = f(x)+g(x) \in R$ and $(fg)(x) = f(x)g(x) \in R$ as $f(x), g(x) \in R$. Then $0 =$ constant map to 0, $1 =$ constant map to 1. Usually checking the axioms involve checking the equations hold pointwise. So we can check ring axioms for R implies that we can check ring axioms for $\text{Fun}(X, R)$.

Example 20.3. Let V be a vector space over $\mathbb{C}$. Define $\mathrm{End}_{\mathbb{C}}(V)$ to be the set of linear maps $T : V \longrightarrow V$. Then $\mathrm{End}_{\mathbb{C}}(V)$ is a ring when endowed with ring addition 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 20.1 (Subring). A subset S of a ring R is a subring if it satisfies the following closure axioms.

(i) $s + s' \in S$ for any $s, s' \in S$

(ii) $ss' \in S$ for any $s, s' \in S$

(iii) $-s \in S$ for any $s \in S$

(iv) $0_R \in S$

(v) $1_R \in S$

In another word, it is a subgroup closed under multiplication and has an one. In this case, the ring addition and multiplication on R restricted to S make S a ring with $1_S = 1_R$.

Example 20.4. $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ are all subrings of $\mathbb{C}$. Also the set of Gaussian integers $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ is a subring, simply check axiom.

Example 20.5. $\mathrm{Fun}(\mathbb{R}^n, \mathbb{R})$ has subring $\mathcal{C}(\mathbb{R})$ of continuous functions and $\mathcal{C}^k(\mathbb{R})$ of k fold differentiable functions.

Example 20.6. $\mathrm{Fun}(\mathbb{C}^n, \mathbb{C})$ had subrings $\mathbb{C}[x_1, x_2, \ldots, x_n]$ of complex polynomial functions in n variables and $\mathbb{R}[x_1, x_2, \ldots, x_n]$ of real polynomial functions in n variables.

Example 20.7. We know that the set of $n \times n$ real or complex matrices $M_n(\mathbb{R})$ and $M_n(\mathbb{C})$ form a ring. The set of upper triangular matrices form a subring.

Proposition 20.1. Two useful observations are

(i) Subrings of subrings are subrings

(ii) The intersection of subrings is a subring

Proof. Just check axioms. We will only do (ii) as an example. Let S_i be a subring of R, $i \in I$. S_i a subgroup of $R \Longrightarrow \bigcap_i S_i$ is a subgroup. Also $1_R \in \bigcap_i S_i$ as $1_R \in S_i \ \forall i$. Also if $s, s' \in S_i \Longrightarrow ss' \in S_i$ for each $i \Longrightarrow ss' \in \bigcap_i S_i$. Thus $\bigcap_i S_i$ is a subring.

Proposition - Definition 20.2 (Invertibility). An element u of a ring R is a unit or invertible if there is some $v \in R$ with $uv = 1_R = vu$. We write R^* for the set of these. Usually we write u^{-1} for v since we have uniqueness of inverses and R^* forms a group under ring multiplication.

Proof. We prove only here R^* is a group. For $u, v \in R^*$, $uv \in R^*$ since $v^{-1}u^{-1}uv = v^{-1}v = 1 = uvv^{-1}u^{-1}$. Hence ring multiplication induces group multiplication map $R^* \times R^* \longrightarrow R^*$. Existence of inverse is hypothesised, i.e. $u \in R^* \Longrightarrow u^{-1} \in R*$. 1_R is the group identity. Associativity is from ring axioms.

Example 20.8. $\mathbb{Z}^* = \{1, -1\}$ and $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$

Definition 20.2 (Commutative Ring). A ring R is commutative if $rs = sr$ for all $r, s \in R$.

Definition 20.3 (Field). A commutative ring R is a field if $R^* = R - 0$.

21 Ideals & Quotient Rings

Let R be a ring.

Definition 21.1 (Ideals). A subgroup I of the underlying abelian group R is called an ideal of for any $r \in R$, $x \in I$, we have $rx \in I$, $xr \in I$. Then we write $I \trianglelefteq R$.

Note that I may not contain 1, so it may not be subring.

Example 21.1. $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ 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.

Example 21.2. Let $Y \subseteq \mathbb{C}^n$. The ideal of polynomials zero on Y is $I(Y) = \{f \in \mathbb{C}[x_1, x_2, \ldots, x_n] : f(\mathbf{y}) = 0 \text{ for all } \mathbf{y} \in Y\}$. Then $I(Y) \trianglelefteq \mathbb{C}[x_1, x_2, \ldots, x_n]$. Check that this is a subgroup of $\mathbb{C}[x_1, x_2, \ldots, x_n]$. Let $f \in I(Y)$, $p \in \mathbb{C}[x_1, x_2, \ldots, x_n]$, $\mathbf{y} \in Y$ then $(fp)(\mathbf{y}) = f(\mathbf{y})p(\mathbf{y}) = 0 = (pf)(\mathbf{y})$ as $f \in I$. So by definition, $fp \in I(Y)$ and $pf \in I(Y)$. Thus $I(Y)$ is an ideal.

Generating ideals are similar to generating subgroups and spanning vector spaces.

Proposition 21.1. Let $I_i \trianglelefteq R$ for $i \in I$ then $\bigcap_i I_i \trianglelefteq R$.

Proof. Just check axioms as for subgroups or subrings. $I_i \trianglelefteq R \Longrightarrow I_i \leq R \Longrightarrow \bigcap_i I_i \leq R$. Now for $x \in \bigcap_i I_i$, $r \in R$, we have $x \in I_i$ for $i \in I$. Hence $xr, rx \in I_i$ for all i as it is an ideal. Hence $xr, rx \in \bigcap_i I_i \Longrightarrow \bigcap_i I_i \trianglelefteq R$.

Corollary 21.1. Let R be a ring and $S \subseteq R$. Let J be the set of all ideals $I \trianglelefteq R$ containing S. The ideal generated by S is $\langle S \rangle = \bigcap_{I \in J} I$.

Note that $\langle S \rangle$, unique smallest one, is an ideal of R containing S and $\langle S \rangle$ is contained in any $I \in J$. To compute this, we use ...

Proposition 21.2. Let R be a ring.

(i) Let I, J be ideals of R. The ideal generated by $I \cup J$ is $I + J = \{i + j : i \in I, j \in J\}$.

(ii) Let $x \in R$ and R be a commutative ring, then $\langle x \rangle = Rx = \{rx : r \in R\} \subseteq R$.

(iii) For R commutative and $x_1, x_2, \ldots, x_n \in R$, we have $\langle x_1, x_2, \ldots, x_n \rangle = Rx_1 + Rx_2 + \ldots + Rx_n =$ set of all R-linear combinations of $x_1, x_2, \ldots, x_n$.

Proof. Note $\langle x \rangle \supseteq Rx$ by definition. $x \in Rx$, so since $\langle x \rangle$ is the unique smallest ideal containing x, it suffices to show Rx is an ideal containing x and then we will have $\langle x \rangle \subseteq Rx$. Check it is a subgroup. (a) $0 = 0.x \in Rx$. (b) If $r, s \in R$, then $rx + sx = (r + s)x \in Rx$. (c) If $r \in R$, note $(-r)x + rx = (-r + r)x = 0x = 0 \Longrightarrow -(rx) = (-r)x \in Rx$ as $-r \in R$. Thus Rx is a subgroup. Check Rx is an ideal. let $r \in R$, so $rx \in Rx$. If $s \in R$ then $s(rx) = (sr)x \in Rx$. Hence by commutativity, $Rx \trianglelefteq R$ and (ii) is proved. (i) is proved similarly by showing $I + J$ is an ideal. (iii) follows from (i) and induction on (ii).

Example 21.3. The ideal generated by $n \in \mathbb{Z}$ in $\mathbb{Z}$ is $n\mathbb{Z} = \mathbb{Z}n$.

Example 21.4. $R = \mathbb{C}[x_1, x_2, \ldots, x_n] \Longrightarrow \langle x_1, x_2, \ldots, x_n \rangle = \mathbb{C}[x_1, x_2, \ldots, x_n]x_1 + \mathbb{C}[x_1, x_2, \ldots, x_n]$ $x_2 + \ldots + \mathbb{C}[x_1, x_2, \ldots, x_n]x_n =$ set of polynomials with constant term $0 = \{f \in \mathbb{C}[x_1, x_2, \ldots, x_n] :$ $f(\mathbf{0}) = 0\} = I(\mathbf{0})$.

Note that the ideal $I \trianglelefteq R$ is also a normal subgroup of R since R is abelian.

Proposition - Definition 21.1 (Quotient Ring). Let $I \trianglelefteq R$. The abelian group R/I has a very well defined multiplication map $\mu : R/I \times R/I \longrightarrow R/I; (r + I, s + I) \longmapsto rs + I$, which makes R/I a ring called the quotient rig of R by I. Also $1_{R/I} = 1_R + I$.

Proof. Check μ is well defined, i.e. $x, y \in I$, 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 ring axioms for R/I follow from ring axioms for R.

Example 21.5. 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.

Example 21.6. $R = \mathbb{C}[x_1, x_2, \ldots, x_n]$, $I = \langle x_1, x_2, \ldots, x_n \rangle$. Note $\mathbb{C}[x_1, x_2, \ldots, x_n] = \dot{\bigcup}_{\alpha \in I}(\alpha + I) =$ union of set of all polynomials with constant α. Thus $R/I = \{\alpha + I : \alpha \in \mathbb{C}\}$. For $\alpha, \beta \in \mathbb{C}$, the ring operations are $(\alpha + I) + (\beta + I) = (\alpha + \beta) + I$ and $(\alpha + I)(\beta + I) = \alpha\beta + I$. Ring R/I just look like ring $\mathbb{C}$, i.e. R/I and $\mathbb{C}$ are isomorphic rings.

Example 21.7. Again let $Y \subseteq \mathbb{C}^n$. We define $\mathbb{C}[Y] = \mathbb{C}[x_1, x_2, \ldots, x_n]/I(Y)$. Let $f, g \in \mathbb{C}$ $[x_1, x_2, \ldots, x_n]$ with $f + I(Y) = g + I(Y) \iff f - g \in I(Y) \iff (f - g)(\mathbf{y}) = 0$ for all $\mathbf{y} \in Y \iff f_{|Y} = g_{|Y}$ (functions with domain restricted to Y). This shows $\mathbb{C}[Y]$ arises naturally as a subring of $\mathrm{Fun}(Y, \mathbb{C})$, i.e. restrict domain to Y.

22 Ring Homomorphisms I

Definition 22.1 (Homomorphism). Let R, S be rings. A ring homomorphism $\phi : R \longrightarrow S$ is group homomorphism $\phi : R \longrightarrow S$ of the underlying abelian groups such that

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

(ii) For $r, r' \in R$, $\phi(rr') = \phi(r)\phi(r')$

Example 22.1 (Quotient Morphism). Let $I \trianglelefteq R$, a ring. The quotient morphism $\pi : R \longrightarrow R/I; r \longmapsto r + I$ is a ring homomorphism. Why? We know π is a group homomorphism. Check now (i) $\pi(1_R) = 1_R + I = 1_{R/I}$ (ii) for $r, r' \in R$, check $\pi(rr') = \pi(r)\pi(r')$. $LHS = rr' + I = (r + I)(r' + I) = RHS$, since I is an ideal, i.e. $rI, r'I \subseteq I$.

Example 22.2 (Evaluation Homomorphism). Let S be a subring of $\mathrm{Fun}(X, R)$ where X is some set and R some ring. Let $x \in X$. The evaluation map $\varepsilon_x : S \longrightarrow R; f \longmapsto f(x)$ is a ring homomorphism. Why? Note (i) $\varepsilon_x(1_S) = \varepsilon_x(\text{constant function } 1) = 1_R$. For $f, g \in S$, we check (ii) $\varepsilon_x(f + g) = (f + g)(x) = f(x) + g(x) = \varepsilon_x(f) + \varepsilon_x(g)$ and (iii) $\varepsilon_x(fg) = (fg)(x) = f(x)g(x) = \varepsilon_x(f)\varepsilon_x(g)$.

Lemma 22.1. Composites of ring homomorphisms are ring homomorphisms.

Proof. Easy exercise.

Definition 22.2 (Isomorphism). A ring isomorphism is a bijective ring homomorphism $\phi : R \longrightarrow S$. In this case ϕ^{-1} is also a ring homomorphism. We write $R \cong S$ as rings.

Example 22.3. $\phi : \mathbb{C} \longrightarrow \mathbb{C}[x, y]/\langle x, y\rangle; \alpha \longmapsto \alpha + \langle x, y\rangle$ (coset of all polynomials with constant α) is a ring homomorphism, because we saw ϕ is bijective and for $\alpha, \beta \in \mathbb{C}$, $(\alpha + \beta) + \langle x, y\rangle = (\alpha + \langle x, y\rangle) + (\beta + \langle x, y\rangle)$ and $(\alpha + \langle x, y\rangle)(\beta + \langle x, y\rangle) = (\alpha\beta) + \langle x, y\rangle$ and $1 + \langle x, y\rangle$ is the identity.

Proposition 22.1. Let $\phi : R \longrightarrow S$ be a ring homomorphism.

(i) If R' is a subring of R the $\phi(R')$ 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 $\phi^{-1}(I) \trianglelefteq R$ (ideals)

Proof. Just check axioms. Let us do (iii). Suppose $I \trianglelefteq R$. $\phi^{-1}(I)$ is a subgroup of R. Suppose $x \in \phi^{-1}(I)$ and $r \in R$. We need to check that $rx, xr \in \phi^{-1}(I)$. But $\phi(rx) = \phi(r)\phi(x) \in I$ as $\phi(x) \in I$ (an ideal), $\phi(r) \in S$. Hence $rx \in \phi^{-1}(I)$. Similarly $xr \in \phi^{-1}(I)$. Hence $\phi^{-1}(I) \trianglelefteq R$. Note that $I \trianglelefteq R$ does not imply $\phi(I) \trianglelefteq S$, i.e. the image of an ideal may not be an ideal.

Corollary 22.1. Let $\phi : R \longrightarrow S$ be a ring homomorphism. Then $\text{Im}(\phi) = \phi(R)$ is a subring of S and $\ker(\phi) = \phi^{-1}(0)$ is an ideal in R.

Proof. Just note R is a subring of R, so must be $\phi(R)$ of S. $0 \trianglelefteq S$ since it is a subgroup and for $s \in S$, $s0 = 0 = 0s \in 0$. Hence $\phi^{-1}(0) \trianglelefteq R$.

Theorem 22.1 (First Isomorphism Theorem). Let R be a ring and $I \trianglelefteq R$ (ideal). Let $\pi : R \longrightarrow R/I$ be a quotient morphism of rings. Let $\phi : R \longrightarrow S$ be ring homomorphism with $\ker(\phi) \supseteq I$. The induced group homomorphism $\psi : R/I \longrightarrow S; r + I \longmapsto \phi(r)$ generated by the Universal Property Of Quotient Groups is also a ring homomorphism. In particular, setting $I = \ker(\phi)$, we find $R/I \cong \text{Im}(\phi)$ as ring isomorphism.

$$\begin{array}{ccc} R & \xrightarrow{\quad\phi\quad} & S \\ {\scriptstyle\pi}\searrow & & \nearrow{\scriptstyle\psi} \\ & R/I & \end{array}$$

$$\begin{array}{ccc} r & \longmapsto & \phi(r) \\ & \searrow \quad \nearrow & \\ & r + I & \end{array}$$

Proof. we know ψ is a group homomorphism, so we shall only check the ring homomorphism axioms. (i) $\psi(1_{R/I}) = \psi(1_R + I) = \phi(1_R) = 1_S$. (ii) For $r, r' \in R$, check $\psi((r + I)(r' + I)) = \psi(rr' + I) = \phi(rr') = \phi(r)\phi(r') = \psi(r + I)\psi(r' + I)$ as ϕ is an homomorphism for rings. Hence theorem is proved.

Example 22.4. $\mathbb{C} \cong \mathbb{R}[x]/\langle x \rangle$ ($\mathbb{R}[x]$ is polynomials in $\mathbb{R}$ with real coefficients) . Consider evaluation homomorphism $\varepsilon_i : \mathbb{R}[x] \longrightarrow \mathbb{C}; p(x) \longmapsto p(i)$. Note if $p(x) = ax + b$, $a, b \in \mathbb{R}$, then $p(i) = ai + b$. So ε_i is surjective. By the First Isomorphism Theorem, it suffices to show that $\ker(\varepsilon_i) = \langle x^2 + 1 \rangle$. Note $x^2 - 1 \in \ker(\varepsilon_i)$ as $i^2 + 1 = 0$. So $\langle x^2 + 1 \rangle \subseteq \ker(\varepsilon_i)$. For the reverse inclusion, suppose $p(x) \in \ker(\varepsilon_i)$, i.e. $p(i) = 0$. Write $p(x) = (x^2 + 1)q(x) + ax + b$, where $a, b \in \mathbb{R}$. $q(x)$ is a real polynomial, i.e. $q \in \mathbb{R}[x]$. Now $0 = p(i) = q(i)(i^2 + 1) + ai + b = ai + b$. Hence both a, b are zero. Hence $p(x) = q(x)(x^2 + 1) \in \mathbb{R}[x](x^2 + 1) = \langle x^2 + 1 \rangle$ and so $\ker(\varepsilon_i) = \langle x^2 + 1 \rangle$.

23 Ring Homomorphisms II

The idea is that knowing everything of a large group should give you everything about the quotient group. Now what about for rings?

Proposition 23.1. Let J be an ideal of ring R and $\pi : R \longrightarrow R/J$ be a quotient morphism. Then $\{\text{ideals } I \trianglelefteq R \text{ such that } I \supseteq J\} \longrightarrow \{\text{ideals } \bar{I} \trianglelefteq R/J\}; I \longmapsto \pi(I) = I/J$ and $\bar{I} \longmapsto \pi^{-1}(I)$ are inverse bijections. In particular, every ideal in R/J has form $\bar{I} = I/J$, where $I \trianglelefteq R$ such that $I \supseteq J$.

Proof. Very similar to classification of subgroups of quotient groups. In fact ideals are subgroups so that classification of subgroups of quotient groups say $I \longmapsto \pi(I)$, $\bar{I} \longmapsto \pi^{-1}(\bar{I})$ are inverses as long as they are well defined. If $\bar{I} \trianglelefteq R/J$ then $\pi^{-1}(\bar{I}) \trianglelefteq R$, so $\bar{I} \longmapsto \pi^{-1}(\bar{I})$ is well defined. Let $I \trianglelefteq R$ with $I \supseteq J$. We need now only show $I/J \trianglelefteq R/J$ so $I \longmapsto \pi(I)$ is well defined. We do know I/J is a subgroup of R/J. Let $x \in I$, $r \in R$. Then $(r + J)(x + J) = rx + J \in I/J$ as $rx \in I$ (since $I \trianglelefteq R$), for $r + J \in R/J$, $x + J \in I/J$. Similarly $(x + J)(r + J) = xr + J \in I/J$. This proves the proposition.

Definition 23.1 (Maximal Ideal). An ideal $I \trianglelefteq R$, with $I \neq R$, is maximal if it is maximal amongst ideals not equal to R, i.e. if $J \trianglelefteq R$ with $I \subseteq J$ then either $J = I$ or R.

Example 23.1. $10\mathbb{Z} \trianglelefteq \mathbb{Z}$ is not maximal as $10\mathbb{Z} \subsetneq 2\mathbb{Z} \trianglelefteq \mathbb{Z}$. However $2\mathbb{Z} \trianglelefteq \mathbb{Z}$ is maximal.

Proposition 23.2. Let $R \neq 0$ be a commutative ring.

(i) R is a field if and only if every ideal is maximal, i.e. 0 ideal is maximum

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

Proof. (ii) follows from Proposition 23.1 and (i). R/I is a field $\implies R/I$ contains R/I and 0 ideals only $\implies R$ has ideals R and I only $\implies I$ is maximal. Conversely $I \trianglelefteq R$, $I \neq R$, is maximal $\implies R/I$ has ideals of the form J/I where $I \trianglelefteq J \leq R \implies J = I$ or R as I is maximal $\implies R$ has only ideals R and 0, and hence is a field by (i). Let us prove (i). Suppose R is a field. Suppose $I \trianglelefteq R$, is non-zero, so contains $x \in I - 0$. Let $r \in R$ then $rx^{-1} \in R$ (x^{-1} exists as R is a field) $\implies r = rx^{-1}x \in I$. Hence $I = R$. Conversely suppose every ideal of R is trivial. Let $r \in R - 0$, then the ideal $\langle r \rangle = Rr \neq 0$. So by hypothesis, we must have $R = Rr$. Hence we can find $s \in R$ with $sr = 1 \in R$. Since R is commutative, r is invertible, i.e. $R^* = R - 0$. This shows R is a field. Note this is useful for constructing fields.

Let $\mathbf{y} \in \mathbb{C}^n$. Recall we have evaluation ring homomorphism $\varepsilon_{\mathbf{y}} : \mathbb{C}[x_1, x_2, \ldots, x_n] \longrightarrow \mathbb{C}; f \longmapsto f(\mathbf{y})$, which is surjective (since $\forall\ \alpha \in \mathbb{C}$, we can let f be the constant polynomial of value α).

An exercise would be to check this map agrees with the quotient morphism $\mathbb{C}[x_1, x_2, \ldots, x_n] \xrightarrow{\pi} \mathbb{C}$ $[x_1, x_2, \ldots, x_n]/I(\mathbf{y}) = \mathbb{C}[\mathbf{y}] \subseteq \mathrm{Fun}(\mathbf{y}, \mathbb{C})$. We claim under these identification $\mathbb{C}[x_1, x_2, \ldots, x_n]/I(\mathbf{y})$ $= \mathrm{Fun}(\mathbf{y}, \mathbb{C}) = \mathbb{C}$. The fact is $I(\mathbf{y}) = \ker(\pi) \cong \ker(\varepsilon_{\mathbf{y}})$ is maximal since by the First Isomorphism Theorem, $\mathbb{C}[x_1, x_2, \ldots, x_n]/I(\mathbf{y}) \cong \mathrm{Im}(\varepsilon_{\mathbf{y}})$ is a field and Proposition 23.2 now shows $I(\mathbf{y})$ is maximal. The converse is also true, but is not proved here. It is part of Hilbert's Nullstellensatz. So points in $\mathbb{C}^n$ gives maximum ideals of $\mathbb{C}[x_1, x_2, \ldots, x_n]$.

Theorem 23.1 (Second Isomorphism Theorem). Let R be a ring. $I \trianglelefteq R$ and $J \subseteq I$ be another ideal. Then $\frac{R/J}{I/J} \cong R/I$ as rings.

Proof. Same as Second Isomorphism Theorem for groups except we apply First Isomorphism Theorem for rings instead for groups to $R \xrightarrow{\pi_J} R/J \xrightarrow{\pi_{I/J}} \frac{R/J}{I/J}$.

Theorem 23.2 (Third Isomorphism Theorem). Let S be a subring of R and $I \trianglelefteq R$. Then $S + I$ is a subring of R and $S \cap I \trianglelefteq R$. Also $\frac{S}{S \cap I} \cong \frac{S+I}{I}$ is a ring isomorphism.

Proof. Both are ring quotients since $S \cap I \trianglelefteq S$ and $I \leq S + I$, $I \trianglelefteq R \implies I \trianglelefteq S + I$. Same as Third Isomorphism Theorem for groups except we apply First Isomorphism Theorem for rings instead for groups to $S \hookrightarrow R \xrightarrow{\pi_I} R/I$.

Example 23.2. $S = \mathbb{C}[x]$ is a subring of $R = \mathbb{C}[x, y]$. Let $I = \langle y \rangle \trianglelefteq \mathbb{C}[x, y]$ and apply Third Isomorphism Theorem. $S \cap I = \mathbb{C}[x] \cap \langle y \rangle = 0$. $S + I = \mathbb{C}[x] + \langle y \rangle = \mathbb{C}[x, y]$. Clearly $\mathbb{C}[x] + \langle y \rangle \subseteq$ $\mathbb{C}[x, y]$ and for $p(x, y) \in \mathbb{C}[x, y]$, we have

$$p(x, y) = \sum_{i,j \geq 0} a_{ij} x^i y^j = \sum_i a_{i0} x^i + \sum_{j>0} a_{ij} x^i y^j \in \mathbb{C}[x] + \langle y \rangle$$

Thus we get ring homomorphism $\frac{S}{S \cap I} \cong \frac{S+I}{I} \implies \mathbb{C}[x] \cong \mathbb{C}[x, y]/\langle y \rangle$.

24 Polynomial Rings

Let R be a ring and x an indeterminant.

Definition 24.1 (Polynomial). A polynomial in x with coefficients in R is a formal expression of the form $p = \sum_{i\geq 0} r_i x^i$ where $r_i \in R$ and $r_i = 0$ for i sufficiently large, i.e. $p = r_0x^0 + r_1x^1 + \ldots + r_nx^n$ for some n. Let $R[x]$ be the set of such polynomials.

Proposition - Definition 24.1 (Polynomial Ring). $R[x]$ is a ring, called the polynomial ring with coefficients in R, when endowed with ring addition $\sum_{i\geq 0} r_i x^i + \sum_{i\geq 0} r'_i x^i = \sum_{i\geq 0}(r_i + r'_i)x^i$ and ring multiplication $(\sum_{i\geq 0} r_i x^i)(\sum_{i\geq 0} r'_i x^i) = \sum_{k\geq 0}(\sum_{i+j=k} r_i r'_j)x^k$. Also $0_{R[x]} = 0 + 0x + 0x^2 + \ldots = 0$ and $1_{R[x]} = 1 + 0x + 0x^2 + \ldots = 1$.

Proof. The proof is really boring, but is not hard, i.e. check axioms.

Proposition 24.1. Let $\phi : R \longrightarrow S$ be a ring homomorphism.

(i) R is a subring of $R[x]$ when you identify elements of R with constant polynomials, i.e. coefficients of $x, x^2, \ldots$ are 0

(ii) The map $\phi[x] : R[x] \longrightarrow S[x]; \sum_{i\geq 0} r_i x^i \longmapsto \sum_{i\geq 0} \phi(r_i)x^i$ is a ring homomorphism

Proof. More boring check of axioms. Let us check some of these for (ii).

$$\begin{aligned}
(\phi[x])((\sum_i r_i x^i)(\sum_j r'_j x^j)) &= (\phi[x])(\sum_k (\sum_{i+j=k} r_i r'_j)x^k) \\
&= \sum_k \phi(\sum_{i+j=k} r_i r'_j)x^k \\
&= \sum_k (\sum_{i+j=k} \phi(r_i r'_j)x^k) \quad \text{(ring homomorphism)} \\
&= \sum_k (\sum_{i+j=k} \phi(r_i)\phi(r'_j))x^k \\
&= (\sum_i \phi(r_i)x^i)(\sum_j \phi(r'_j)x^j) \\
&= (\phi[x](\sum_i r_i x^i))(\phi[x](\sum_j r'_j x^j))
\end{aligned}$$

Also $\phi[x](1_{r[x]}) = \phi(1_R) = 1_S = 1_{S[x]}$. As an exercise, check others as you feel like.

Let S be a subring of R and $r \in R$ such that $rs = sr$ for all $s \in S$. Define the evaluation map or substitution $\varepsilon_r : S[x] \longrightarrow R; p = \sum_{i\geq 0} s_i x^i \longmapsto \sum_{i\geq 0} s_i r^i = p(r)$.

Proposition 24.2. The map ε_r above is a ring homomorphism.

Proof. Note $\varepsilon_r(1_{s[x]}) = \varepsilon_r(1_S + 0x + 0x^2 + \ldots) = 1_S = 1_R$ as $S \leq R$. For polynomials $\sum_{i\geq 0} s_i x^i, \sum_{i\geq 0} s'_i x^i \in S[x]$, we have

$$\begin{aligned}
\varepsilon_r(\sum_{i\geq 0} s_i x^i + \sum_{i\geq 0} s'_i x^i) &= \varepsilon_r(\sum_{i\geq 0}(s_i + s'_i)x^i) \\
&= \sum_{i\geq 0}(s_i + s'_i)r^i \\
&= \sum_{i\geq 0} s_i r^i + \sum_{i\geq 0} s'_i r^i \quad \text{(distributive law)} \\
&= \varepsilon_r(\sum_{i\geq 0}(s_i)x^i)\varepsilon_r(\sum_{i\geq 0}(s'_i)x^i)
\end{aligned}$$

So ε_r is a group homomorphism.

$$\begin{aligned}
\varepsilon_r((\sum_{i\geq 0} s_i x^i)(\sum_{i\geq 0} s'_i x^i)) &= \varepsilon_r(\sum_{k\geq 0}(\sum_{i+j=k} s_i s'_j)x^k) \\
&= \sum_{i\geq 0}(\sum_{i+j=k} s_i s'_j)r^k \\
&= \sum_{k\geq 0}\sum_{i+j=k}(s_i x^i)(s'_j x^j) \quad (\text{as } s_j r = r s_j) \\
&= (\sum_{i\geq 0} s_i r^i)(\sum_{j\geq 0} s'_j r^j) \quad \text{(distributive law)} \\
&= \varepsilon_r(\sum_{i\geq 0}(s_i)x^i)\varepsilon_r(\sum_{j\geq 0}(s'_j)x^j)
\end{aligned}$$

Hence ε_r is a ring homomorphism. Note checking pointwise gives ...

Corollary 24.1. If R is commutative then the map $c : S[x] \longrightarrow \mathrm{Fun}(R, R); r \longmapsto$ function sending r to $p(r)$, i.e. polynomials to polynomial functions, is a ring homomorphism.

Note the map c is not necessarily injective, so $R[x]$ may not be naturally identified with a ring of functions.

Example 24.1. $S = R = \mathbb{Z}/2\mathbb{Z}$. Consider $p = x^2 + x = (1 + 2\mathbb{Z})x + (1 + 2\mathbb{Z})x^2 \in (\mathbb{Z}/2\mathbb{Z})[x]$. We have $c : (\mathbb{Z}/2\mathbb{Z})[x] \longrightarrow \mathrm{Fun}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$. Find $c(p)$. $c(p)(0 + 2\mathbb{Z}) = p(0 + 2\mathbb{Z}) = 0^2 + 0 = 0$. $c(p)(1 + 2\mathbb{Z}) = p(1 + 2\mathbb{Z}) = 1^2_{\mathbb{Z}/2\mathbb{Z}} + 1_{\mathbb{Z}/2\mathbb{Z}} = 1 + 2\mathbb{Z} + 1 + 2\mathbb{Z} = 2 + 2\mathbb{Z} = 0_{\mathbb{Z}/2\mathbb{Z}}$. $\therefore c(p)$ is the zero function, i.e. outputs 0 for all input values. So it is the zero polynomial function but is not the zero polynomial.

Let S be a subring of R and $x_1, x_2, \ldots, x_n$ indeterminants. We can define polynomial ring in determinants $x_1, x_2, \ldots x_n$ as before or inductively as $S[x_1, x_2, \ldots x_n] = (\ldots((S[x_1])[x_2])\ldots)[x_n]$. Similarly if $r_1, r_2, \ldots, r_n \in R$ are such that $r_i r_j = r_j r_i$ and $r_i s = s r_i$ for all i, j with $s \in S$, we have a ring homomorphism by substitution or evaluation $\varepsilon_{r_1,r_2,\ldots,r_n} : S[x_1, x_2, \ldots, x_n] \longrightarrow R; p = \sum_{i_1,i_2,\ldots,i_n\geq 0} S_{i_1,i_2,\ldots,i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \longmapsto \sum_{i_1,i_2,\ldots,i_n\geq 0} S_{i_1,i_2,\ldots,i_n} r_1^{i_1} r_2^{i_2} \ldots r_n^{i_n} = p(r_1, r_2, \ldots, r_n)$.

With notation as above, we define the subring of R generated by S and $r_1, r_2, \ldots, r_n$ to be $\mathrm{Im}(\varepsilon_{r_1,r_2,\ldots,r_n} : S[x_1, x_2, \ldots, x_n] \longrightarrow R) = S[r_1, r_2, \ldots, r_n]$.

Example 24.2. $S = \mathbb{Z}$, $R = \mathbb{C}$, $\mathbb{Z}[i] = \text{Im}(\varepsilon_i : \mathbb{Z}[x] \longmapsto \mathbb{C}) = \{\sum_{j\geq 0} a_j i^j : a_j \in \mathbb{Z}\} = \{a + bi : a, b \in \mathbb{Z}\}$.

Proposition 24.3. With the above notation, let S' be a subring of R containing $S, r_1, r_2, \ldots, r_n$. Then $S' \supseteq S[r_1, r_2, \ldots, r_n]$, i.e. $S[r_1, r_2, \ldots, r_n]$ is the smallest such S'.

Proof. For $S_{i_1,i_2,\ldots,i_n} \in S$, closure axioms $\Longrightarrow \sum_{i_1,i_2,\ldots,i_n} S_{i_1,i_2,\ldots,i_n} r_1^{i_1} r_2^{i_2} \ldots r_n^{i_n} \in S'$. This applies to any $\sum_{i_1,i_2,\ldots,i_n} S_{i_1,i_2,\ldots,i_n} r_1^{i_1} r_2^{i_2} \ldots r_n^{i_n} \in \text{Im}(\varepsilon_{r_1,r_2,\ldots,r_n} : S[x_1, x_2, \ldots, x_n] \longrightarrow R)$. So $S[r_1, r_2, \ldots, r_n] \supseteq S'$.

25 Matrix Rings & Direct Product

Let R be a ring with the identity. $(r_{ij}) = \begin{pmatrix} r_{11} & r_{12} & \ldots & r_{1n} \\ r_{21} & r_{22} & \ldots & r_{2n} \\ \vdots & \vdots & & \vdots \\ r_{n1} & r_{n2} & \ldots & r_{nn} \end{pmatrix}$ is an $n \times n$ matrix with entries from R. $M_n(R)$ is the set of all such matrices.

Proposition - Definition 25.1 (Matrix Ring). $M_n(R)$ is a ring, called the matrix ring, with addition and multiplication defined by $(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$ and $(a_{ij})(b_{ij}) = (c_{ij})$ where $c_{ij} = \sum_k a_{ik} b_{kj}$. The identity is $I_{M_n(R)} = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix}$.

Proof. Very obvious, just check axioms.

Example 25.1. In $M_2(\mathbb{C}[x])$, $\begin{pmatrix} 1 & x \\ 0 & 2 \end{pmatrix} \begin{pmatrix} x^3 & 0 \\ 4 & -x^5 \end{pmatrix} = \begin{pmatrix} 4x + x^3 & -x^6 \\ 8 & -2x^5 \end{pmatrix}$.

Let R_i, $i \in I$, be rings. Since each R_i is an abelian group, we have that

$$\prod_{i \in I} R_i = R_1 \times R_2 \times \ldots = \{(r_1, r_2, \ldots)\}$$

Proposition 25.1. $\prod_{i \in I} R_i$ becomes a ring with multiplication defined by coordinatewise via $(r_1, r_2, \ldots)(s_1, s_2, \ldots) = (r_1 s_1, r_2 s_2, \ldots)$.

Proof. All fairly obvious, e.g. associativity, $((r_i)(s_i))(t_i) = (r_i s_i)(t_i) = ((r_i s_i) t_i)$ (by definition) $= (r_i (s_i t_i))$ (since each R_i is a ring and is associative) $= (r_i)(s_i t_i) = (r_i)((s_i)(t_i))$. Note the notation used here $(r_i) = (r_1, r_2, \ldots)$.

If all R_i are commutative so is $\prod_{i \in I} R_i$ since multiplication is done componentwise. So $\prod_{i \in I} R_i$ is a ring. Could it be a field if all R_i are fields? No. $(1, 0)(0, 1) = (0, 0)$. So there exists zero divisors, i.e. in a field, $ab = 0 \Longrightarrow a = 0$ or $b = 0$.

Define for each $j \in I$, $\pi_j : \prod_{i \in I} R_i \longrightarrow R_j; (r_i) \longmapsto r_j$ is the projection on R_j.

Proposition 25.2. Two important observations

(i) Each π_j is a ring homomorphism.

(ii) Given ring homomorphism $\phi_i : S \longrightarrow R_i$, define $\phi : S \longrightarrow \prod_{i\in I} R_i$ by $\phi((s_i)) = (\phi_i(s_i))$. Then ϕ is an homomorphism.

Proof. Tedious but based on Universal Property Of Product of groups and monomorphisms of groups, e.g. $\pi_j(1_{\prod_{i\in I} R_i}) = \pi_j((1_{R_i})) = 1_{R_j}$; $\pi_j((r_i)(s_i)) = \pi_j(r_i s_i) = r_j s_j = \pi_j((r_i))\pi_j((s_i))$.

Lemma 25.1. Suppose R is a commutative ring and $I_1, I_2, \ldots, I_n \trianglelefteq R$ (ideals) such that $I_i + I_j = R$ for each pair of i, j. Then $I_1 + \bigcap_{i>1} I_i = R$.

Proof. Pick $a_i \in I_1$ and $b_i \in I_i$ such that $a_i + b_i = 1$ for $i = 2, 3, \ldots, n$, since $I_1 + I_i = R$. Then $1 = (a_2 + a_3)(a_3 + b_3)\ldots(a_n + b_n) = (b_2 b_3 \ldots b_n)+$ terms each involving a_i's (distributive law) $\in I_1 + \bigcap_{i\geq 2} I_i$ (by properties of ideals). So $R = I_1 + \bigcap_{i\geq 2} I_i$ as $\forall\ r \in R$, $r1 = r \in I_1 + \bigcap_{i\geq 2} I_i$.

Theorem 25.1 (Chinese Remainder Theorem). Suppose R is a commutative ring and $I_1, I_2, \ldots, I_n \trianglelefteq R$ (ideals) such that $I_i + I_j = R$ for each pair of i, j. Then the natural map $R/\bigcap_{i=1}^n I_i \longrightarrow R/I_1 \times R/I_2 \times \ldots \times R/I_n; r + \bigcap_{i=1}^n I_i \longmapsto (r + I_1, r + I_2, \ldots, r + I_n)$ is a ring homomorphism.

Proof. Induction on n. Let $n = 2$. Consider $\psi : R \longmapsto R/I_1 \times R/I_2; r \longmapsto (r + I_1, r + I_2)$, a ring homomorphism. Clearly $\ker(\psi) = \{r : (r+I_1, r+I_2) = (0_{R/I_1}, 0_{R/I_2})\} = \{r : r \in I_1, r \in I_2\} = I_1 \cap I_2$. We now show ψ is surjective. Hence by the First Isomorphism Theorem, $\frac{R}{I_1\cap I_2} \cong R/I_1 \times R/I_2$. Let $r_1, r_2 \in R$. Choose $x_1 \in I_1, x_2 \in I_2$ with $x_1 + x_2 = 1$ (can do this since $I_1 + I_2 = R$). Thus $\psi(r_2x_1 + r_1x_2) = (r_2x_1 + r_1x_2 + I_1, r_2x_1 + r_1x_2 + I_2)$. Consider $r_2x_1 + r_1x_2 + I_1$. $r_2x_1 \in I_1$ as $x_1 \in I_1$ and $r_1x_2 = r_1(1 - x_1) = r_1 - r_1x_1$ (distributive law), with $x_1 \in I_1 \implies r_2x_1 + r_1x_2 + I_1 = r_1 + I_1$. Similarly $r_2x_1 + r_1x_2 + I_2 = r_2 + I_2$. So $\psi(r_2x_1 + r_1x_2) = (r_1 + I_1, r_2 + I_2)$. Hence ψ is onto. Using Lemma 25.1, we have the $n = 2$ case $R/\bigcap_{i=1}^n I_i \cong R/I_1 \times R/\bigcap_{i=2}^n I_i \cong R/I_1 \times R/I_2 \times \ldots \times R/I_n$ (by inductive hypothesis).

Example 25.2. $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$ if and only if $\gcd(m, n) = 1$. Hence $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, i.e. the usual Chinese Remainder Theorem.

26 Fields Of Fractions

This lecture works only with commutative rings.

Definition 26.1 (Domain). A commutative ring R is called a domain or integral domain of for any $r, s \in R$ with $rs = 0$, we have $r = 0$ or $s = 0$.

Note that in a domain, if $u \in R - 0$ and $v, w \in R$ then $uv = uw \iff u(v - w) = 0 \iff v - w = 0 \iff v = w$, i.e. domains do not have zero divisors.

Example 26.1. $\mathbb{Z}, \mathbb{C}[x_1, x_2, \ldots, x_n]$ are domains. $\mathbb{Z}/6\mathbb{Z}$ is not a domain, e.g. $(2 + 6\mathbb{Z})(3 + 6\mathbb{Z}) = 6 + 6\mathbb{Z} = 6\mathbb{Z} = 0_{\mathbb{Z}/6\mathbb{Z}}$. In fact $\mathbb{Z}/p\mathbb{Z}$ is a domain if and only if p is prime. And any field is a domain.

Let R be a commutative domain. Let $\tilde{R} = R \times (R-0) = \{\begin{pmatrix} a \\ b \end{pmatrix} : a \in R, b \in R-0\}$ Define a relation $\sim$ on $\tilde{R}$ by $\begin{pmatrix} a \\ b \end{pmatrix} \sim \begin{pmatrix} a' \\ b' \end{pmatrix}$ if and only if $ab' = a'b$, i.e. like equalities of fractions.

Lemma 26.1. $\sim$ is an equivalence relation on $\tilde{R}$.

Proof. Immediate that $\sim$ is reflexive and symmetric. For transitivity, suppose that $\begin{pmatrix} a \\ b \end{pmatrix} \sim \begin{pmatrix} a' \\ b' \end{pmatrix}$ and $\begin{pmatrix} a' \\ b' \end{pmatrix} \sim \begin{pmatrix} a'' \\ b'' \end{pmatrix}$. Then $ab' = a'b$ and $a'b'' = a''b'$. So $ab'b'' = a'bb'' = ba'b'' = ba''b' \implies b'(ab'') = b'(a''b')$ by commutativity. Hence since R is a domain, and $b' \neq 0$, we get $ab'' = a''b$, so $\begin{pmatrix} a \\ b \end{pmatrix} \sim \begin{pmatrix} a'' \\ b'' \end{pmatrix}$.

In terms of notations, let $\frac{a}{b}$ denote the equivalence class containing $\begin{pmatrix} a \\ b \end{pmatrix}$ and write $K(R)$ for $\tilde{R}/\sim$, the set of all such fractions.

Lemma 26.2. The following operations give well defined addition and multiplication on $K(R)$.

(i) $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$

(ii) $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$

Proof. (i) Exercise. Note $bd \neq 0$ since $b \neq 0$, $d \neq 0$ (R is a domain). (ii) Commutativity of multiplication means it suffices to check that if $\begin{pmatrix} c \\ d \end{pmatrix} \sim \begin{pmatrix} c' \\ d' \end{pmatrix}$ then $\begin{pmatrix} ac \\ bd \end{pmatrix} \sim \begin{pmatrix} ac' \\ bd' \end{pmatrix}$. But $c'd = cd' \implies acbd' = ac'bd$. So $\begin{pmatrix} ac \\ bd \end{pmatrix} \sim \begin{pmatrix} ac' \\ bd' \end{pmatrix}$ as required.

Theorem 26.1. The ring addition and multiplication maps in Lemma 26.2 makes $K(R)$ into a field with zero $\frac{0}{1}$ and $1_{K(R)} = \frac{1}{1}$.

Proof. Long and tedious, and mostly omitted. Most of the tricks used for $\mathbb{Q}$ have analogous in $K(R)$. In particular, any two fractions $\frac{a}{b}$, $\frac{c}{d}$ can be put on a common denominator, $\frac{a}{b} = \frac{ad}{bd}$, $\frac{c}{d} = \frac{bc}{bd}$. Also $\frac{a}{d} + \frac{b}{d} = \frac{ad+bd}{d^2} = \frac{a+b}{d}$. Hence to check associativity of addition it suffices to check $(\frac{a}{d} + \frac{b}{d}) + \frac{c}{d} = \frac{a}{b} + (\frac{b}{d} + \frac{c}{d})$, Note $K(R)$ is a field since if $\frac{a}{b} \neq \frac{0}{1}$, then $a \neq 0$, so $\frac{b}{a} \in K(R)$ and $(\frac{a}{b})^{-1} = \frac{b}{a}$. As exercises, prove some of the other axioms for $K(R)$ to be a field.

Example 26.2. $K(\mathbb{Z}) = \mathbb{Q}$, $K(\mathbb{R}[x])$ = set of real rational functions $\frac{p(x)}{q(x)}$. Write for F, $K(F[x_1, x_2, \ldots, x_n]) = F(x_1, x_2, \ldots, x_n)$.

Proposition 26.1. Let R be a commutative domain.

(i) The map $\iota : R \longmapsto K(R); \alpha \longmapsto \frac{\alpha}{1}$ 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 $K(R)$.

Proof. (ii) is fairly clear. (i) $\frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} \implies \iota(a+b) = \iota(a) + \iota(b)$. So ι is a group homomorphism. $\frac{a}{1}\frac{b}{1} = \frac{ab}{1}$, i.e. $\iota(ab) = \iota(a)\iota(b)$. Also $\frac{1}{1} = \iota(1) = 1_{K(R)}$. So ι is a ring homomorphism. Finally $\frac{a}{1} = \frac{b}{1} \iff a = a1 = b1 = b$. So ι is injective.

Proposition 26.2. Let F be a field. Then $K(F) = F$.

Proof. If suffices to check the map $\phi : F \longmapsto K(F); a \longmapsto \frac{a}{1}$ is surjective as we know it is an injective homomorphism. But we know $\frac{a}{b} = \frac{ab^{-1}}{1} = \phi(ab^{-1})$ as $a1 = aab^{-1}b$. So we are done.

Example 26.3. What $K(\mathbb{Z}[i])$? Guess $\mathbb{Q}[i] = \{r + si : r, s \in \mathbb{Q}\}$. Note that $\mathbb{Q}[i] \subseteq K(\mathbb{Z}[i])$ as $\frac{a}{b} + \frac{c}{d}i = \frac{ad+bci}{bd} \in K(\mathbb{Z}[i])$ But $\mathbb{Q}[i]$ is a field, given $r, s \in \mathbb{Q}$ not both zero, $(r+si)^{-1} = \frac{r-si}{r^2+s^2} \in \mathbb{Q}[i]$. So by Proposition 26.2, $K(\mathbb{Q}[i]) = \mathbb{Q}[i]$. But also by Proposition 26.1, $\mathbb{Z}[i] \leq \mathbb{Q}[i] \implies K(\mathbb{Z}[i]) \leq K(\mathbb{Q}[i])$. Hence $K(\mathbb{Z}[i]) = \mathbb{Q}[i]$. This is true more generally, i.e. $K(R)$ is the smallest field containing R. Prove it as an exercise.

27 Introduction To Factorisation Theory

Here, we introduce factorisation in arbitrary commutative domains and work with commutative domains over the next few lectures. Let R be one such.

Definition 27.1 (Prime Ideal). $P \trianglelefteq R$, with $P \neq R$, is prime if and only if R/P is a domain. Equivalently, whenever $r, s \in R$ are such that $rs \in P = 0_{R/P}$, then $r \in P$ or $s \in P$.

Example 27.1. $\mathbb{Z}/p\mathbb{Z}$ is prime if and only if p is prime.

Example 27.2. $\langle y \rangle \trianglelefteq \mathbb{C}[x, y]$ is prime because $\mathbb{C}[x, y]/\langle y \rangle \cong \mathbb{C}[x]$ which is a domain.

Example 27.3. If $M \trianglelefteq R$, with $M \neq R$, is maximal then M is prime because R/M is field, thus a domain. So all maximal ideals are prime ideals.

Definition 27.2 (Divisibility). We say $r \in R$ divides $s \in R$, write $r \mid s$, if $s \in \langle r \rangle = Rr$, or equivalently $\langle s \rangle \subseteq \langle r \rangle$.

Example 27.4. $3 \mid 6$ as $6\mathbb{Z} \subseteq 3\mathbb{Z}$.

Proposition - Definition 27.1 (Associates). We say that $r, s \in R - 0$ are associates if one of the following two equivalent conditions hold.

(i) $\langle r \rangle = \langle s \rangle$

(ii) There is a unit $u \in R^*$ with $r = us$

Proof. (ii) $\implies$ (i) Suppose that $r = us$, where $u \in R^*$, then $r \in \langle s \rangle$, so $\langle r \rangle \subseteq \langle s \rangle$. But also $s = u^{-1}r$ ($u \in R^*$). So by the same argument, $\langle s \rangle \subseteq \langle r \rangle$. Hence (i) follows. (i) $\implies$ (ii) Since $\langle r \rangle = \langle s \rangle$, we can write $r = vs$, $s = wr$ for some $v, w \in R$. Then $r = vs = vwr$. So since R is a domain and $r \neq 0$, $vw = 1$, $v, w \in R^*$, giving (ii) (as R is also commutative).

Example 27.5. $\langle -2 \rangle = \langle 2 \rangle \trianglelefteq \mathbb{Z}$, so 2 and -2 are associates.

Definition 27.3 (Prime). An element $p \in R - 0$ is prime if $\langle p \rangle$ is prime. That is whenever $r, s \in R$ such that $p \mid rs$ then $p \mid r$ or $p \mid s$.

Note that $\langle p \rangle$ is prime $\iff$ $R/\langle p \rangle$ is a domain. So $rs \in \langle p \rangle \iff p \mid rs \iff rs + \langle p \rangle = \langle p \rangle = 0_{R/\langle p \rangle} = (r + \langle p \rangle)(s + \langle p \rangle) \iff r + \langle p \rangle = 0_{R/\langle p \rangle}$ or $s + \langle p \rangle = 0_{R/\langle p \rangle} \iff r \in \langle p \rangle$ or $s \in \langle p \rangle \iff p \mid r$ or $p \mid s$.

Example 27.6. $\pm 2, \pm 3, \pm 5$ are primes in $\mathbb{Z}$.

Definition 27.4 (Irreducibility). A non-unit $p \in R - R^*$ is irreducible if for any factorisation $p = rs$, we have $r \in R^*$ or $s \in R^*$ (note we cannot have both $r, s \in R^*$ as that would imply $p = rs \in R^*$).

Proposition 27.1. In the commutative domain R, every prime element is irreducible.

Proof. Let $p \in R$ be a prime. If p is prime, how do we know that $p \notin R^*$. p prime $\implies \langle p \rangle$ prime. If $p \in R^*$ then $\langle p \rangle = \langle 1_R \rangle = R$. But prime ideals are proper by definition. $\therefore$ we know $p \notin R^*$. Suppose $p = rs$ where $r, s \in R$. Since p is prime, WLOG, $p \mid r$, Hence $r = pq$ for some $q \in R$. So $p = rs = pqs \implies qs = 1$ as R is a domain and $p \neq 0$. By commutativity of R, $s \in R^*$, making p irreducible.

It is important to note that primes are always irreducible but the converse is not true. Apparently this created a hole in early proofs of Fermat's Last Theorem.

Definition 27.5 (Unique Factorisation Domain). A commutative domain R is factorial or a unique factorisation domain (UFD) if we have both

(i) Every non-zero non-unit $r \in R$ can be factorised as $r = p_1 p_2 \dots p_n$ with all p_i irreducibles

(ii) If we have two factorisations of the same element $r = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$ with all p_i, q_i irreducible then $n = m$ and we can re-index the q_i so that p_i and q_i are associates for all i, i.e. equal up to unit multiples

Example 27.7. $\mathbb{Z}$ is a UFD.

Lemma 27.1. Let R be a commutative domain in which every irreducible elements is prime. If $r \in R$ can be factorised into a product of irreducibles as in Definition 27.5, then the factorisation is unique in the sense that it is equal up to unit multiples.

Proof. Suppose that $r \in R$, satisfies that $r = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$ with p_i, q_i irreducibles and hence are all primes by assumption. We use induction on n. For $n = 1$, the result is true by definition of irreducibility. If $n > 1$, we have $p_1 \mid q_1 q_2 \dots q_m$, so $p_1 \mid q_j$ say (as p_1 is prime). Re-index the q_i's so that $j = 1$. Then $q_1 = p_1 u$ for some $u \in R$. We must have $u \in R^*$ since q_1 is irreducible. So p_1 and q_1 are associates. Cancel p_1 to obtain $p_2 p_3 \dots p_n = u q_2 q_3 \dots q_m$. Since $u \in R^*$, we have $\langle u q_2 \rangle = \langle q_2 \rangle$ which is prime. So uq_2 is also prime thus irreducible. The inductive hypothesis finishes the proof, i.e. $p_2 p_3 \dots p_n = q_2' q_3 \dots q_m$, where $q_2' = u q_2$ is prime.

Example 27.8. $R = \mathbb{C}[x]$ then $\mathbb{C}[x]^* = \mathbb{C}^*$. Any complex polynomials factor into linear factors, so the irreducible elements of $\mathbb{C}[x]$ are of the form $\alpha(x - \beta)$, where $\alpha, \beta \in \mathbb{C}$, $\alpha \neq 0$. Now $\langle \alpha(x-\beta) \rangle = \langle x-\beta \rangle$ (α is a unit) $= I(\beta) =$ set of all polynomials with root β. As $I(\beta)$ is a maximum ideal, $I(\beta)$ is a prime. Hence $\alpha(x - \beta)$ is prime. So all irreducibles are prime. Lemma 27.1 gives that $\mathbb{C}[x]$ is a unique factorisation domain.

Example 27.9. In $R = \mathbb{Z}[\sqrt{-5}]$, we have $2 \times 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, i.e. factorisation is not unique. So need to show $2, 3, 1 + \sqrt{5}, 1 - \sqrt{5}$ are irreducibles, then $\mathbb{Z}[\sqrt{-5}]$ is not a unique factorisation domain.

28 Principal Ideal Domains

The motivation here is to give a sufficient criterion for a commutative domain to be a UFD.

Definition 28.1 (Principal Ideal Domain). Let R be a commutative ring. An ideal I is principal if $I = \langle x \rangle$ for some $x \in R$. A principal ideal domain or PID is a commutative domain in which every ideal is principal.

Example 28.1. $R = \mathbb{Z}$ is a PID since every ideal is of the $n\mathbb{Z} = \langle n \rangle$ and is thus principal.

Proposition 28.1. Let R be a commutative domain and $r \in R - 0$, $s \in R$. Then $\langle r \rangle = \langle rs \rangle$ and equality occurs if and only if $s \in R^*$.

Proof. The only unknown fact is $\langle r \rangle = \langle rs \rangle \implies s \in R^*$. Suppose $\langle r \rangle = \langle rs \rangle = R(rs)$. So $r \in \langle rs \rangle$ or $r = rst$ for some $t \in R$. Since R is a domain, so we can cancel to get $1 = st = ts$ (commutativity) and hence $s \in R^*$.

Proposition 28.2. let R be a PID. Then $p \in R - 0$ is irreducible if and only if $\langle p \rangle$ is maximal. In particular, any irreducible element in R is prime, since maximal ideals are always prime ideals (the quotient is a field which is always a domain).

Proof. Assume first, p not irreducible. Say $p = rs$. By Proposition 28.1, $\langle p \rangle = \langle rs \rangle \subseteq \langle r \rangle$. So $\langle p \rangle$ is not maximal. Suppose p is irreducible. Let $I \trianglelefteq R$ be such that $\langle p \rangle \subseteq I$. Since R is a PID, every ideal, including I, is principal, i.e. $I = \langle q \rangle$ for some $q \in R$. Hence $\langle p \rangle \subseteq \langle q \rangle$, thus $p \in \langle q \rangle$, i.e. $p = qr$ for some $r \in R$. But p is irreducible, so either q or r is a unit. Suppose $q \in R^*$, then $I = \langle q \rangle = Rq = R1 = R$ ($\langle q \rangle = \langle 1 \rangle = R$, as q and 1 are associates, i.e. $q = q1$). Suppose $r \in R^*$. Then $qr = p$ and q are associates, so $\langle p \rangle = \langle q \rangle = I$. Hence by definition, I is maximal.

Note that by Lemma 27.1, factorisation in a PID is unique if it exists, i.e. every irreducible is a prime.

Lemma 28.1. Let S be any ring and $I_0, I_1, I_2, \ldots \trianglelefteq S$ be such that $I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$ Then $I = \bigcup_{j \in \mathbb{N}} I_j \trianglelefteq S$.

Proof. Let $x, x' \in I$. We can assume $x \in I_j$ and $x' \in I_{j'}$ and WLOG, assume $j \geq j'$. Note $0 \in I_0 \subseteq I$ (subgroup) and $-x \in I_j \subseteq I$. $\because x' \in I_{j'} \subseteq I_j \therefore x + x' \in I_j \subseteq I$ (closure of subgroups). So I is a subgroup of S. Further for $s \in S$, $sx, xs \in I_j \subseteq I$. Thus $I \trianglelefteq S$ by definition.

Theorem 28.1. Any PID R is a UFD.

Proof. It is sufficient to show that for any $r \in R - 0$, not a unit, we can express $r = p_1 p_2 \ldots p_n$ with $p_i \in R$ irreducible, hence prime as shown in Proposition 28.2. We will assume this is false and derive a contradiction. Suppose r not a product of irreducibles, i.e. r cannot be irreducible itself. $\therefore r$ reducible and we can write $r = r_0 = r_1 q_1$, with q_1, r_1 not units. WLOG, r_1 is not a product of irreducibles (if q_1, r_1 are both product of irreducibles, then so will be $r = r_1 q_1$). Can similarly factorise $r_1 = q_2 r_2$ with $q_2, r_2 \notin R^*$ and r_2 not a product of irreducibles. We continue to define inductively $q_3, q_4, \ldots$; $r_3, r_4, \ldots \notin R^*$ with $r_k = r_{k+1} q_{k+1}$. By Proposition 28.1, we get a strictly increasing chain of ideals $\langle r \rangle = \langle r_0 \rangle = \langle r_1 q_1 \rangle \subsetneqq \langle r_1 \rangle = \langle r_2 q_2 \rangle \subsetneqq \langle r_2 \rangle = \ldots$ Let $I = \bigcup_{j \in \mathbb{N}} \langle r_j \rangle$. But R is a PID. So by Lemma 28.1, $I = \langle r_\infty \rangle$ for some $r_\infty \in R$. But $r_\infty \in \langle r_j \rangle$ for some j, as $r_\infty \in I = \bigcup_{j \in \mathbb{N}} \langle r_j \rangle$. So $I = \langle r_\infty \rangle \subseteq \langle r_i \rangle \subseteq I$. So $\langle r_j \rangle = I$ and the chain of ideals must stabilise in the sense $\langle r_j \rangle = \langle r_{j+1} \rangle = \ldots$ This contradiction proves the theorem.

Definition 28.2 (Greatest Common Divisor). Let R be a PID. Let $r, s \in R - 0$. Then a greatest common divisor for r, s is an element $d \in R$ such that $d \mid r$ and $d \mid s$, and further given any other common divisor, i.e. $c \in R$ such that $c \mid r$ and $c \mid s$, we have $c \mid d$. Write $d = \gcd(r, s)$.

Proposition 28.3. Let R be a PID and $r, s \in R - 0$. Then r, s have a greatest common divisor, say d , such that $\langle d \rangle = \langle r, s \rangle$.

Proof. Since R is PID, $\langle r, s \rangle = \langle d \rangle$ for some $d \in R$. We will show it is a greatest common divisor of r and s. Note $\langle d \rangle = \langle r, s \rangle \supseteq \langle r \rangle, \langle s \rangle$. $\therefore r, s \in \langle d \rangle \implies d \mid r$ and $d \mid s$, i.e. $\exists\ k, l \in R$ such that $r = kd$, $s = ld$. Consider another common divisor c, i.e. $c \mid r$ and $c \mid s \implies \langle c \rangle \supseteq \langle r \rangle, \langle s \rangle$, since $r, s \in \langle c \rangle$. $\therefore \langle c \rangle \supseteq \langle r, s \rangle = \langle r \rangle + \langle s \rangle = \langle d \rangle$. So $d = mc$ for $m \in R$, i.e. $c \mid d$. Hence the greatest common divisor for r and s is d.

29 Euclidean Domains

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

Proposition 29.1. $R = \mathbb{C}[x]$ is a PID.

Proof. Let I be a non-zero ideal. Note that $I = 0 = \langle 0 \rangle$ is principal. Pick $p \in I - 0$, which is minimum degree. We know $I \supseteq \langle p \rangle$. We show in fact $I = \langle p \rangle$. Let $f \in I$. Long division shows that we can write $f = pq + r$, where $q, r \in \mathbb{C}[x]$ and $\deg(r) < \deg(p)$ if $r \neq 0$. However $f \in I$ and $pq \in \langle p \rangle \subseteq I$. $\therefore r = f - pq \in I$. Minimality of $\deg(p) \implies r = 0$. So $f = pq \in \langle p \rangle$. Hence I is principal and $\mathbb{C}[x]$ is a PID.

This is the same proof for $\mathbb{Z}$ is a PID. Define Euclidean domains to be rings where this works. More precisely ...

Definition 29.1 (Euclidean Domain). Let R be a commutative domain. A function $\nu : R - 0 \longrightarrow \mathbb{N}$ is called an Euclidean norm on R if

(i) For $f \in R$, $p \in R - 0$, there exists $q, r \in R$ with $\nu(r) < \nu(p)$ and $f = pq + r$ if $r \neq 0$, (ν is like a degree function)

(ii) For $f, g \in R - 0$, $\nu(f) \leq \nu(fg)$ (just like a degree function)

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

Example 29.1. Let $F =$ ring. Then we can define the degree function $\deg : F[x] - 0 \longrightarrow \mathbb{N}$. If F is also a field, then the usual long division works to show $\nu = \deg$ is an Euclidean norm. Note that if F is a field then $F[x]$ is a commutative domain.

Example 29.2. $\nu : \mathbb{Z} - 0 \longrightarrow \mathbb{N}; n \longmapsto |n|$ is an Euclidean norm on $\mathbb{Z}$.

Theorem 29.1. Let R be an Euclidean domain with Euclidean norm ν. Then R is a PID and hence a UFD.

Proof. Let $I \trianglelefteq R$ be non-zero (note $0 = \langle 0 \rangle$). Pick $p \in I - 0$ with $\nu(p)$ minimal (minimum exists in $\mathbb{N}$). Note $I \supseteq \langle p \rangle$. We show $I = \langle p \rangle$. Let $f \in I$. Using Definition 29.1 (i) to write $f = pq + r$ with $q, r \in R$, $\nu(r) \leq \nu(p)$ if $r \neq 0$. But $I \ni f - pq$ as $pq \in \langle p \rangle \subseteq I$. $\therefore r \in I$. Minimality of $\nu(p) \implies r = 0$. So $f = pq \in \langle p \rangle$. Hence $I = \langle p \rangle$ and R is a PID.

In number theory, often look at small over-rings of $\mathbb{Z}$, where over-rings are rings containing another ring.

Lemma 29.1. Consider function $\nu : \mathbb{C} \longrightarrow \mathbb{R}; z \longmapsto |z|^2$ so $\nu(z_1 z_2) = \nu(z_1)\nu(z_2)$ for $z_1, z_2 \in \mathbb{C}$. Let R be one of the following subrings of $\mathbb{C}$: $\mathbb{Z}[i], \mathbb{Z}[i\sqrt{2}], \mathbb{Z}[\frac{1+\sqrt{3}i}{2}], \mathbb{Z}[\frac{1+\sqrt{7}i}{2}], \mathbb{Z}[\frac{1+\sqrt{11}i}{2}]$. Then

(i) ν takes integer values on R

(ii) For any $z \in \mathbb{C}$, there is some $s \in R$ with $\nu(z-s) < 1$

Proof. We will only do case $R = \mathbb{Z}[i\sqrt{2}]$. $R = \mathbb{Z}[i]$ is similar. other cases require simple modification of the argument. What is $R = \mathbb{Z}[i\sqrt{2}]$? It is the $\mathrm{Im}(\varepsilon_{i\sqrt{2}} : \mathbb{Z}[x] \longrightarrow \mathbb{C}; p(x) \longmapsto p(i\sqrt{2}))$. Let $p = \sum_j a_j x^j$, $a_j \in \mathbb{Z}$. Then $p(i\sqrt{2}) = \sum_j a_j i^j (\sqrt{2})^j \in \mathbb{Z} + \mathbb{Z}(i\sqrt{2})$. This is because j even $\implies i^j(\sqrt{2})^j = (-1)^{\frac{j}{2}} 2^{\frac{j}{2}} \in \mathbb{Z}$; j odd $\implies i^j(\sqrt{2})^j = i\sqrt{2}i^{j-1}(\sqrt{2})^{j-1} \in (i\sqrt{2})\mathbb{Z}$ (as $j-1$ is even). $\therefore \mathbb{Z}[i\sqrt{2}] \subseteq \{a + bi\sqrt{2} : a, b \in \mathbb{Z}\}$. The reverse inclusion is by definition. Hence $\mathbb{Z}[i\sqrt{2}] = \{a + bi\sqrt{2} : a, b \in \mathbb{Z}\}$. (i) For $a, b \in \mathbb{Z}$, $\nu(a + bi\sqrt{2}) = a^2 + 2b^2 \in \mathbb{N}$. (ii) Look at Argand diagram. Elements of R form a lattice. The worst case scenario is $\frac{1+i\sqrt{2}}{2}$. But pick $s = 0$, we see $\nu(z-s) = \left|\frac{1+i\sqrt{2}}{2}\right|^2 = \frac{1}{4} + \frac{2}{4} = \frac{3}{4} < 1$. This proves the lemma.

Theorem 29.2. Let ν be the function in Lemma 29.1 and R be one of the following. $\mathbb{Z}[i], \mathbb{Z}[i\sqrt{2}]$, $\mathbb{Z}[\frac{1+\sqrt{3}i}{2}], \mathbb{Z}[\frac{1+\sqrt{7}i}{2}], \mathbb{Z}[\frac{1+\sqrt{11}i}{2}]$. Then ν is an Euclidean norm on R.

Proof. Check axiom (ii). for $f, g \in R - 0$, $\nu(f), \nu(g) \in \mathbb{N} - 0$. Hence $\nu(fg) = \nu(f)\nu(g) \geq \nu(f)$ as $\nu(g) \geq 1$. Check axiom (i). Let $f \in R$, $p \in R - 0$. Pick $s \in R$ as in Lemma 29.1, so $\nu(\frac{f}{p} - s) < 1$ ($\frac{f}{p} \in \mathbb{C}, s \in R$). Note $\nu(r) = \nu(f - ps) = \nu(p)\nu(\frac{f}{p} - s) < \nu(p)$ as $\nu(\frac{f}{p} - s) < 1$. So $f = ps + r$ where $\nu(r) < \nu(p)$. Thus ν is an Euclidean norm and R is an Euclidean domain.

30 Fun With Euclidean Domains

For this lecture, R is an Euclidean domain with Euclidean norm ν.

Proposition 30.1. Let $I \trianglelefteq R$ be non-zero. Then $p \in I - 0$ generates I if and only if $\nu(p)$ is minimal. In particular $u \in R^*$ if and only if $\nu(u) = \nu(1)$.

Proof. Saw in the proof of Theorem 29.1 that $p \in I - 0$ with $\nu(p)$ minimal $\implies I = \langle p \rangle$. Suppose conversely that $I = \langle p \rangle$ then for $q \in R - 0$, $\nu(pq) \geq \nu(p)$ ((ii) of Definition 29.1). $\therefore \nu(p)$ is minimal. Also $u \in R^*$ if and only if $\langle u \rangle = \langle 1 \rangle = R$, i.e. $\nu(p) = \nu(1)$.

Example 30.1. $\mathbb{Z}[i\sqrt{2}]^* = \{1, -1\}$ for $\nu(z) = |z|^2$.

Let $f, g \in R - 0$. We wish to compute $d = \gcd(f, g)$. By Proposition 28.3, $\langle f, g \rangle = \langle d \rangle$. By Proposition 30.1, seek to minimise $\nu(x)$ as x ranges over $\langle f, g \rangle - 0$. How?

Theorem 30.1 (Euclidean Algorithm). Assume $\nu(f) \geq \nu(g)$. Find $q, r \in R$ with $f = qg + r$ with $\nu(r) < \nu(p)$ or $r = 0$. Case $r = 0 \implies \langle f, g \rangle = \langle qg, g \rangle = \langle g \rangle$. $\therefore \gcd(f, g) = g$. Case $r \neq 0$, observe $\langle f, g \rangle = \langle g, r \rangle$ 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. (Note the algorithm terminates because $\nu(r) < \nu(g)$ and $\mathbb{N}$ has a minimum at 0).

Example 30.2. Consider Euclidean domain $R = \mathbb{Z}[i\sqrt{2}] = \{a + bi : a, b \in \mathbb{Z}\}$ with Euclidean norm $\nu : R - 0 \longrightarrow \mathbb{N}; z \longmapsto |z|^2$. What is $\gcd(y + i\sqrt{2}, 2i\sqrt{2})$? Note $i\sqrt{2}(2i\sqrt{2}) = -4$ as $i\sqrt{2} \in R$. Using Theorem 30.1, we see $\gcd(y + i\sqrt{2}, 2i\sqrt{2}) = \gcd(2i\sqrt{2}, y + i\sqrt{2} - ni\sqrt{2}(2i\sqrt{2})) = \gcd(2i\sqrt{2}, (y - 4n) + i\sqrt{2})$ for any $n \in \mathbb{Z}$. $\therefore \gcd(y + i\sqrt{2}, 2i\sqrt{2}) = \gcd(\bar{y} + i\sqrt{2}, 2i\sqrt{2})$, where $\bar{y} \in \{-1, 0, 1, 2\}$ and $y + 4\mathbb{Z} = \bar{y} + 4\mathbb{Z}$. (i) $\bar{y} = 0 \implies \gcd(2i\sqrt{2}, i\sqrt{2}) = i\sqrt{2}$. (ii) $\bar{y} = 2 \implies f = 2i\sqrt{2}, g = 2 + i\sqrt{2} \implies \frac{f}{g} = \frac{2i\sqrt{2}}{2+i\sqrt{2}} = \frac{4+4i\sqrt{2}}{6} \approx 1 + i\sqrt{2} = q \implies qg = (1 + i\sqrt{2})(2 + i\sqrt{2}) = 2 + 3i\sqrt{2} - 2 = 3i\sqrt{2} \implies r = f - gq = 2i\sqrt{2} - 3i\sqrt{2} = -i\sqrt{2}$ and $\nu(r) = 2 < 6 = \nu(p)$. $\therefore \langle f, g\rangle = \langle g, r\rangle = \langle 2 + i\sqrt{2}, -i\sqrt{2}\rangle = \langle -i\sqrt{2}(-1 + i\sqrt{2}), -i\sqrt{2}\rangle = \langle i\sqrt{2}\rangle$, i.e. $\gcd(f, g) = i\sqrt{2}$. (iii) $\bar{y} = \pm 1 \implies f = 2i\sqrt{2}, g = \pm 1 + i\sqrt{2} \implies \frac{f}{g} = \frac{2i\sqrt{2}}{\pm 1+i\sqrt{2}} = \frac{4\pm 2i\sqrt{2}}{3} \approx 1 \pm i\sqrt{2} = q \therefore qg = (1 \pm i\sqrt{2})(\pm 1 + i\sqrt{2}) = \pm 1 + i\sqrt{2} + i\sqrt{2} \mp 2 = \mp 1 + 2\sqrt{2}i \implies r = f - gq = 2i\sqrt{2} - (\mp 1 + 2i\sqrt{2}) = \pm 1$, i.e. $\langle f, g\rangle = \langle g, r\rangle = \langle g, 1\rangle = \langle 1\rangle = R \implies \gcd(f, g) = 1$.

Theorem 30.2. The only integer solution to $y^2 + 2 = x^3$ are $y = \pm 5, x = 3$.

Proof. Suppose y is even then $2 \mid y^2 + 2 \implies 2 \mid x^3 \implies 2 \mid x \implies 8 \mid x^3$. But $4 \mid y^2 \implies 4 \nmid y^2 + 2$. So $8 \nmid y^2 + 2$. $\therefore y$ is odd. Work in PID, $\mathbb{Z}[i\sqrt{2}]$, $y^2 + 2 = (y + i\sqrt{2})(y - i\sqrt{2}) = x^3$. Note $\langle y + i\sqrt{2}, y - i\sqrt{2}\rangle = \langle y + i\sqrt{2}, y + i\sqrt{2} - (y - i\sqrt{2})\rangle = \langle y + i\sqrt{2}, 2i\sqrt{2}\rangle = 1$ for y odd. By prime factorisation both sides and noting $y + i\sqrt{2}$ and $y - i\sqrt{2}$ have $\gcd(y + i\sqrt{2}, y - i\sqrt{2}) = 1$, with $\mathbb{Z}[i\sqrt{2}]^* = \{-1 = (-1)^3, 1 = 1^3\}$, $y + i\sqrt{2}$ is a cube and so is $y - i\sqrt{2}$. So can find $a, b \in \mathbb{Z}$ with $(a + ib\sqrt{2})^3 = y + i\sqrt{2} = (a^3 - 6ab^2) + (3a^2b\sqrt{2} - 2b^3\sqrt{2})i$. Thus equating real and imaginary parts, $1 = 3a^2b - 2b^3 = b(3a^2 - 2b^2)$. So $b \mid 1 \implies b = \pm 1$. $b = -1 \implies$ no solution. $b = 1 \implies 3a^2 - 2 = 1 \implies a = \pm 1$. Real part is $y = a^3 - 6ab^2 = a(a^2 - 6b^2) = \mp 5$. So $x = 3$ by the original equation.

31 UFDs & Gauss' Lemma

Lemma 31.1. Let R be a UFD and $r, s \in R - 0$ with factorisation in irreducibles $r = p_1p_2 \dots p_m$, $s = q_1q_2 \dots q_n$. Then $r \mid s$ if and only if $m \leq n$ and permuting the q_i's if necessary, we can assume p_i and q_i are associates for $i = 1, 2, \dots, m$.

Proof. It is clear that if p_i and q_i are associates for $i = 1, 2, \dots, m$ and $m \leq n$ then $r \mid s$. To prove the converse, suppose $s = rt$ and $t = r_1r_2 \dots r_k$ is a factorisation into irreducibles. Then $p_1p_2 \dots p_mr_1r_2 \dots r_k = q_1q_2 \dots q_n$. So uniqueness of factorisation gives the observation.

Corollary 31.1. In a UFD, any irreducibles are primes.

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

Let R be a UFD and $r_1, r_2, \dots, r_k \in R$. A greatest common divisor $d \in R$ for $r_1, r_2, \dots, r_k$ is an element such that $d \mid r_i$ for all i and if $c \in R$ with $c \mid r_i$ for all i then $c \mid d$. Two greatest common divisors differ by at most a unit. They divide each other, and hence generate the same principal ideal.

Corollary 31.2. Let R be a UFD and $r_1, r_2, \dots, r_k \in R - 0$. Then there is a greatest common divisor for $r_1, r_2, \dots, r_k$.

Proof. Just prime factorise (irreducibles are primes in UFDs) each of the r_i's and pull out common factors (up to associates).

Let R be a UFD.

Definition 31.1 (Primitivity). $f \in R[x] - 0$ is primitive if 1 is the greatest common divisor for its coefficients.

Example 31.1. $3x^2 + 2 \in \mathbb{Z}[x]$ is primitive but $6x^2 + 4$ is not.

Proposition 31.1. Let R be a UFD, $K = K(R)$.

(i) Let $f \in K[x] - 0$, then there is some $\alpha \in K^*$ with $\alpha f \in R[x]$ and is primitive

(ii) If $f \in R[x] - 0$ is primitive and also there is $\alpha \in K^*$ such that $\alpha f \in R[x]$, then $\alpha \in R$

Proof. (i) Pick common denominator $d \in R - 0$ for all coefficients of f Then $df \in R[x]$. let c be the greatest common divisor of coefficients of df. Then $\alpha f = (\frac{d}{c})f \in R[x]$ is primitive as coefficients of $(\frac{d}{c})f$ has now greatest common divisor 1. (ii) Let $\alpha = \frac{n}{d}$ with $n \in R$, $d \in R - 0$. Then gcd(coefficients of $nf \in R[x]) = n\,\gcd$(coefficients of $f) = n \times 1 = n = d\,\gcd$(coefficients of $(\frac{b}{d})f$) $= d\,\gcd$(coefficients of $\alpha f \in R[x]) \implies n =$ multiple of $d \implies \alpha \in R$.

Theorem 31.1 (Gauss' Lemma). Let R be a UFD. The product of primitive polynomials in $R[x]$ is primitive.

Proof. Let $f = f_0 + f_1x + \ldots + f_mx^m \in R[x]$ and $g = g_0 + g_1x + \ldots + g_nx^n \in R[x]$ be primitive. It suffices to show that for any prime $p \in R$, p does not divide all the coefficients of $h = fg$. Pick a so that $p \nmid f_a$ but $f \mid f_{a+1}, p \mid p_{a+2}, \ldots$ and similarly pick b so $p \nmid g_b$ but $p \mid g_{b+1}, p \mid g_{b+2}, \ldots$ Look at $h_{a+b} =$ coefficient of x^{a+b} in $h = (f_0g_{a+b} + f_1g_{a+b-1} + \ldots + f_{a-1}g_{b+1}) + f_ag_b + (f_{a+1}g_{b-1} + \ldots + f_{a+b}g_0)$. $\because p$ divides all of $g_{b+1}, g_{b+2}, \ldots, g_{a+b}$ and p divides $f_{a+1}, f_{a+2}, \ldots, f_{a+b}$, but p does not divide f_ag_b $\therefore p \nmid h_{a+b}$ and h must be primitive.

Corollary 31.3. Let R be a UFD and $K = K(R)$. Let $f \in R[x]$ and suppose $f = gh$ with $g, h \in K[x]$. Then $f = \bar{g}\bar{h}$ with $\bar{g}, \bar{h} \in R[x]$ and $\bar{g} = \alpha_g g, \bar{h} = \alpha_h h$ where $\alpha_g, \alpha_h \in K[x]^* = K^*$.

Proof. By Proposition 31.1 (i), write $g = \beta_g g', h = \beta_h h'$ and $f = \beta_f f'$ where $f', g', h' \in R[x]$ are primitive and $\beta_f, \beta_g, \beta_h \in K^*$. Then $\beta_f f = (\beta_g\beta_h)g'h' = f \in R[x]$. By Gauss' Lemma, $g'h'$ is primitive. $\because f \in R[x]$ $\therefore \beta_g\beta_h \in R$ by Proposition 31.1 (ii). So we are done on setting $\bar{g} = \beta_g\beta_h g'$ and $\bar{h} = h'$.

Theorem 31.2. Let $R =$ UFD and $K = K(R)$.

(i) The primes in $R[x]$ are the primes of R or primitive polynomials (positive degree) which are irreducible in $K[x]$

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

Proof. (i) Follow from Corollary 31.3. (ii) $K[x]$ is a UFD. Check factorisation exists. let $f \in K[x]-0$. Factorise $f = \alpha f_1 f_2 \dots f_m$ in $K[x]$ with f_i irreducible in $K[x]$ and $\alpha \in K^*$. By Proposition 31.1(i), can assume all $f_i \in R[x]$ and are primitive. Gauss' Lemma $\implies f_1 f_2 \dots f_m$ is primitive. So Proposition 31.1 (ii) $\implies \alpha \in R$. Now prime factorisation $\alpha = \alpha_1 \alpha_2 \dots \alpha_n$ in R to get prime factorisation $f = \alpha_1 \alpha_2 \dots \alpha_n f_1 f_2 \dots f_m$. Check uniqueness. $K[x]$ is a UFD $\implies f_i$'s are unique up to scalar multiples in $K[x]^* = K^*$. Proposition 31.1 (ii) $\implies$ since these are primitive, they are unique up to primitives, i.e. R^*.

Corollary 31.4. Let R = UFD. Then $R[x_1, x_2, \dots x_n]$ is a UFD.

32 Simple Field Extensions

Definition 32.1 (Ring & Field Extension). Let F be a subring of E. Then we say E is a ring extension of F. Suppose further E and F are both fields. Then we say F is a subfield of E, or E or E/F is a field extension of F.

Let E/F be a field extension and $\alpha_1, \alpha_2, \dots, \alpha_n \in E$. Recall subring $F[\alpha_1, \alpha_2, \dots, \alpha_n] \subseteq E$, which is a domain. By Proposition 26.1 (ii), $F(\alpha_1, \alpha_2, \dots, \alpha_n) = K(F[\alpha_1, \alpha_2, \dots, \alpha_n])$ is a subfield of $K(E) = E$. It is called the subfield of E generated by $F, \alpha_1, \alpha_2, \dots, \alpha_n$.

Proposition 32.1. Let E/F be a field extension and $\alpha_1, \alpha_2, \dots, \alpha_n \in E$. Let $F_1 \subseteq E$ be a subfield containing $F, \alpha_1, \alpha_2, \dots, \alpha_n$. Then $F_1 \supseteq F(\alpha_1, \alpha_2, \dots, \alpha_n)$.

Proof. F_1 is a subring containing $F, \alpha_1, \alpha_2, \dots, \alpha_n$ so $F_1 \supseteq F[\alpha_1, \alpha_2, \dots, \alpha_n]$. But F is a field, so it contains all fractions in $F[\alpha_1, \alpha_2, \dots, \alpha_n]$. $\therefore F_1 \supseteq F(\alpha_1, \alpha_2, \dots, \alpha_n)$.

Example 32.1. $i \in \mathbb{C}$, $\mathbb{Q}(i) = K(\mathbb{Z}[i]) = \{a + bi : a, b \in \mathbb{Q}\}$.

Let E be a commutative ring extension of field F. E is a vector space over F with addition equal to ring addition and scalar multiplication equal to ring multiplication ($F \leq E$ as rings). The degree of the ring extension E/F is $[E : F] = \dim_F E$. We say E/F is finite if $[E : F]$ is finite.

Example 32.2. $[\mathbb{C} : \mathbb{R}] = 2$, so $\mathbb{C}/\mathbb{R}$ is finite.

Let E be a commutative ring extension of field F. Let $\alpha \in E$. Recall $F[\alpha] = \mathrm{Im}(\varepsilon_\alpha : F[x] \longrightarrow E; p(x) \longmapsto p(\alpha))$.

Proposition - Definition 32.1 (Transcendental & Algebraic). With above notation, exactly one of the following occurs.

(i) ε_α is injective, i.e. α is not a zero for any polynomial in $F[x]$ other than $p(x) \equiv 0$. In this case, we say α is transcendental over F.

(ii) $\ker(\varepsilon_\alpha) \neq 0$. But $F[x]$ is Euclidean domain with degree norm, hence is a PID, i.e. $\ker(\varepsilon_\alpha) = \langle p(x) \rangle$ where $p(x) \in \ker(\varepsilon_\alpha)$ is chosen to have minimal degree. So $p(\alpha) = 0$ and p is minimal with respect to degree. In this case, we say that α is algebraic over F and p is called the minimal or irreducible polynomial for α over F.

Example 32.3. The minimal polynomial for $\sqrt{2}$ is $x^2 - 2$ over $\mathbb{Q}$ and $x - \sqrt{2}$ over $\mathbb{Q}[\sqrt{2}]$.

Definition 32.2 (Algebraic Field Extension). Let E be a commutative ring extension of field F. We say E/F is algebraic if every $\alpha \in E$ is algebraic over F.

E is always algebraic over E as $\forall\ \alpha \in E$, we have $x - \alpha \in E[x]$.

Example 32.4. $\mathbb{C}/\mathbb{R}$ is algebraic for if $a, b \in \mathbb{R}$, then $x = a + bi$ satisfies $(x-a)^2 + b^2 = 0 \in \mathbb{R}[x]$.

Proposition 32.2. Let E be a finite commutative ring extension of field F. Then E/F is algebraic.

Proof. $F[x]$ and E are ring extensions of F, hence are vector spaces over F. Let $\alpha \in E$. But $\varepsilon_\alpha : F[x] \longrightarrow E$ is F-linear since it preserves addition and scalar multiplication, i.e. $\varepsilon_\alpha(ap) = \varepsilon_\alpha(a)\varepsilon_\alpha(p)$ (ring homomorphism) $= a\varepsilon_\alpha(p)$ for $a \in F, p \in F[x]$. Now $\dim_F F[x] = \infty$ and $\dim_F E < \infty$. So ε_α is not injective and α is algebraic.

Proposition 32.3. Let E be an algebraic commutative ring extension of field F. Suppose E is a domain. Then E is a field.

Proof. Let $\alpha \in E$ and $p(x) \in F[x]$ be its minimal polynomial. $p(x) = p_n x^n + p_{n-1}x^{n-1} + \ldots + p_1 x + p_0$. So $p_n\alpha^n + p_{n-1}\alpha^{n-1} + \ldots + p_1\alpha + p_0 = 0$. Note $p_0 \neq 0$, otherwise $\alpha(p_n\alpha^{n-1} + p_{n-1}\alpha^{n-2} + \ldots + p_1) = 0 \implies p_n\alpha^{n-1} + p_{n-1}\alpha^{n-2} + \ldots + p_1 = 0$ ($\alpha \neq 0$ and $F[x]$ is a domain). So α is a zero of $\frac{p(x)}{x}$. This contradicts minimality of $\deg(p)$. $\therefore\ p_0 \neq 0 \implies \alpha(p_n\alpha^{n-1} + \ldots + p_1) = -p_0 \implies \alpha^{-1} = -p_0^{-1}(p_n\alpha^{n-1} + p_{n-1}\alpha^{n-2} + \ldots + p_1)$, i.e. α is invertible and E is a field.

Let F be a field. A finitely generated field extension of F is a field extension of form $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. A simple field extension is one of the form $F(\alpha)$.

Theorem 32.1. Let E/F be a field extension. Let $\alpha \in E$.

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

(ii) If α is transcendental then $F(\alpha) \cong F(x) = K(F[x])$.

Proof. (i) Let $p = p_n x^n + p_{n-1}x^{n-1} + \ldots + p_0$, $p_n \neq 0$. $F[x]/\langle p \rangle \cong F[\alpha]$ (First Isomorphism Theorem) is spanned by $\{1 + \langle p \rangle, x + \langle p \rangle, \ldots, x^{n-1} + \langle p \rangle\}$. $\therefore F[\alpha]/F$ is finite. By Proposition 32.2, $F[\alpha]/F$ is algebraic and hence is also a field. $F(\alpha) = F[\alpha]$. Now $F[x]/\langle p \rangle$ is a field $\implies \langle p \rangle \trianglelefteq F[x]$, $\langle p \rangle \neq F[x]$ is maximum $\implies p \in F[x]$ irreducible, i.e. if $p = rs$, $r, s \in F[x]$, then $p \in \langle r \rangle \implies \langle p \rangle \subseteq \langle r \rangle \implies \langle p \rangle = \langle r \rangle$ as p is maximum $\implies s$ is a unit for $\langle p \rangle = \langle r \rangle$ or r is a unit for $\langle r \rangle = F[x]$. This gives (i). (ii) is clear as $\varepsilon_\alpha : F[x] \longrightarrow F[\alpha] \subseteq E$ is an isomorphism, due to bijectivity from transcendency. This gives isomorphism $F[x] \cong F[\alpha] \implies K(F[x]) \cong K(F[\alpha]) \implies F(x) \cong F(\alpha)$.

33 Algebraic Extensions

Theorem 33.1. Let $K \supseteq E \supseteq F$, E/F and K/E be finite field extensions. Then K/F is finite and $[K : F] = [K : E][E : F]$.

Proof. Let $e_1, e_2, \ldots, e_n$ be an F basis for E and $k_1, k_2, \ldots, k_m$ be an E basis for K. It suffices to show $B = \{e_i k_j : i = 1, 2, \ldots, n; j = 1, 2, \ldots, m\}$ is an F basis for K. Check B linearly independent over F. Suppose $\sum_{i,j} \alpha_{ij} e_i k_j = 0$ where $\alpha_{ij} \in F$. $\therefore (\sum_i \alpha_{i1} e_i)k_1 + (\sum_i \alpha_{i2} e_i)k_2 + \ldots + (\sum_i \alpha_{im} e_i)k_m = 0$ where $\sum_i \alpha_{ij} e_i \in E$ for all j. But k_i's are linearly independent over E $\implies \sum_i \alpha_{ij} e_i = 0$ for each j. But $\{e_i\}$ are also linearly independent over F. $\therefore \alpha_{ij} = 0$. So B is linearly independent. Check B spans. Let $k \in K$. We can write $k = \alpha_1 k_1 + \alpha_2 k_2 + \ldots + \alpha_m k_m$ where $\alpha_i \in E$. But each α_i is F linear combination of e_i's, so we are done.

Proposition 33.1. Let E/F be a field extension and $\alpha \in E$ algebraic over F with minimum polynomial $p(x) \in F[x]$ of degree d. Then $[F(\alpha) : F] = d$.

Proof. Suppose $p(x) = p_d x^d + \ldots + p_1 x + p_0$, $p_d \neq 0$. It suffices to show $B = \{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ in an F basis for $F(\alpha)$. Note $p_d \alpha^d + p_{d-1}\alpha^{d-1} + \ldots + p_1 \alpha + p_0 = 0 \implies \alpha^d$ is a linear combination of $\alpha^{d-1}, \alpha^{d-2}, \ldots, \alpha, 1$. So $\{1, \alpha, \ldots, \alpha^{d-1}\}$ spans $F[\alpha] = F(\alpha)$ ($F[\alpha]$ is a field). Check B linearly independent. But any linear relation amongst $\{1, \alpha, \ldots, \alpha^{d-1}\}$ gives a polynomial $p(x)$ with $p(\alpha) = 0$ and $\deg(p) < d$. This contradicts minimality of $\deg(p) = d$. Hence B is linearly independent and hence a basis. So property proved.

Example 33.1. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$ as $(\sqrt[4]{2})^2 = \sqrt{2}$. $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ as minimal polynomial is $x^2 - 2$. $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] = 2$ as minimal polynomial is $x^2 - \sqrt{2}$. $\therefore [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2^2 = 4$ and the minimal polynomial for $\sqrt[4]{2}$ over $\mathbb{Q}$ is $x^4 - 2$.

Corollary 33.1. Let E/F be a field extension and $\alpha_1, \alpha_2, \ldots, \alpha_n$ be algebraic over F. Then $F(\alpha_1, \alpha_2, \ldots, \alpha_n)/F$ is finite.

Proof. Just use induction on Theorem 33.1 and use Proposition 33.1 on $F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2) = F(\alpha_1)(\alpha_2) \subseteq \ldots \subseteq F(\alpha_1, \alpha_2, \ldots, \alpha_n)$, i.e. $[F(\alpha_1, \alpha_2, \ldots \alpha_n) : F] = [F(\alpha_1, \alpha_2, \ldots \alpha_{n-1})(\alpha_n) : F(\alpha_1, \alpha_2, \ldots \alpha_{n-1})][F(\alpha_1, \alpha_2, \ldots \alpha_{n-2})(\alpha_{n-1}) : F(\alpha_1, \alpha_2, \ldots \alpha_{n-2})] \ldots [F(\alpha_1) : F]$ and each term is finite, equal to the degree of the corresponding minimal polynomial ($\alpha_1, \alpha_2, \ldots, \alpha_n$ are all algebraic).

Theorem 33.2 (Eisenstein's Criterion). Let R be a UFD and $f = f_0 + f_1 x + \ldots + f_n x^n \in R[x]$. Suppose $p \in R$ is prime and $p \mid f_0, p \nmid f_n, p^2 \nmid f_0, p \mid f_i$ for $0 < i < n$, then f is irreducible.

Proof. By contradiction. Suppose $f = gh$ where $g = g_0 + g_1 x + \ldots + g_r x^r \in R[x]$, $h = h_0 + h_1 x + \ldots + h_s x^s \in R[x]$ and $r, s > 0$. $p \mid f_0 = g_0 h_0$ but $p^2 \nmid f_0$, i.e. p does not divide both g_0 and h_0. So we can assume $p \mid g_0$ but $p \nmid h_0$. We will derive a contradiction to $p \nmid f_n$ by showing $p \mid g$. We show $p \mid g$ by induction on i. For $i < n$, $f_i = g_0 h_i + g_1 h_{i-1} + \ldots + g_{i-1} h_1 + g_i h_0 \in \langle p \rangle$ as $p \mid f_i$. $\because$ $p \mid g_1 h_{i-1}, p \mid g_2 h_{i-2}, \ldots, p \mid g_{h-1} h_1$ $\therefore p \mid g_i h_0$. But $p \nmid h_0$ $\therefore p \mid g_i$. This completes the proof.

Example 33.2. Different ways of showing minimum polynomial for $\sqrt[4]{2}$ over $\mathbb{Q}$ is $x^4 - 2$. Let p be minimum polynomial for $\sqrt[4]{2}$. So $p \mid x^4 - 2$. Eisenstein's Criterion with $p = 2 \implies x^4 - 2$ is irreducible. So p and $x^4 - 2$ are associates.

Proposition 33.2. let $\phi : F \longrightarrow R$ be a ring homomorphism with F a field and $R \neq 0$. Then ϕ is injective.

Proof. ϕ not injective $\Longrightarrow \ker(\phi) \neq 0 \Longrightarrow \ker(\phi)$ contains units $\Longrightarrow \ker(\phi) = F$ ($\ker(\phi)$ is an ideal with units, $\phi(1) = 1 = 0$) $\Longrightarrow$ id $= 0$ map on $R \Longrightarrow R = 0$, which is a contradiction.

Proposition - Definition 33.1 (Algebraic Closure). A field F is algebraically closed if one of the following equivalent conditions hold.

(i) Any $p(x) \in F[x]$ has zero in F.

(ii) There are no non-trivial algebraic extension of F (the trivial extension being F/F).

Proof. (i) $\Longrightarrow$ (ii). Use contradiction. Suppose E/F is an algebraic field extension and $\alpha \in E - F$. Let $p \in F[x]$ be minimum (irreducible) polynomial for α over F. Also $\deg(p) > 1$. But $p(x)$ has zero, say γ in F. So by factor theorem, $x - \gamma$ is a factor of $p(x)$. This contradicts the irreducibility of $p(x)$. Note $\deg(p) = 1 \Longrightarrow \alpha \in F$, so $\alpha \in E - F \Longrightarrow \deg(p) > 1$. (ii) $\Longrightarrow$ (i). Let $p \in F[x]$. Replacing p with prime factor $\Longrightarrow$ can assume p is irreducible. Consider $F[x]/\langle p \rangle$. $\because F[x]$ is an Euclidean domain hence a PID. $\langle p \rangle$ is maximal, so $F[x]/\langle p \rangle$ is a field. So by Proposition 33.2, we see $F \longrightarrow F[x]/\langle p \rangle$ is injective. So $F[x]/\langle p \rangle$ is a finite field extension of F. So $F[x]/\langle p \rangle$ is algebraic. Given (ii), it must be trivial. By Proposition 33.1, degree of extension is p, i.e. $F[x]/\langle p \rangle \cong F[\alpha] = F(\alpha) \Longrightarrow [F[x]/\langle p \rangle : F] = [F(\alpha) : F] = \deg(p)$. So $\deg(p) = 1$, i.e. linear polynomial in $F \Longrightarrow p$ has a zero in F.

Theorem 33.3. Any field F has an algebraic extension $\tilde{F}$ which is algebraically closure of F and is unique up to isomorphism.

34 Ruler & Compass Constructions

Bisection of an angle, constructions of an equilateral triangle and a regular hexagon can all be carried out easily with a ruler and a pair of compasses. Can you trisect an angle or constrict a regular pentagon in the same way?

The following is known as the Ruler and Compass Game. Start with subfield $F \subseteq \mathbb{R}$ and set of points Pt_0 in $\mathbb{R}^2$ with all coordinates in F, i.e. $Pt_0 \subseteq F^2 \subseteq \mathbb{R}^2$. Set $LC_0 = \emptyset$. Construct inductively set of points Pt_i in $\mathbb{R}^2$ and LC_i, set of lines and circles in $\mathbb{R}^2$, suppose Pt_{i-1} and LC_{i-1} defined.

1. Either draw a line through 2 points in Pt_{i-1} and add this to get LC_i or draw a circle with centre in Pt_{i-1} and passing through another point in Pt_{i-1} and add this circle to LC_{i-1} to get LC_i.

2. Enlarge Pt_{i-1} to Pt_i by adding in all the points of intersection of all lines and circles in LC_i.

3. Repeat steps 1 and 2 as desired.

A figure is constructible from F if you can get it from the Ruler and Compass Game. Say it is constructible if $F = \mathbb{Q}$.

Suppose in step 1 of the Ruler and Compass Game, you only add lines. Then $Pt_i \subseteq F^2$ always for $Pt_0 \subseteq F^2$, i.e. points always have coordinates in F. By induction, suppose $a, b, c, d \in Pt_{i-1} \subseteq F^2$. New points arise from intersecting lines such as ab and cd. To compute points of intersection, solve $a + \lambda(b-a) = c + \mu(d-c)$ for $\lambda, \mu \in \mathbb{R}$. This corresponds to system of liner equations in F. Hence $\lambda, \mu \in F$, so must be coordinates of the points of intersection.

Proposition 34.1. Suppose in the Ruler and Compass Game, $Pt_{i-1} \subseteq E^2$ for some field E.

(i) Any line (circle) in LC_i is defined by a linear (quadratic) equation with coefficients in E.

(ii) The point of intersection of two circles in LC_i has coordinates in E (quadratic terms cancel).

(iii) Let L, C be a line, a circle respectively in LC_i. Then there is some $\Delta \in E$ such that coordinates of point of intersection of L and C lie in $E(\Delta)$ (due to the quadratic formula).

Proof. (i) By induction, suppose C is a circle with centre $(a, b) \in E^2$ and passing through $(c, d) \in E^2$. Then C is defined by $(x-a)^2 + (y-b)^2 = (a-c)^2 + (b-d)^2$ which is quadratic in x, y with coefficients in E. Case for lines is similar. (ii) is similar to the proof of (iii). (iii)By (i), can assume L, C given by $C : x^2 + y^2 + a_1 x + b_1 y = c_1$ and $L : a_2 x + b_2 y = c_2$. Assume $b_2 \neq 0$ (since at least one of a_2, b_2 is non-zero, else swap roles of x, y). Use equation of L to eliminate y from equation of C. This gives a quadratic in x with say discriminant Δ. Quadratic formula $\implies x \in E(\sqrt{\Delta})$. From equation of L, we see $y \in E(\sqrt{\Delta})$ as well. Note $E(\sqrt{\Delta}) = E$ if and only if $\sqrt{\Delta} \in E$, i.e. Δ is a square in E. $[E(\sqrt{\Delta}) : E] = 2$.

Theorem 34.1. Suppose in the Ruler and Compass Game, $p \in Pt_j$ for some j. Then there is a tower of field extensions $F \subseteq F_1 \subseteq F_2 \subseteq \ldots \subseteq F_n$, where $F_{i+1} = F_i(\sqrt{\Delta_i})$ for some non-square $\Delta_i \in F_i$ and such that $p \in F_n^2$. Note $[F_n : F] = [F_n : F_{n-1}][F_{n-1} : F_{n-2}] \ldots [F_1 : F] = 2^n$.

Proof. Use induction on Proposition 34.1.

Theorem 34.2. It is impossible to trisect angles using rulers and compasses in general.

Proof. We will prove the impossibility of trisecting an angle of $60°$. Start with $F = \mathbb{Q}(\sqrt{3})$. $Pt_0 = \{(0,0), (1, \sqrt{3}), (1, 0)\}$. Suppose trisecting line L of a $60°$ angle is constructible from F. Then add unit circle. We see there is a field extension F_n/F as in Theorem 34.1 with $(\cos 20°, \sin 20°) \in F_n^2$. Seek contradiction. What is minimum polynomial of α over $\mathbb{Q}$? Recall $\cos 3\theta = \cos^3\theta - 3\cos\theta$. So $4\alpha^3 - 3\alpha = \cos 60° = \frac{1}{2}$, i.e. α satisfies $8\alpha^3 - 6\alpha - 1 = 0$. We can show this is irreducible over $\mathbb{Q}$ by noting the following are not roots $\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$. So $8x^3 - 6x - 1$ is not reducible over $\mathbb{Q}$. So $8x^3 - 6x - 1 = 0$ is minimum polynomial for α. Hence $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. But $[F_n : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = [F_n : \mathbb{Q}] = [F_n : F][F : \mathbb{Q}] = [F_n : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] \implies 3k = 2^n \times 2 = 2^{n+1}$. But $3 \nmid 2^{n+1}$. So contradiction gives impossibility of trisecting $60°$ with rulers and compasses.

35 Finite Fields

Example 35.1. Let $p \in \mathbb{N} - 0$ be prime. Then $\langle p \rangle \trianglelefteq \mathbb{Z}$ is maximal, so $\mathbb{Z}/p\mathbb{Z}$ is a field denoted $\mathbb{F}_p$.

Proposition 35.1. Let F be a field.

(i) The map $\phi : \mathbb{Z} \longrightarrow F; n \longmapsto n = \underbrace{1+1+\ldots+1}_{n}$ is a ring homomorphism.

(ii) Exactly one of the following holds.

(a) ϕ is injective and so induces an injection of fields $\phi : \mathbb{Q} \longrightarrow F$. In this case, we say F has characteristic 0 and write $\text{char}(F) = 0$.

(b) $\ker(\phi) \neq 0$, i.e. $\ker(\phi) = \langle p \rangle$ (ideal), where $p \in \mathbb{N} - 0$ is prime. In this case, we say F has characteristic p and write $\text{char}(F) = p$. Induced map $\bar{\phi} : \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \longrightarrow F$ makes F a field extension of $\mathbb{F}_p$ ($\bar{\phi}$ is injective).

Proof. (i) Check definition. (ii) Easy exercise, using fact that $\mathbb{Z}/n\mathbb{Z}$ is domain if and only if n is prime.

Example 35.2. $\text{char}(\mathbb{R}) = 0, \text{char}(\tilde{\mathbb{F}}_p) = p$. For a field F, the algebraic closure is denoted by $\tilde{F}$.

Proposition 35.2. Let F be a finite (as set) field. Then $\text{char}(F) = p > 0$ and $|F| = p^{[F:\mathbb{F}_p]}$, i.e. any finite field has prime characteristic.

Proof. F finite $\Longrightarrow \mathbb{Z}$ not a subset. So in this case, we have case (b) of Proposition 35.1 (ii). Also as F is a field extension of $\mathbb{F}_p$, then F is a vector space over $\mathbb{F}_p$ of dimension $[F : \mathbb{F}_p] = d$. Hence $F \cong \underbrace{\mathbb{F}_p \times \mathbb{F}_p \times \ldots \mathbb{F}_p}_{[F:\mathbb{F}_p]}$ as vector spaces, i.e. $|F| = |\mathbb{F}_p|^{[F:\mathbb{F}_p]} = p^{[F:\mathbb{F}_p]}$.

Let $p \in \mathbb{N} - 0$ be prime and $n \in \mathbb{N}$. Write $\mathbb{F}_{p^n}$ for any field with p^n elements. We can show existence and uniqueness of $\mathbb{F}_{p^n}$.

Proposition - Definition 35.1 (Frobenius Norm). Let F be a field. $\text{char}(p) > 0$. The map $\phi : F \longrightarrow F; x \longmapsto x^p$ is a ring homomorphism called Frobenius norm.

Proof. $\phi(x+y) = (x+y)^p = x^p + \binom{p}{1} x^{p-1}y + \binom{p}{2} x^{p-2}y^2 + \ldots + \binom{p}{p-1} xy^{p-1} + y^p$. Now $\binom{p}{1}, \binom{p}{2}, \ldots, \binom{p}{p-1}$ are all divisible by p and 0 in F. So $\phi(x+y) = x^p + y^p = \phi(x) + \phi(y)$. Also $\phi(xy) = (xy)^p = x^p y^p = \phi(x)\phi(y)$. Lastly, $\phi(1) = 1 = 1^p$, so ϕ is a ring homomorphism.

Lemma 35.1. Let E/F and K/E ($F \subseteq E \subseteq K$) be algebraic field extensions. Then K/F is algebraic.

Proof. Suffice to show $\alpha \in K$ is algebraic over F. K/E algebraic $\Longrightarrow \alpha^n + e_{n-1}\alpha^{n-1} + \ldots + e_0 = 0$ for some $e_{n-1}, e_{n-2}, \ldots, e_0 \in E$. Now $F(e_{n-1}, e_{n-2}, \ldots, e_0)/F$ is algebraic as $F(e_{n-1}, e_{n-2}, \ldots, e_0) \subseteq E$. Using Corollary 33.1, $F(e_{n-1}, e_{n-2}, \ldots, e_0)/F$ is finite. Also α is algebraic over $F(e_{n-1}, e_{n-2}, \ldots, e_0) \Longrightarrow$ $F(\alpha, e_{n-1}, e_{n-2}, \ldots, e_0)/F(e_{n-1}, e_{n-2}, \ldots, e_0) = F(e_{n-1}, e_{n-2}, \ldots, e_0)(\alpha)/F(e_{n-1}, e_{n-2}, \ldots, e_0)$ is finite. Using Theorem 33.1, $F(\alpha, e_{n-1}, e_{n-2}, \ldots, e_0)/F$ is finite and hence α is finite over F. So we have transitivity of algebraic field extensions.

Proposition 35.3. A finite field of characteristic p is a subfield of $\tilde{\mathbb{F}}_p$.

Proof. $F \subseteq \tilde{F}$ with $\tilde{F}/F$ algebraic by definition. $\tilde{F}/\mathbb{F}_p$ is finite and hence algebraic. Lemma 35.1 $\implies \tilde{F}/\mathbb{F}_p$ is algebraic. But $\tilde{F}$ is algebraically closed, so uniqueness of algebraic closure $\implies \tilde{\mathbb{F}}_p \cong \tilde{F} \supseteq F$ as desired.

Theorem 35.1. Let $\phi : \tilde{\mathbb{F}}_p \longrightarrow \tilde{\mathbb{F}}_p; x \longmapsto x^p$ be Frobenius norm. Let $F_{p^n} = \{\alpha \in \tilde{\mathbb{F}}_p : \phi^n(\alpha) = \alpha\} =$ set of zeros of $x^{p^n} - x$ in $\tilde{\mathbb{F}}_p$.

(i) F_{p^n} is a subfield of $\tilde{\mathbb{F}}_p$.

(ii) $|F_{p^n}| = p^n$.

(iii) Any subfield F of $\mathbb{F}_p$ with p^n elements is equal to F_{p^n}.

Proof. Do (iii) and (ii) first. Let F be as in (iii). Lagrange's Theorem on $F^* \implies |F^*| = |F| - 1 = p^n - 1$ (exclude 0). So for any $\alpha \in F^*$, $\alpha^{p^n-1} = 1$ (order $p^n - 1$). So $\alpha^{p^n} - \alpha = 0$ for any $\alpha \in F$, i.e. α is a solution to $x^{p^n} - x$. Hence $F \subseteq F_{p^n}$. Using factor theorem, $x^{p^n} - x$ factors into linear factors in $\tilde{\mathbb{F}}_p[x]$. $\therefore$ number of zeros $\leq \deg(x^{p^n} - x) = p^n \implies |F_{p^n}| \leq p^n$. But $|F_{p^n}| \geq |F| = p^n$, so $|F_{p^n}| = p^n$ and $F_{p^n} = F$. So (iii) holds. To finish proof of (ii), suffice to show zeros of $x^{p^n} - x$ are distinct. $x^{p^n} - x = x(x^{p^n-1} - 1)$, so $x = 0$ is not a multiple root. Check another zero α is not multiple by changing variable to $y = x - \alpha$. $x^{p^n} - x = (y+\alpha)^{p^n} - (y+\alpha) = y^{p^n} + \binom{p^n}{1} y^{p^n-1}\alpha + \ldots + \alpha^{p^n} - y - \alpha$ (note $\binom{p^n}{1}, \binom{p^n}{2} \ldots$ are all zero, as they are all multiples of p) $= y^{p^n} - y$ (as $\alpha^{p^n} - \alpha = 0$ by assumption) $= y(y^{p^n-1} - 1)$. As y is not a multiple factor, $x - \alpha$ is not a multiple factor for $x^{p^n} - x$. So $x^{p^n} - x$ has p^n distinct zeros and (ii) holds. Alternatively, using Galois Theory, note $\frac{d}{dx}(x^{p^n} - x) = p^n x^{p^n-1} - 1 = 0 - 1 = -1 \neq 0$. So no multiple root exists. (i) To show F_{p^n} is a subfield, suffices to check closure axioms for subring because then it is a finite field extension of $\mathbb{F}_p$ which is a domain. Check closure under addition. Note ϕ^n is ring homomorphism, begin composite of such. Let $x, y \in F_{p^n}$. Then $\phi^n(x + y) = \phi^n(x) + \phi^n(y) = x + y \in F_{p^n}$. Other closure axioms similarly proved. This shows $F_{p^n} = \mathbb{F}_{p^n}$.

36 Conjugation & p-Groups

Let G be a group. Define $\mathrm{Aut}(G)$ to be the set of automorphisms $\phi : G \xrightarrow{\sim} G \leq \mathrm{Perm}(G)$.

Proposition 36.1. $\mathrm{Aut}(G) \leq \mathrm{Perm}(G)$.

Proof. Straight forward, just check axioms.

Conjugation aims to study groups via internal symmetry. Let $g \in G$, we redefine conjugation by g to be the map $C_g : G \longrightarrow G; h \longmapsto ghg^{-1}$. Recall from Proposition 36.1 that $C_g \in \mathrm{Aut}(G)$.

Proposition 36.2. The map $C : G \longrightarrow \mathrm{Aut}(G); g \longmapsto C_g$ is a group homomorphism.

Proof. $g_1, g_2, h \in G$. $C_{g_1g_2}(h) = g_1g_2h(g_1g_2)^{-1} = g_1g_2hg_2^{-1}g_1^{-1} = C_{g_1}(g_2hg_2^{-1}) = C_{g_1}C_{g_2}(h)$. So C is a group homomorphism.

Note that the Propositions 36.1 and 36.2 gives composite group homomorphism $G : \xrightarrow{C} \mathrm{Aut}(G) \hookrightarrow \mathrm{Perm}(G)$. So we have permutation representation of G on G. We say G acts G by conjugation. There is a corresponding G-set with G-action for $g, h \in G$, $h.g = C_h(g) = hgh^{-1}$.

Let group G act on G by conjugation. We define the G-orbits to be conjugate classes and they have form $G.h = \{ghg^{-1} : g \in G\}$. We define the centre of G to be the fixed point set. It is denoted by

$$\begin{aligned} Z(G) &= \{z \in G : gzg^{-1} = z \text{ for all } g \in G\} \\ &= \{z \in G : gz = zg \text{ for all } g \in G\} \\ &= \{z \in G : \text{conjugate class } G.z \text{ with just } \{z\}\} \\ &= \{z \in G : zgz^{-1} = g \text{ for all } g \in G\} \\ &= \text{kernel of conjugation map } C : G \longrightarrow \mathrm{Aut}(G); g \longmapsto C_g \end{aligned}$$

Proposition 36.3. $Z(G) \trianglelefteq G$ (since kernels are normal subgroups).

Definition 36.1. Let $p \in \mathbb{N} - 0$ be prime. We say G is a p-group if $|G| = p^r$ for some $r \in \mathbb{N}$. Suppose $|G| = p^r q$ for some q with $\gcd(p, q) = 1$. A subgroup H of G is a Sylow p-subgroup if $|H| = p^r$.

Example 36.1. G is the dihedral group. D_p with p odd prime. Say $G = \langle \sigma, \tau \rangle$ with $\sigma^p = 1 = \tau^2$, $\tau\sigma = \sigma^{-1}\tau$. Then $|G| = 2p$ and $\langle \sigma \rangle$ is a Sylow p-subgroup. $\langle \tau \rangle, \langle \sigma\tau \rangle, \ldots, \langle \sigma^{p-1}\tau \rangle$ are Sylow 2-subgroups.

Lemma 36.1. Let $G \neq 1$ be a p-group acting on a finite set S. Then

(i) $p \mid |S - S^G| = |S| - |S^G|$

(ii) $Z(G) \neq 1$ (not trivial)

Proof. (i) The elements of S^G are precisely the one element orbit of S. Hence we have $S = S^G \dot\cup G.s_1 \dot\cup \ldots \dot\cup G.s_r$ by grouping one point orbits together. But $s_i \notin S^G$ means $\mathrm{stab}_G(s_i) \lneq G$. So $|G.s_i| = |\frac{G}{\mathrm{stab}_G(s_i)}| = \frac{|G|}{|\mathrm{stab}_G(s_i)|} \Longrightarrow$ power of $p > 1 \Longrightarrow |G| = |G.s_i||\mathrm{stab}_G(s_i)|$, i.e. $p \mid |G.s_i| \Longrightarrow p|\sum_i |G.s_i| = |Gs_1 \dot\cup Gs_2 \dot\cup \ldots \dot\cup Gs_r| = |S - S^G|$. (ii) Apply (i) to G acting on $S = G$ by conjugation, $p \mid |S| - |Z(G)| = |G| - |Z(G)|$. But $p \mid |G|$, so $p \mid |Z(G)| \Longrightarrow Z(G) \neq 1$.

Corollary 36.1. Let $p \in \mathbb{N} - 0$ be prime. Let G be a group of order p^2. Then G is isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Proof. Suppose G is not cyclic, so there are no elements of order p^2. Lagrange's Theorem says that orders of all non-trivial subgroups and non-identity element is p. Lemma 36.1 $\Longrightarrow Z(G) \neq 1$. So let us pick $z \in Z(G) - 1$. z is order p so $\langle z \rangle \cong \mathbb{Z}/p\mathbb{Z}$. Pick $y \in G - \langle z \rangle$ and again $\langle y \rangle \cong \mathbb{Z}/p\mathbb{Z}$. It suffices to prove $G \cong \langle z \rangle \times \langle y \rangle$. We use internal characteristics of direct products, i.e. Proposition 12.2. We check the conditions of the proposition. (i) $\langle z, y \rangle \supsetneq \langle z \rangle$ so $|\langle z, y \rangle| > p \Longrightarrow \langle z, y \rangle = G$ as $\langle z, y \rangle \leq G$. So z and y generates G. (ii) $\langle z \rangle \cap \langle y \rangle$ is a proper subgroup of $\langle z \rangle \cong \mathbb{Z}/p\mathbb{Z}$, which has only two subgroups, so $\langle z \rangle \cap \langle y \rangle = 1$. (iii) Now $\langle z \rangle \subseteq Z(G)$, so elements of $\langle z \rangle$ certainly commute with all elements of G, hence $\langle y \rangle$. This shows $G \cong \langle z \rangle \times \langle y \rangle = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

37 Sylow's Theorems

Lemma 37.1. Let G be a group of order$|G| = p^r q$ and let S be set of all subsets of G with p^r elements. Then $p \nmid |S| = \begin{pmatrix} p^r q \\ p^r \end{pmatrix}$.

Proof. For $i \in \mathbb{N}$ and $l \in \{1, 2, \ldots, p^r - 1\}$, we have $p^i \mid l$ if and only if $p^i \mid p^r q - l$. $|S| = \frac{p^r q(p^r q-1)\ldots(p^r q-p^r+1)}{p^r(p^r-1)\ldots 2\times 1}$. By pairing $\frac{p^r q-l}{l}$ for $l \in \{1, 2, \ldots, p^r - 1\}$, all powers of p in numerator cancels with powers of p in denominator. Hence $p \nmid |S|$.

Theorem 37.1 (Sylow's Theorem). Let $p \in \mathbb{N}-0$ be a prime. Let G be a group of order$|G| = p^r q$ where $r \in \mathbb{N}$, $\gcd(p, q) = 1$.

(i) There exist Sylow p-subgroups and let P be one such.

(ii) If H is any p-subgroup then H is contained in a conjugate of P, in particular two Sylow p-subgroups are conjugate.

(iii) Let m be the number of Sylow p-subgroups, then $m \mid |G|$ and $p \mid m - 1$.

Proof. (i) Let S be set of all subsets of G with p^r elements. We define G-action of S by $g.S = \{gs : s \in S\}$ for $g \in G, s \in S$. Check it is a G-set. $1.s = 1s = s$ and $g.(h.s) = g.hs = ghs = (gh)s = (gh).s$. Hence S is a G-set. Decompose S into G-orbits, $S = G.s_1 \dot\cup G.s_2 \dot\cup \ldots \dot\cup G.s_r$. By Lemma 37.1, we can pick S_i with $p \nmid |G.s_i|$. We now need only prove claim $P = \text{stab}_G(s_i)$ has order p^r. $p \nmid |G.s_i| = \frac{|G|}{|\text{stab}_G(s_i)|}$, i.e. $p^r \mid |P|$. Suffices to show $|P| \leq p^r$. Pick an element s_i. Note $P = \text{stab}_G(s_i)$ means any s_i satisfies $PS_i \cong S_i$. In particular, $Ps_i \in S_i$. Hence $|PS| \leq |S_i| = p^r$. This shows $|P| = p^r$. So P is a Sylow p-subgroup. (ii) Let $P \leq G$ be a Sylow p-subgroup. Let $H \leq G$ be any p-subgroup. Wish to show $H \subseteq$ conjugate of P. Let $S = G/P$. Define H-action by $h.(gP) = (hg)P$ $(h \in H, gP \in G/P)$. As an exercise, check it is an H-set. In fact, it comes from G-set G/P by restricting action to H. By Lemma 36.1, $p \mid |S| - |S^H|$. But $|S| = |G/P| = \frac{|G|}{|P|} = q$ not divisible by $p \implies p \nmid |S^H|$. So $S^H \neq 0$. Let $P \in S^H$. this means for any $h \in H$, we have $gP = h.gP = (hg)P \implies P = (g^{-1}hg)P$ for all $h \in H \iff g^{-1}hg \in P$ for all $h \in H$. Hence $g^{-1}Hg \subseteq P$ or $H \subseteq gPg^{-1}$. Hence H is contained in a conjugate of P, giving (ii). (iii)Prove that $m \mid |G|$. Let $S = \{P_1, P_2, \ldots, P_m\}$ be the Sylow p-subgroups of G. Define G-action on S by $g.P_i = gP_ig^{-1}$ for $g \in G$. Note $|gP_ig^{-1}| = |P_i| = p^r$, so $gP_ig^{-1} \in S$. As an exercise, check S is a G-set. Sylow's Theorem (ii) says all elements of S are conjugate of P_i say. So S is a single G-orbit. $|S| = |\frac{G}{\text{stab}_G(P_i)}| \implies m \mid |G|$.

Theorem 37.2. Let p be an odd prime. Then any subgroup G of order $2p$ is isomorphic to D_p or $\mathbb{Z}/2\mathbb{Z}$.

Proof. Suppose G is not cyclic. Lagrange' Theorem $\implies$ non-trivial subgroups have order 2 or p. Also non-identity elements have order 2 or p. Sylow's Theorem (i) $\implies$ there is a $P \leq G$ with $|P| = p$ and $[G : P] = \frac{|G|}{|P|} = 2 \implies P$ is normal in $G \implies P \trianglelefteq G, P \neq G$. Sylow's Theorem (ii) $\implies P$ is the unique subgroup of order p. $p = |P|$ prime $\implies P = \langle\sigma\rangle$ with $\sigma^p = 1$. Pick $\tau \in G - P$. Order of τ is 2. Otherwise it generates distinct Sylow p-subgroups. Similarly $\tau\sigma$ has order 2. Note $[G : P] = 2$. We have $G = P \dot\cup \tau P = \{1, \sigma, \sigma^2, \ldots, \sigma^{p-1}, \tau, \tau\sigma, \ldots, \tau\sigma^{p-1}\}$ with $\sigma^p = \tau^2 = 1$. Also $(\tau\sigma)^2 = \tau\sigma\tau\sigma = 1 \implies \sigma\tau = \tau\sigma^{-1}$. Using these relations, we can determine multiplication for G. So D_p and G have same multiplication table, so are isomorphic.