MATH456 - Algebra 3

Groups; ring theory; fields.

Based on lectures from Fall 2024 by Prof. Henri Darmon.
Notes by Louis Meunier

Contents

§1 Groups

§1.1 Definitions

↪**Definition 1.1** (Group): A **group** is a set G endowed with a binary composition rule $G \times G \to G, (a,b) \mapsto a \star b$, satisfying

1. $\exists\, e \in G$ s.t. $a \star e = e \star a = a \;\forall\, a \in G$
2. $\forall\, a \in G, \exists\, a' \in G$ s.t. $a \star a' = a' \star a = e$
3. $\forall\, a,b,c \in G, (a \star b) \star c = a \star (b \star c)$.

If the operation on G also commutative for all elements in G, we say that G is *abelian* or *commutative*, in which case we typically adopt additive notation (i.e. $a+b$, $a^{-1} = -a$, etc).

⊛ **Example 1.1**: An easy way to "generate" groups is consider some "object" X (be it a set, a vector space, a geometric object, etc.) and consider the set of symmetries of X, denoted $\mathrm{Aut}(X)$, i.e. the set of bijections of X that preserve some desired quality of X.

1. If X just a set with no additional structure, $\mathrm{Aut}(X)$ is just the group of permutations of X. In particular, if X finite, then $\mathrm{Aut}(X) \cong S_{\#X}$.
2. If X a vector space over some field $\mathbb{F}$, $\mathrm{Aut}(X) = \{T : X \to X \mid \text{linear, invertible}\}$. If $\dim(X) = n < \infty$, $X \cong \mathbb{F}^n$ as a vector space, hence $\mathrm{Aut}(X) = \mathrm{GL}_n(\mathbb{F})$, the "general linear group" consisting of invertible $n \times n$ matrices with entires in $\mathbb{F}$.
3. If X a ring, we can always derive two groups from it; $(R, +, 0)$, which is always commutative, using the addition in the ring, and $(R^\times, \times, 1)$, the units under multiplication (need to consider the units such that inverses exist in the group).
4. If X a regular n-gon, $\mathrm{Aut}(X)$ can be considered the group of symmetries of the polygon that leave it globally invariant. We typically denote this group by D_{2n}.
5. If X a vector space over $\mathbb{R}$ endowed with an inner product $(\cdot,\cdot) : V \times V \to \mathbb{R}$, with $\dim V < \infty$, we have $\mathrm{Aut}(V) = O(V) = \{T : V \to V \mid T(v \cdot w) = v \cdot w \;\forall\, v,w \in V\}$, the "orthogonal group".

↪**Definition 1.2** (Group Homomorphism): Given two groups G_1, G_2, a *group homomorphism* $\varphi : G_1 \to G_2$ is a function satisfying $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G_1$.

If φ is bijective, we call it an *isomorphism* and say G_1, G_2 are *isomorphic*.

↪**Proposition 1.1**:

- $\varphi\left(1_{G_1}\right) = 1_{G_2}$
- $\varphi\left(a^{-1}\right) = \varphi(a)^{-1}$

⊛ **Example 1.2**: Let $G = \mathbb{Z}/n\mathbb{Z} = \{0, ..., n-1\}$ be the cyclic group of order n. Let $\varphi \in \mathrm{Aut}(G)$; it is completely determined by $\varphi(1)$, as $\varphi(k) = k \cdot \varphi(1)$ for any k. Moreover, it must be then that $\varphi(1)$ is a generate of G, hence $\varphi(1) \in (\mathbb{Z}/n\mathbb{Z})^\times$ (ie the units of the group considered as a ring), and thus

$$\mathrm{Aut}(G) \cong \left((\mathbb{Z}/n\mathbb{Z})^\times, *\right).$$

§1.2 Actions of Groups

↪**Definition 1.3** (Group Action): An *action* of G on an object X is a function $G \times X \to X, (g, x) \mapsto g \cdot$ such that

- $1 \cdot x = x$
- $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$
- $m_g : x \mapsto g \cdot x$ an *automorphism* of X.

↪**Proposition 1.2**: The map $m : G \to \mathrm{Aut}(X), g \mapsto m_g$ a group homomorphism.

Proof. One need show $m_{g_1 g_2} = m_{g_1} \circ m_{g_2}$. ■

↪**Definition 1.4** (G-set): A *G-set* is a set X endowed with an action of G.

↪**Definition 1.5** (Transitive): We say a G-set X is *transitive* if $\forall\, x, y \in X$, there is a $g \in G$ such that $g \cdot x = y$.

A transitive G-subset of X is called on *orbit* of G on X.

↪**Proposition 1.3**: Every G-set is a disjoint union of orbits.

Proof. Define a relation on X by $x \sim y$ if there exists a $g \in G$ such that $g \cdot x = y$. One can prove this is an equivalence relation on X. Equivalence relations partition sets into equivalence classes, which we denote in this case by X/G. The proof is done by remarking that an equivalence class is precisely an orbit. ■

Remark 1.1: As with most abstract objects, we are more interested in classifying them up to isomorphism. The same follows for G-sets.

↪**Definition 1.6**: An *isomorphism of G-sets* is a map between G-sets that respects the group actions. Specifically, if G a group and X_1, X_2 are G-sets, with the action G on X_1 denoted $\star$ and G on X_2 denoted $*$, then an isomorphism is a bijection

$$f : X_1 \to X_2,$$

such that

$$f(g \star x) = g * f(x)$$

for all $g \in G$, $x \in X_1$.

↪**Definition 1.7** (Cosets): Let $H \subseteq G$ be a subgroup of a group G. Then G carries a natural structure as an H set; namely we can define

$$H \times G \to g, \quad (h, g) \mapsto g \cdot h,$$

which can readily be seen to be a well-defined group action. We call, in this case, the set of orbits of the action of H on G *left cosets* of H in G, denoted

$$\begin{aligned} G/H &= \{\text{orbits of } H \text{ acting on } G\} \\ &= \{aH : a \in G\} = \{\{ah : h \in H\} : a \in G\} \subseteq 2^G. \end{aligned}$$

Symmetric definitions give rise to the set of *right cosets* of H in G, denoted $H \setminus G$, of orbits of H acting by left multiplication on G.

Remark 1.2: In general, $G/H \neq H \setminus G$. Further, note that at face value these are nothing more than sets; in general they will not have any natural group structure. They do, however, have a natural structure as G-sets, as a theorem to follow will elucidate.

↪**Theorem 1.1**: Let $H \subseteq G$ be a finite subgroup of a group G. Then every coset of H in G has the same cardinality.

Proof. Define the map $H \mapsto aH$ by $h \mapsto ah$. This is a bijection. ■

Remark 1.3: In general, if one considers the general action of G on some set X, then the orbits X/G need not all have the same size, though they do partition the set. It is in the special case where X a group and G a subgroup of X that we can guarantee equal-sized partitions.

↪**Theorem 1.2** (Lagrange's): Let G be a finite group and H a subgroup. Then

$$\#G = \#H \cdot \#(G/H).$$

In particular, $\#H \mid \#G$ for any subgroup H.

Proof. We know that G/H is a partition of G, so eg $G = H \sqcup H_1 \sqcup \cdots \sqcup H_n$. By the previous theorem, each of these partitions are the same size, hence

$$\begin{aligned}\#G &= \#(H \sqcup H_1 \sqcup \cdots \sqcup H_n) \\ &= \#H + \#H_1 + \cdots + \#H_{n-1} \quad \text{since } H_i\text{'s disjoint} \\ &= n \cdot \#H \quad \text{since each } H \text{ same cardinality} \\ &= \#(G/H) \cdot \#H.\end{aligned}$$

■

↪**Proposition 1.4**: G/H has a natural left-action of G given by

$$G \times G/H \to G/H, \quad (g, aH) \mapsto (ga)H.$$

Further, this action is always transitive.

↪**Proposition 1.5**: If X is a transitive G-set, there exists a subgroup $H \subseteq G$ such that $X \cong G/H$ as a G-set.

In short, then, it suffices to consider coset spaces G/H to characterize G-sets.

Proof. Fix $x_0 \in X$, and define the *stabilizer* of x_0 by

$$H := \mathrm{Stab}_G(x_0) := \{g \in G : gx_0 = x_0\}.$$

One can verify H indeed a subgroup of G. Define now a function

$$f : G/H \to X, \quad gH \mapsto g \cdot x_0,$$

which we aim to show is an isomorphism of G-sets.

First, note that this is well-defined, i.e. independent of choice of coset representative. Let $gH = g'H$, that is $\exists\, h \in H$ s.t. $g = g'h$. Then,

$$f(gH) = gx_0 = (g'h)x_0 = g'(hx_0) = g'x_0 = f(g'H),$$

since h is in the stabilizer of x_0.

For surjectivity, we have that for any $y \in X$, there exists some $g \in G$ such that $gx_0 = y$, by transitivity of the group action on X. Hence,

$$f(gH) = gx_0 = y$$

and so f surjective.

For injectivity, we have that

$$\begin{aligned} g_1x_0 = g_2x_0 &\Rightarrow g_2^{-1}g_1x_0 = x_0 \\ &\Rightarrow g_2^{-1}g_1 \in H \\ &\Rightarrow g_2h = g_1 \text{ for some } h \in H \\ &\Rightarrow g_2H = g_1H, \end{aligned}$$

as required.

Finally, we have that for any coset aH and $g \in G$, that

$$f(g(aH)) = f((ga)H) = (ga)x_0,$$

and on the other hand

$$gf(aH) = g(ax_0) = (ga)x_0.$$

Note that we were very casual with the notation in these final two lines; make sure it is clear what each "multiplication" refers to, be it group action on X or actual group multiplication. ■

↪**Corollary 1.1**: If X is a transitive G set with G finite, then $\#X \mid \#G$. More precisely,

$$X \cong G/\mathrm{Stab}_G(x_0)$$

for any $x_0 \in X$. In particular, the *orbit-stabilizer formula* holds:

$$\#G = \#X \cdot \#\mathrm{Stab}_G(x_0).$$

The assignment $X \to H$ for subgroups H of G is not well-defined in general; given $x_1, x_2 \in X$, we ask how $\mathrm{Stab}_G(x_1)$, $\mathrm{Stab}_G(x_2)$ are related?

Since X transitive, then there must exist some $g \in G$ such that $x_2 = gx_1$. Let $h \in \mathrm{Stab}(x_2)$. Then,

$$hx_1 = x_2 \Rightarrow (hg)x_1 = gx_1 \Rightarrow g^{-1}hgx_1 = x_1,$$

hence $g^{-1}hg \in \mathrm{Stab}\ (x_1)$ for all $g \in G, h \in \mathrm{Stab}(x_2)$. So, putting $H_i = \mathrm{Stab}\ (x_i)$, we have that

$$H_2 = gH_1g^{-1}.$$

This induces natural bijections

$$\begin{aligned} \{\text{pointed transitive } G-\text{sets}\} &\leftrightarrow \{\text{subgroups of } G\} \\ (X, x_0) &\rightsquigarrow H = \mathrm{Stab}(x_0) \\ (G/H, H) &\rightsquigarrow H, \end{aligned}$$

and

$$\begin{aligned} \{\text{transitive } G-\text{sets}\} &\leftrightarrow \{\text{subgroups of } G\}/\text{ conjugation} \\ H_i &= gH_jg^{-1}, \text{some } g \in G. \end{aligned}$$

Given a G, then, we classify all transitive G-sets of a given size n, up to isomorphism, by classifying conjugacy classes of subgroups of "index n" $:= [G : H] = \frac{\#G}{n} = \#(G/H)$.

⊛ **Example 1.3**:

0. $G, \{e\}$ are always subgroups of any G, which give rise to the coset spaces $X = \{\star\}, G$ respectively. The first is "not faithful" (not injective into the group of permutations), and the second gives rise to an injection $G \hookrightarrow S_G$.
1. Let $G = S_n$. We can view $X = \{1, ..., n\}$ as a transitive S_n-set. We should be able to view X as G/H, where $\#(G/H) = \#X = n = \frac{\#G}{\#}(H) = \frac{n!}{\#H}$, i.e. we seek an $H \subset G$ such that $\#H = \frac{n!}{n} = (n-1)!$.

Moreover, we should have H as the stabilizer of some element $x_0 \in \{1, ..., n\}$; so, fixing for instance $1 \in \{1, ..., n\}$, we have $H = \mathrm{Stab}(1)$, i.e. the permutations of $\{1, ..., n\}$ that leave 1 fixed. But we can simply see this as the permutation group on $n-1$ elements, i.e. S_{n-1}, and thus $X \cong S_n/S_{n-1}$. Remark moreover that this works out with the required size of the subgroup, since $\#S_{n-1} = (n-1)!$.

2. Let $X =$ regular tetrahedron and consider

$$G = \mathrm{Aut}(X) := \{\text{rotations leaving } X \text{ globally invariant}\}.$$

We can easily compute the size of G without necessarily knowing G by utilizing the orbit-stabilizer theorem (and from there, somewhat easily deduce G). We can view the tetrahedron as the set $\{1, 2, 3, 4\}$, labeling the vertices, and so we must have

$$\#G = \#X \cdot \#\,\mathrm{Stab}(1),$$

where $\mathrm{Stab}(1) \cong \mathbb{Z}/3\mathbb{Z}$. Hence $\#G = 12$.

From here, there are several candidates for G; for instance, $\mathbb{Z}/12\mathbb{Z}$, D_{12}, A_4, ... Since X can be viewed as the set $\{1, 2, 3, 4\}$, we can view $X \twoheadrightarrow G \hookrightarrow S_4$, where $\hookrightarrow$ an injective homomorphism, that is, embed G as a subgroup S_4. We can show both D_{12} and $\mathbb{Z}/12\mathbb{Z}$ cannot be realized as such (by considering the order of elements in each; there exists an element in D_{12} of order 6, which does not exist in S_4, and there exists an element in $\mathbb{Z}/12\mathbb{Z}$ of order 12 which also doesn't exist in S_4). We can embed $A_4 \subset S_4$, and moreover $G \cong A_4$. If we were to extend G to include planar reflections as well that preserve X, then our G is actually isomorphic to all of S_4.

4. Let X be the cube, $G = \{\text{rotations of } X\}$. There are several ways we can view X as a transitive G sets; for instance $F =$ faces, $E =$ edges, $V =$ vertices, where $\#F = 6, \#E = 12, \#V = 8$. Let's work with F, being the smallest. Letting $x_0 \in F$, we have that $\mathrm{Stab}\,(x_0) \cong \mathbb{Z}/4\mathbb{Z}$ so the orbit-stabilizer theorem gives $\#G = 24$.

This seems to perhaps imply that $G = S_4$, since $\#S_4 = 24$. But this further implies that if this is the case, we should be able to consider some group of size 4 "in the cube" on which G acts.

§1.3 Homomorphisms, Isomorphisms, Kernels

↪**Proposition 1.6**: If $\varphi : G \to H$ a homomorphism, φ injective iff φ has a trivial kernel, that is, $\ker \varphi = \{a \in G : \varphi(a) = e_H\} = \{e\}$.

↪**Definition 1.8** (Normal subgroup): A subgroup $N \subset G$ is called *normal* if for all $g \in G, h \in N$, then $ghg^{-1} \in N$.

↪**Proposition 1.7**: The kernel of a group homomorphism $\varphi : G \to H$ is a normal subgroup of G.

↪**Proposition 1.8**: Let $N \subset G$ be a normal subgroup. Then $G/N = N \setminus G$ (that is, $gN = Ng$) and G/N a group under the rule $(g_1N)(g_2N) = (g_1g_2)N$.

↪**Theorem 1.3** (Fundamental Isomorphism Theorem): If $\varphi : G \to H$ a homomorphism with $N := \ker \varphi$, then φ induces an injective homomorphism $\overline{\varphi} : G/N \hookrightarrow H$ with $\overline{\varphi}(aN) := \varphi(a)$.

↪**Corollary 1.2**: $\mathrm{im}(\varphi) \cong G/N$, by $\overline{\varphi}$ into $\mathrm{im}(\overline{\varphi})$.

⊛ **Example 1.4**: We return to the cube example. Let $\tilde{G} = \widetilde{\mathrm{Aut}}(X) =$ rotations and reflections that leave X globally invariant. Clearly, $G \subset \tilde{G}$, so it must be that $\#\tilde{G}$ a multiple of 24. Moreover, remark that relfections reverse orientation, while rotations preserve it; this implies that the index of G in $\tilde{G}$ is 2. Hence, the action of $\tilde{G}$ on a set $O = \{\text{orientations on} \mathbb{R}^3\}$ with $\#O = 2$ is transitive. We then have the induced map

$$\eta : \tilde{G} \to \mathrm{Aut}(O) \cong \mathbb{Z}/2$$

with kernel given by all of G; G fixes orientations after all.

Remark now the existence of a particular element in $\tilde{G}$ that "reflects through the origin", swapping each corner that is joined by a diagonal. This is not in G, but notice that it actually commutes with every other element in $\tilde{G}$ (one can view such an element by the matrix $\begin{pmatrix} -1 & & \\ & -1 & \\ & & -1 \end{pmatrix}$ acting on $\mathbb{R}^3$). Call this element τ. Then, since $\tau \notin G$, $\tau g \neq g$ for any $g \in G$. Hence, we can write $\tilde{G} = G \sqcup \tau G$; that is, $\tilde{G}$ is a disjoint union of two copies of S_4, and so

$$\tilde{G} \cong S_4 \times \mathbb{Z}/2\mathbb{Z}$$

$$f : S_4 \times \mathbb{Z}/2\mathbb{Z} \to \tilde{G}, \quad (g, j) \mapsto \tau^j g.$$

§1.4 Conjugation and Conjugacy

↪**Definition 1.9**: Two elements $g_1, g_2 \in G$ are *conjugate* if $\exists\, h \in G$ such that $g_2 = hg_1h^{-1}$.

Recall that we can naturally define G as a G-set in three ways; by left multiplication, by right multiplication (with an extra inverse), and by conjugation. The first two are always transitive, while the last is never (outside of trivial cases); note that if $g^n = 1$, then $\left(hgh^{-1}\right)^n = 1$, that is, conjugation preserves order, hence G will preserve the order of 1 of the identity element, and conjugation will thus always have an orbit of size 1, $\{e\}$.

An orbit, in this case, is called a *conjugacy class*.

↪**Proposition 1.9**: Conjugation on S_n preserves cycle shape.

PROOF. Just to show an example, consider $(13)(245) \in S_5$ and let $g \in S_5$, and put $\sigma := g(13)(245)g^{-1}$. Then, we can consider what $\sigma g(k)$ is for each k;

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

hence, we simply have $\sigma = (g(1)g(3))(g(2)g(4)g(5))$, which has the same cycle shape as our original permutation. A similar logic holds for general cycles. ■

↪**Definition 1.10**: The cycle shape of $\sigma \in S_n$ is the partition of n by σ. For instance,

$$\begin{aligned}1 &\leftrightarrow 1+1+\ldots+1\\ \sigma = (12\ldots n) &\leftrightarrow n.\end{aligned}$$

⊛ **Example 1.5**: We compute all the "types" of elements in S_4 by consider different types of partitions of 4:

Partition	Size of Class
$1+1+1+1$	1
$2+1+1$	$\binom{4}{2} = 6$
$3+1$	$4 \cdot 2 = 8$ (4 points fixed, 2 possible orders)
4	$3! = 6$ (pick 1 first, then 3 choices, then 2)
$2+2$	3

The converse of ↪Proposition 1.9 actually holds as well:

↪**Theorem 1.4**: Two permutations in S_n are conjugate if and only if they induce the same cycle shape.

Proof. We need to show the converse, that if two permutations have the same cycle shape, then they are conjugate.

We show by example. Let $g = (123)(45)(6), g' = (615)(24)(3) \in S_6$. We can let $h \in S_6$ such that it sends $1 \mapsto 6, 2 \mapsto 1, 3 \mapsto 5$, etc; precisely

$$h = (163542).$$

Remark that h need not be unique! Indeed, we could rewrite $g' = (156)(42)(3)$ (which is the same permutation of course), but would result in

$$h = (1)(25)(36)(4),$$

which is not the same as the h above. ■

⊛ **Example 1.6**: We return to ⊛ Example 1.5, and recall that $S_4 \cong \mathrm{Aut}(\text{cube})$. Can we identify the conjugacy classes of S_4 with "classes" of symmetries in the cube?

Conjugation Class	#	**Cube Symmetry**
1	1	id
(12)	6	Rotations about edge diagonals
(12)(34)	3	Rotations about the face centers by π
(123)	8	Rotations about principal diagonals
(1234)	6	Rotations about the face centers by $\frac{\pi}{2}$

⊛ **Example 1.7**: Let $\mathbb{F}$ be a field and consider the vector space $V = \mathbb{F}^n$. Then

$$\mathrm{Aut}(V) = \mathrm{GL}_n(\mathbb{F}) = \{\text{invertible } n \times n \text{ matrices}\}.$$

Recall that linear transformations are described by matrices, after choosing a basis for V; i.e.

$$\{\text{linear transformations on } V\} \longleftrightarrow M_n(\mathbb{F}) := \{n \times n \text{ matrices with entries in } \mathbb{F}\}.$$

However, this identification *depends* on the choose of basis; picking a different basis induces a different bijection. Suppose we have two bases β, β', then $\beta' = P\beta$ for some $P \in \mathrm{GL}_n(\mathbb{F})$ (P called a "change of basis matrix"). Then for $T : V \to V$, and with $M := [T]_\beta, M' := [T]_{\beta'}$, then as discussed in linear algebra, $M' = PMP^{-1}$. Hence, understanding $M_n(\mathbb{F}) \leftrightarrow \mathrm{Hom}(V \to V)$ can be thought of as understanding $M_n(\mathbb{F})$ as a G-set of $G = \mathrm{GL}_n(\mathbb{F})$ under conjugation; then orbits $\leftrightarrow$ conjugacy classes.

Conjugacy Invariants

- The trace tr and determinant det are invariant under conjugation; $\mathrm{tr}\left(PMP^{-1}\right) = \mathrm{tr}(M)$ and $\det\left(PMP^{-1}\right) = \det(M)$
- spec (M) := set of eigenvalues is a conjugate invariant (with caveats on the field, etc)
- Characteristic polynomial, minimal polynomial

§1.5 The Sylow Theorems

Recall that if $H \subseteq G$ a subgroup, then Lagrange's gives us that $\#H \mid \#G$. We are interested in a (partial) converse; given some integer n such that $n \mid \#G$, is there a subgroup of cardinality n?

To see that this is not true in general, let $G = S_5$. $\#G = 120$; the divisors and the (if existing) subgroups:

$$\begin{aligned}
1 &\to \{1\} \\
2 &\to \{1, (12)\} \\
3 &\to \mathbb{Z}/3\mathbb{Z} \\
4 &\to \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\
5 &\to \mathbb{Z}/5\mathbb{Z} \\
6 &\to \langle (12)(345) \rangle \cong \mathbb{Z}/6\mathbb{Z}, S_3 \\
8 &\to D_8 \\
10 &\to D_{10} \\
12 &\to A_4 \\
15 &\to \text{None :(}
\end{aligned}$$

There is a unique group of order 15, $\mathbb{Z}/15\mathbb{Z}$; but this would need an element of order 15, which doesn't exist in S_5.

↪**Theorem 1.5** (Sylow 1): Fix a prime number p. If $\#G = p^t \cdot m$ with $p \nmid m$, then G has a subgroup of cardinality p^t.

We often call such a subgroup a *Sylow-p* subgroup of G.

⊛ **Example 1.8**: We consider the Sylow subgroups of several permutation groups.

(S_5) $\#S_5 = 120 = 2^3 \cdot 3 \cdot 5$, so by the Sylow theorem, S_5 contains subgroups of cardinality 8, 3, and 5.

(S_6) We have $\#S_6 = 720 = 2^4 \cdot 3^2 \cdot 5$, so by the Sylow theorem we have subgroups H of order $16, 9$, and 5.

$\#H = 9$ is given by

$$H = \langle (123), (456) \rangle := \left\{ (123)^i (456)^j : 0 \leq i, j \leq 2 \right\} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z},$$

or similarly for any other two disjoint cycles of three elements.

$\#H = 16$ is given by $H \cong D_8 \times S_2$.

(S_7) We have $\#S_7 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$. Subgroups of size $16, 9, 5$ can be simply realized as those from S_6, and of size 7 as just the cyclic subgroup generated by an element of order 7.

(S_8) We have $\#S_8 = 2^7 \cdot 3^2 \cdot 5 \cdot 7$ so we have subgroups of size $128, 9, 5, 7$. The latter 3 subgroups are easy to find; the first is found by

$$H \cong \langle (15)(26)(48)(37), D_8 \times D_8 \rangle,$$

where we can view the first copy of D_8 acting on a square labeled $1, 2, 3, 4$, the second acting on a square labeled $5, 6, 7, 8$, and the distinguished permutation swapping all the vertices ??

↪**Theorem 1.6**: Fix a group G and a prime p. TFAE:

1. There exists a G-set X of cardinality prime to p with no orbit of size 1.
2. There is a transitive G-set of cardinality > 1 and of cardinality prime to p.
3. G has a proper subgroup of index prime to p.

Proof. (1. $\Rightarrow$ 2.) We can write $X = X_1 \sqcup X_2 \sqcup \ldots \sqcup X_t$ where X_i the orbits of the action; note that the action of G on each X_i transitive. Since $p \nmid \#X$, then $\exists\, i$ for which $p \nmid \#X_i$. $\#X_i > 1$ necessarily, since X was assumed to have no orbit of size 1.

(2. $\Rightarrow$ 3.) We have $X \cong G/H$ for some subgroup H, where $H = \mathrm{Stab}_G(x_0)$ for some $x_0 \in X$. Moreover, $\#X = [G : H]$ hence $p \nmid [G : H]$.

(3 $\Rightarrow$ 1.) Given H, take $X = G/H$. Then G necessarily acts transitively on X so X has no orbit of size 1, and has cardinality $\#X = [G : H]$, so X also has cardinality prime to p as $[G : H]$ prime to p. ■

↪**Theorem 1.7**: For any finite group G and any prime $p \mid \#G$ with $\#G = p^t \cdot m$, $m \neq 1$, then (G, p) satisfies the properties of the previous theorem.

Proof. It suffices to prove 1. holds. Let

$$X = \{\text{all subsets of } G \text{ of size } p^t\}.$$

X a G-set; for any $A \in X$, gA also a set of size p^t hence $gA \in X$. Moreover, G acts on X without fixed points (why?). We have in addition

$$\#X = \binom{p^t \cdot m}{p^t} = \frac{(p^t m)(p^t m - 1)(\cdots)(p^t m - p^t + 1)}{(p^t)!} = \prod_{j=0}^{p^t-1} \left(\frac{p^t m - j}{p^t - j} \right).$$

The max power of p dividing $p^t m - j$ will be the same as the maximum power of p dividing j itself (since $p \mid p^t m$), and by the same logic the same power that divides $p^t - j$. That is, then, the max power of p that divides both numerator and denominator in each term of this product for each j, hence they will cancel identically in each term. Thus, $p \nmid \#X$ as desired.

■

Proof. (Of ↪Theorem 1.5) Fix a prime p and let G be a group of minimal cardinality for which the theorem fails for (G, p). By 3. of ↪Theorem 1.6, there exists a subgroup $H \subsetneq G$ such that $p \nmid [G : H]$. We have $\#G = p^t m$, and $\#H = p^t m'$; since $p \nmid \frac{\#G}{\#H} = \frac{p^t m}{p^t m'} = \frac{m}{m'}$.

Then, by our hypothesis H contains a subgroup N of cardinality p^t; N is also a subgroup of G and thus a Sylow-p subgroup of G, contradicting our hypothesis of minimality. ■

Proof. (A Second Proof of ↪Theorem 1.5) We may write

$$G = C_1 \sqcup C_2 \sqcup \cdots \sqcup C_h,$$

where $C_j = \{gag^{-1} : g \in G\}$. We must have (at least one) some C_j where $\#C_j = 1$, so $C_j = \{a\}$; it must be that a commutes with every $g \in G$. Consider the center of G,

$$Z(G) = \{a : ag = ga \; \forall \, g \in G\}.$$

Note that $Z(G)$ is a subgroup of G;

$$G = Z(G) \sqcup C_1 \sqcup \cdots \sqcup C_{h'},$$

where C_j are the conjugacy classes of size > 1 (all the conjugacy classes of size 1 are included in $Z(G)$). By the orbit-stabilizer theorem, the cardinality of each C_j divides the cardinality of G (and as $Z(G)$ a subgroup, so does the cardinality of $Z(G)$). We call this decomposition a "class equation of G".

With this setup, we assume again G is the smallest group for which the theorem fails for p. We consider the following cases:

Case 1: $p \nmid \#Z(G)$, then at least one C_j must be of cardinality prime to p (if all were divisible by p, then we'd have

$$\#G \underset{p}{\equiv} 0 \underset{p}{\equiv} (\text{not } 0) + 0 + \cdots + 0,$$

which is impossible). Then, $C_j \cong G/H$ for some subgroup H of G, with $\#H = p^t m' < \#G$, so by our assumption H has a Sylow p-subgroup, and thus so does G.

Case 2: $p \mid \#Z(G)$. $Z(G)$ an abelian subgroup, so there exists a subgroup $Z \subseteq Z(G)$ with $\#Z = p$ (why? For every abelian group with $p \mid \#Z(G)$, $Z(G)$ has an element of that order, hence take the cyclic subgroup generated by that element; see following lemma). Then, since Z is a normal subgroup, and we may consider $\overline{G} = G/Z$, which is then a group with cardinality

$$\#\overline{G} = \frac{\#G}{\#Z} = \frac{p^t m}{p} = p^{t-1} \cdot m < \#G,$$

so we may apply the induction hypothesis to $\overline{G}$, i.e. $\overline{G}$ has a Sylow p-subgroup $\overline{H}$ of cardinality p^{t-1}. We have a natural, surjective homomorphism

$$\pi : G \twoheadrightarrow \overline{G} \supseteq \overline{H}.$$

Take

$$H = \bigcup_{gZ \in \overline{H}} gZ,$$

or equivalently, $H = \pi^{-1}\left(\overline{H}\right)$. We have an induced surjective homomorphism

$$\pi : H \twoheadrightarrow \overline{H}$$

with $\ker(\pi) = Z$, so $\overline{H} \cong H/Z$, and thus $\#H = \#\overline{H} \cdot \#Z = p^t$, and thus H a Sylow p-subgroup of G. ■

↪**Lemma 1.1**: Let p be prime. If G a finite abelian group and $p \mid \#G$, then G has an element of order p, i.e. there is a subgroup $Z \subset G$ of cardinality p.

Proof. We can write $\#G = p \cdot m$. Remark that it suffices to find an element g of order t such that $p \mid t$; indeed, then the element $g^{\frac{t}{p}}$ has order p, which exists since then $\frac{t}{p}$ an integer.

Let $g_1, g_2, \ldots, g_t$ be a set of generators for G and put $n_j := \operatorname{ord}\left(g_j\right)$. Define now

$$\varphi : (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_t\mathbb{Z}) \to G,$$

$$(a_1, a_2, \ldots, a_t) \mapsto g_1^{a_1} g_2^{a_2} \cdots g_t^{a_t}.$$

One can show that this is a homomorphism; moreover, it is surjective, since any element in G can be written in terms of these generators. Hence, $\#G \mid \#(\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_t\mathbb{Z}) = n_1 n_2 \cdots n_t$. Since $p \mid \#G$, then it follows too that $p \mid n_1 n_2 \cdots n_t$

and thus there is some n_i such that $p \mid n_i$ ("Gauss's Lemma"). Hence, g_j has order divisible by p. ■

↪**Theorem 1.8** (Sylow 2): If H_1, H_2 are Sylow p-subgroups of G, then $\exists g \in G$ s.t. $gH_1g^{-1} = H_2$.

Proof. Consider G/H_1 as an H_2-set. We may write

$$G/H_1 = X_1 \sqcup X_2 \sqcup \cdots \sqcup X_N,$$

where the X_j's are disjoint orbits, then $\#X_j \mid \#H_2$, so $\#X_j = p^a$, some $a \leq t$. Then, there must be some orbit X_j of cardinality 1; since $p \mid \#X_j$, but $p \nmid G/H_1$, but each must be a power of p hence the power a of some cardinality must be 0. Then, we may write $X_j = \{gH_1\}$. This is fixed by every element in H_2, i.e. $\forall\, h \in H_2, hgH_1 = gH_1$ i.e.

$$(g^{-1}hg)H_1 = H_1,$$

i.e. $g^{-1}hg \in H_1$ for all $h \in H_2$, and thus $g^{-1}H_2g = H_1$. ■

↪**Theorem 1.9** (Sylow 3): The number N_p of distinct Sylow p-subgroups satisfies
1. $N_p \mid m$,
2. $N_p \underset{p}{\equiv} 1$,

where $\#G = p^t m$.

Proof.

1. Let $X = \{\text{all Sylow } p\text{-subgroups}\}$. By Sylow 2, G acts transitively on X by conjugation. Then, by the orbit-stabilizer theorem,

$$\#X = \frac{\#G}{\#N},$$

where N the *normalizer* of $H = \{g \in G : gHg^{-1} = H\}$. We know that $H \subset N$, hence $p^t = \#H \mid \#N$, so $\#X \mid \frac{\#G}{\#H} = m$ and so $\#X \mid m$.

2. Let H be a Sylow p-subgroup and let X be the set of all Sylow p-subgroups as above, viewed as a G-set by conjugation. Again, this is a transitive action. We can also view X as an H-set. Then,

$$X = X_1 \sqcup \cdots \sqcup X_a,$$

where

$$\#X_j \mid \#H = p^t,$$

i.e. $\#X_j = 1, p, p^2, \ldots, p^t$. We claim there is exactly one X_j of size 1. Let $X_j = \{H'\}$ be an orbit of size 1 (remarking that there exists at least one, namely just H itself.) Then, we must have $aH'a^{-1} = H'$ for all $a \in H$. Then, H is contained in the normalizer of H', N,

$$H \subset N = \left\{a \in G : aH'a^{-1} = H'\right\}.$$

$H' \subset N$, but moreover, H' a normal subgroup of N. Then,

$$p \nmid \#(N/H').$$

We have the natural map

$$\varphi : N \to N/H',$$

and we consider $\varphi(H)$; its cardinality must be 1, since it must simultaneously divide p^t and something prime to p. Thus, $H \subset \ker(\varphi) = H'$. But $\#H = \#H'$, and thus $H = H'$. Hence, there is a unique orbit of size 1, just H itself.

Thus, the cardinality of X will be, modulo p, 1. ■

1.5.1 Illustrations of the Sylow Theorems

1. $G = S_4$; $\#G = 2^3 \cdot 3$. The Sylow 8-subgroup is D_8,

$$\{1, (1234), (13)(24), (1432), (12)(34), (14)(23), (13), (24)\}.$$

N_2 must divide 3 and must equal 1 modulo 2, so $N_2 = 1$ or 3. In this case, $N_2 = 3$ indeed; D_8 is not normal in S_4, which it would have to be if $N_2 = 1$. Inside S_4, we also have the "Klein group"

$$V = \{1, (12)(34), (13)(24), (14)(23)\},$$

which is normal in S_4. The resulting quotient

$$S_4/V$$

is then a group of cardinality 6, isomorphic to S_3. Consider the homomorphism

$$\varphi : S_4 \to S_3.$$

S_3 has 3 elements of order 2, $(ab), (ac), (bc)$ which generate subgroups of order 2. If A one of these subgroups of order 2, then $\varphi^{-1}(A)$ is a Sylow 2-subgroup.

2.

↪**Theorem 1.10**: Let p, q be primes with $p < q$, $p \nmid q - 1$. If G is a group of cardinality $p \cdot q$, then $G \cong \mathbb{Z}/pq\mathbb{Z}$.

What if $p \mid q - 1$? Consider, for instance, $p = 2, q = 3$, then S_3 has cardinality $p \cdot q$. More generally, suppose $p = 2$ and q any odd prime. Then $p \mid q - 1$ always, and we may consider D_{2q}.

For $p \neq 2$, consider the field $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$, and let

$$G = \left\{T_{a,b} : \mathbb{F}_q \to \mathbb{F}_q, T_{a,b}(x) := ax + b : a \in \mathbb{F}_q^\times, b \in \mathbb{F}_q\right\}$$

be the group of affine-linear transformations on the field. We have that $\#G = (q-1)q$ ($q-1$ choices for a, q choices for b), and that G *not* abelian;

$$\left(T_{a_1,b_1} \circ T_{a_2,b_2}\right)(x) = a_1(a_2x + b_2) + b_1 = a_1a_2x + a_2b_2 + b_1 = T_{a_1a_2,a_2b_2+b_1}(x) \neq \left(T_{a_2,b_2} \circ T_{a_1,b_1}\right)(x).$$

There exists a subgroup $H \subset \mathbb{F}_q^\times$ with $\#H = p$, since $\mathbb{F}_q^\times$ abelian and $p \mid \#\mathbb{F}_q^\times = q-1$, so we may consider the subgroup of G given by

$$G_{pq} = \left\{T_{a,b} : \mathbb{F}_q \to \mathbb{F}_q : a \in H, b \in \mathbb{F}_q\right\} \subset G,$$

with $\#G_{pq} = p \cdot q$. Let us consider the Sylow subgroups of G_{pq}.

A Sylow p-subgroup can be given by $P := \{T_{a,0} : a \in H\}$, and a Sylow q-subgroup can be given by $\left\{T_{1,b} : b \in \mathbb{F}_q\right\}$. Let N_p, N_q the number of Sylow p-, q-subgroups. By Sylow 3, we know that $N_p \underset{p}{\equiv} 1$ and $N_p \mid q$, hence it must be that $N_p = 1$ *or* q. Similarly, $N_q \underset{q}{\equiv} 1$ and $N_q \mid p$, so it must be that $N_q = 1$ so the Sylow q-subgroup we found is unique, and moreover normal.

Remark that the map

$$T_{a,b} \mapsto a, \qquad G \to \mathbb{F}_q^\times \text{ and } G_{pq} \to H$$

is a homomorphism.

To further investigate if $N_p = 1$ or q, we can see how P behaves under conjugation; if it is normal, then it is unique and so $N_p = 1$, else if we can find any second conjugate subgroup then it must be that $N_p = q$. Consider

$$\left(T_{1,1} \circ T_{a,0} \circ T_{1,-1}\right)(x) = a(x-1) + 1 = ax - a + 1 = T_{a,-a+1}(x) \notin P \text{ if } a = 1,$$

hence P not normal and thus $N_p = q$.

§1.6 Burnside's Counting Lemma

↪**Definition 1.11** (Fixed Point Set): Let G a finite group and X a finite G-set. Given $g \in G$, we denote

$$X^g := \{x \in X \mid gx = x\}.$$

the *fixed-point set* of g, and

$$\mathrm{FP}_X(g) := \#X^g.$$

⊛ **Example 1.9**: If $G = S_4$ acting on $X = \{1,2,3,4\}$, then for instance

$$\mathrm{FP}_X((12)) = 2, \mathrm{FP}_X((12)(34)) = 0.$$

↪**Proposition 1.10**: $\mathrm{FP}_X\left(hgh^{-1}\right) = \mathrm{FP}_X(g)$; we say FP_X a *class function* on G, being constant on conjugacy classes.

Proof. Define $X^g \to X^{hgh^{-1}}$ by $x \mapsto hx$, noting $hgh^1hx = x$ for $x \in X^g$; this is a bijection. ■

↪**Theorem 1.11** (Burnside):

$$\frac{1}{\#G}\sum_{g\in G}\mathrm{FP}_X(g) = \#(X/G) = \#G - \text{orbits on } X.$$

Proof. Let $\Sigma \subseteq G \times X$ such that

$$\Sigma = \{(g,x) : gx = x\}.$$

We will count $\#\Sigma$ in two different ways, by noting that we can "project" Σ either to G or X on the first or second coordinate, respectively. On the one hand (the "G view"), we have

$$\#\Sigma = \sum_{g\in G}\mathrm{FP}_X(g),$$

and on the other (the "X view")

$$\#\Sigma = \sum_{x\in X}\#\mathrm{Stab}_G(x) = \sum_{O\in X/G}\sum_{x\in O}\#\mathrm{Stab}_G(x).$$

The orbit-stabilizer theorem gives us that for any $x \in O$, $\#\mathrm{Stab}_G(x)\cdot\#O = \#G$, hence further

$$\#\Sigma = \sum_{O\in X/G}\sum_{x\in O}\frac{\#G}{\#O} = \sum_{O\in X/G}\#G,$$

where the simplification in the final equality comes from the fact that we remove dependence on x in the inner summation, and we are just summing a constant $\#O$ times. Hence,

$$\#\Sigma = \#(X/G)\cdot\#G,$$

and so bringing in our original computation ("G view"),

$$\sum_{g\in G}\mathrm{FP}_X(g) = \#(X/G)\cdot\#G \Rightarrow \frac{1}{\#G}\sum_{g\in G}\mathrm{FP}_X(g) = \#(X/G),$$

completing the proof. ■

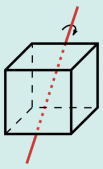
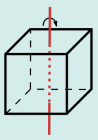
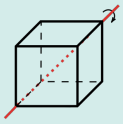
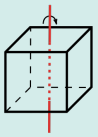
↪**Corollary 1.3**: If X is a transitive G-set with $\#X > 1$, then $\exists g \in G$ such that $\mathrm{FP}_X(g) = 0$.

Proof. By Burnside's,

$$\frac{1}{\#G}\sum_{g\in G}\mathrm{FP}_X(g) = 1,$$

but we have that $\mathrm{FP}_X(1) = \#X > 1$ since 1 fixes everything, so there must be at least a g such that $\mathrm{FP}_X(g) = 0$. ■

⊛ **Example 1.10** (Application of Burnside's): Let $G = S_4 = \mathrm{Aut}(\text{cube})$. We can realize several different (transitive) G-sets; for instance $X = \{1,2,3,4\}, F = \{\text{faces}\}, E = \{\text{edges}\}, V = \{\text{vertices}\}$. We can compute the number of fixed points $\mathrm{FP}_X(g)$ of different elements of G on these G-sets. Recall that it suffices to check one element per conjugacy class of G.

Conj. Class	#	X	F	E	V	**Geometric Desc.**	
id	1	4	6	12	8	id	
(12)	6	2	0	2	0	Rotations about "edge diagonals"	
(12)(34)	3	0	2	0	0	Rotations about "face diagonals", π	
(123)	8	1	0	0	2	Rotations about "principal diagonals"	
(1234)	6	0	2	0	0	Rotations about "face diagonals", $\pi/2$	
$\frac{1}{\#G}\sum \mathrm{FP}_{"X"}(g)$:		1	1	1	1		

The number of orbits, hence, in each case is 1, as we already knew since G acts transitively on all of these sets.

Remark that for two G-sets X_1, X_2, $\mathrm{FP}_{X_1 \times X_2}(g) = \mathrm{FP}_{X_1}(g) \cdot \mathrm{FP}_{X_2}(g)$, where the action of G on $X_1 \times X_2$ defined by $g(x_1, x_2) = (gx_1, gx_2)$. Using this we can consider actions on "pairs" of elements;

Conj. Class	$F \times F$	$F \times V$	$V \times V$
id	36	48	64
(12)	0	0	0
(12)(34)	4	0	0
(123)	0	0	4
(1234)	4	0	0
$\frac{1}{\#G}\sum \mathrm{FP}_{"X"}(g)$:	3	2	4

↪**Definition 1.12** (Colorings of a G-set): Let $C := \{1, 2, \ldots, t\}$ be a set of "colors". A coloring of X by C is a function $X \to C$. The set of all such functions is denoted C^X. Then, G acts on C^X naturally by

$$G \times C^X \to C^X, \qquad (g, f) \mapsto gf : X \to C, \qquad gf(x) := f\left(g^{-1}x\right).$$

⊛ **Example 1.11**: How many ways may we color the *faces* of a cube with t colors? There are 6 faces with t choices per face, so t^6 faces. More interestingly, how many *distinct* ways are there, up to an automorphism (symmetry) of the cube? G acts on F, and hence on the set of "t-colorings". Let F again be the set of faces and $X := C^F$. Then,

$$\#X = t^6.$$

We would like to calculate the number of orbits of G acting on X, namely $\#(X/G)$. We compute the number of fixed points for each conjugacy class of G; in general, $\#\left(C^F\right)^g = t^{\#(F/\langle g\rangle)} = t^{\#\text{ orbits of } <g> \text{ on } F}$. $(g \leftrightarrow (abc)(de)(f)(g)$ for each element a, say, we have t choices for the coloring of a. Then b, c must be the same color. This repeats for each transposition. etc

C	#	F	Shape	X
id	1	6	1^6	t^6
(12)	6	0	$(ab)(cd)(ef)$	t^3
(12)(34)	3	2	$(ab)(cd)$	t^4
(123)	8	0	$(abc)(def)$	t^2
(1234)	6	2	$(abcd)$	t^3

By Burnside's then,

$$\begin{aligned}\#\left(C^F/G\right) &= \frac{1}{24}\sum_{g\in G}\mathrm{FP}_{C^F}(g)\\ &= \frac{1}{24}\left(t^6 + 6t^3 + 3t^4 + 8t^2 + 6t^3\right)\\ &= \frac{1}{24}\left(t^6 + 3t^4 + 12t^3 + 8t^2\right).\end{aligned}$$

Remark that this polynomial does not have integer coefficients, but indeed must have integer outputs for integer t's. This is not obvious.

⊛ **Example 1.12**: We consider the fixed points of S_5 acting on various sets, in particular the quotient space S_5/F_{20}, where F_{20} the *Frobenius group* of affine linear transformations $\sigma : x \mapsto ax + b, a \in \mathbb{F}_5^\times, b \in \mathbb{F}_5$. The possible orders of elements $\sigma \in F_{20} \subset S_5$ are

$$1 \leftrightarrow 1^5, 5 \leftrightarrow (01234), 4 \leftrightarrow (1243), 2 \leftrightarrow (14)(23).$$

In particular, each (non-identity) permutation has *at most* one fixed point. Remark that to find the cycle shape when acting on S_5/F_{20}, it suffices to check if the permutation given is conjugate to an element in F_{20}, since $(12)gF_{20} = gF_{20} \Leftrightarrow g^{-1}(12)g \in F_{20}$.

C	#	$\{1,2,3,4,5\}$	$\{1,2,3,4,5,6\}$	S_5/F_{20}	Shape on S_5/F_{20}
id	1	5	6	6	$()$
(12)	10	3	4	0	$(ab)(cd)(ef)$
$(12)(34)$	15	1	2	2	$(ab)(cd)$
(123)	20	2	3	0	$(abc)(def)$
(1234)	30	1	2	2	$(abcd)$
(12345)	24	0	1	1	$(abcde)$
$(123)(45)$	20	0	1	0	$(abcdef)$

Hence, the list of elements in the right-most column is precisely the cycle shapes of elements in the "exotic" $S_5 \subset S_6$, not conjugate to the typical inclusion $S_5 \hookrightarrow S_6$.

§2 Rings and Fields

Groups are to symmetries as rings are to numbers.

§2.1 Definitions

↪**Definition 2.1** (Ring): A *ring* is a set R endowed with two operations, $+, \times : R \times R \to R$ satisfying

- (*addition*) $(R, +)$ is an abelian group, with neutral element 0_R and (additive) inverses of $a \in R$ denoted $-a$;
- (*multiplication*) $(R, \times)$ is a *monoid* i.e. it has a neutral element 1_R and is associative;
- (*distribution 1*) $a \times (b + c) = a \times b + a \times c$ for all $a, b, c \in R$;
- (*distribution 2*) $(b + c) \times a = b \times a + c \times a$ for all $a, b, c \in R$.

Remark 2.1:

1. Conventions differ; some texts do not require 1, and call such objects with one a "ring with unity".
2. We will blanketly assume $1 \neq 0$, else R is trivial.
3. 0 is never invertible; $1 \times a = (0+1) \times a = 0 \times a + 1 \times a \Rightarrow 0 \times a = 0$ for any $a \in \mathbb{R}$, so in particular there is no a such that $0 \times a = 1$.
4. Exercise: show $(-a) \times (-b) = a \times b$.

⊛ **Example 2.1** (Examples of Rings):

1. $\mathbb{Z}$
2. $\mathbb{Q}$ (essentially $\mathbb{Z}$ appending inverses)
3. Completions of $\mathbb{Q}$; taking $\{\text{Cauchy Sequences}\}/\{\text{Null Sequences}\} = \mathbb{R}$ under the standard distance $d(x,y) = |x-y|$. Alternatively, let p be a prime and take the p-adic metric $|x - y|_p := p^{-\text{ord}_p(x-y)}$ on $\mathbb{Q}$, and consider the completion with respect to $|\cdot|_p$, denoted $\mathbb{Q}_p$, called the *field of p-adic numbers*.
4. $\mathbb{C} := \mathbb{R}[i] = \{a + bi : a, b \in \mathbb{R}\}$
5. Polynomial rings; given a ring R, we may define $R[x] := \{a_0 + a_1 x + \cdots + a_n x^n : a_i \in R\}$ where x a "formal" indeterminate variable.
6. The *Hamilton quaternions*, $\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$, where $i^2 = j^2 = k^2 = -1$ and $ij = -ji = k, jk = -kj = i, ik = -ki = -j$.
7. For any commutative ring R, $M_n(R) = n \times n$ matrices with entries in R is a ring. In particular, associativity of multiplication in $M_n(R)$ follows from the identification of matrices with R-linear functions $R^n \to R^n$ and the fact that function composition is associative.
8. Given a ring R, we can canonically associate two groups, $(R, +, 0)$ ("forgetting" multiplication) and $(R^\times, \times, 1)$ ("forgetting" addition and restricting to elements with inverses, i.e. *units*).
9. If G is any finite group and R a ring, we may consider $R[G] = \left\{\sum_{g \in G} a_g g : a_g \in R\right\}$, a *group ring*. Addition is defined component-wise, and multiplication

$$\left(\sum_{g \in G} a_g g\right)\left(\sum_{h \in H} b_h h\right) = \sum_{g,h \in G} a_g b_h \cdot gh = \sum_{g \in G}\left(\sum_{h_1 \cdot h_2 = h \in G} a_{h_1} b_{h_2}\right) g.$$

§2.2 Homomorphisms

↪**Definition 2.2** (Homomorphism of Rings): A *homomorphism* from a ring R_1 to a ring R_2 is a map $\varphi : R_1 \to R_2$ satisfying:

- $\varphi(a+b) = \varphi(a) + \varphi(b)$ for all $a, b \in R_1$ (that is, φ a group homomorphism of the additive groups $(R_1, +)$, $(R_2, +)$)
- $\varphi(ab) = \varphi(a)\varphi(b)$
- $\varphi\left(1_{R_1}\right) = \varphi\left(1_{R_2}\right)$

↪**Definition 2.3** (Kernel): The *kernel* of a ring homomorphism φ is the kernel as a homomorphism of additive groups, namely

$$\ker(\varphi) = \left\{a \in R_1 : \varphi(a) = 0_{R_2}\right\}.$$

↪**Definition 2.4** (Ideal): A subset $I \subseteq R$ is an *ideal* of R if

1. I an additive subgroup of $(R, +)$, in particular $0 \in I$, I closed under addition and additive inverses
2. I closed under multiplication by elements in R, i.e. for all $a \in R, b \in I$, $ab \in I$ *and* $ba \in I$ (the second condition only being necessary when R non-commutative.)

↪**Proposition 2.1**: If φ is a ring homomorphism, then $\ker(\varphi)$ is an ideal of R_1.

Proof. The first requirement follows from the fact that φ an additive group homomorphism. For the second, let $a \in R_1, b \in \ker(\varphi)$, then $\varphi(ab) = \varphi(a)\varphi(b) = \varphi(a) \cdot 0 = 0$ so $ab \in \ker(\varphi)$. ■

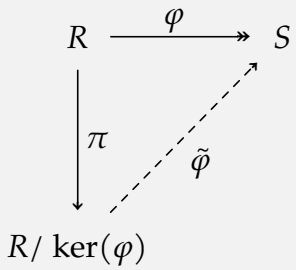
↪**Proposition 2.2**: If I an ideal of R_1, then there exists a ring R_2 and a ring homomorphism $\varphi : R_1 \to R_2$ such that $I = \ker(\varphi)$.

Proof. Let $R_2 = R_1/I = \{a + I : a \in R_1\}$ be the quotient group of R_1 additively. We can define multiplication by $(a + I)(b + I) := ab + I$. One may verify this indeed makes R_2 a ring. Then take φ to be the quotient map

$$\varphi : R_1 \to R_2, \qquad a \mapsto a + I.$$

Then, this is indeed a (surjective) ring homomorphism, with $\ker(\varphi) = I$. ■

↪**Theorem 2.1** (Isomorphism Theorem): Let R be a ring (group) and φ be a surjective homomorphism of rings (groups) $\varphi : R \twoheadrightarrow S$. Then, S is isomorphic to $R/\ker(\varphi)$.



Proof. Define

$$\tilde{\varphi} : R/\ker(\varphi) \to S, \qquad a + \ker(\varphi) \mapsto \varphi(a).$$

One can verify this indeed an isomorphism. ■

§2.3 Maximal and Prime Ideals

↪**Definition 2.5** (Maximal): An ideal $I \subseteq R$ is *maximal* if it is not properly contained in any proper ideal of R, namely if $I \subsetneq I'$ for any other ideal I', then $I' = R$.

↪**Definition 2.6** (Prime): An ideal $I \subseteq R$ is *prime* if $ab \in I$, then a or b in I.

⊛ **Example 2.2**: Let $R = \mathbb{Z}$ and $I = (n) = n\mathbb{Z} = \{na : a \in \mathbb{Z}\}$ for some $n \in \mathbb{N}$. We claim (n) is prime iff n is prime. If n prime, then if $ab \in I$, then $n \mid ab$. By Gauss's Lemma, then n divides at least one of a or b, and hence either a or b in I. Conversely, if n not prime, then we may write $n = ab$ where $|a|, |b| < n$. Then, $a, b \in I$, but n divides neither and so $a, b \notin I$.

↪**Theorem 2.2**: If $I \subseteq \mathbb{Z}$ an ideal, then there exists $n \in \mathbb{Z}$ such that $I = (n)$.

Proof. Consider $\mathbb{Z}/I$. As an abelian group, it is cyclic, generated by $1 + I$. Let $n = \#(\mathbb{Z}/I) = \text{ord}(1 + I)$. If $n = \infty$, then $\mathbb{Z} \to \mathbb{Z}/I$ is injective and $I = (0)$. Else, $I = (n)$.

Alternatively, assume that $I \neq (0)$. Let $n = \min\{a \in I : a > 0\}$. Let $a \in I$, then we may write $a = q \cdot n + r$ where $0 \leq r < n$. $a \in I$ by assumption as is n, and thus so must be $qn \in I$. Hence, $a - qn = r \in I$, and so $r = 0$, by assumption on the minimality of n. ■

↪**Definition 2.7** (Principal Ideal): An ideal of a ring R which is of the form $aR = (a)$ is called *principal*. A ring in which every ideal is of this type is called a *principal ideal ring*.

⊛ **Example 2.3**: $\mathbb{Z}$ is a principal ideal ring. Another example is $R = \mathbb{F}[x]$ where $\mathbb{F}$ a field.

↪**Theorem 2.3**: If I an ideal of $\mathbb{F}[x]$, then I is a principal ideal.

Proof. Let $f(x) \in I$ non-zero and of minimal degree, which necessarily exists if $I \neq (0)$. Put $d := \deg f$. If $g(x) \in I$, then $g(x) = f(x)q(x) + r(x)$ where $\deg r < d$. Then, we have that $r \in I$, so by minimality of d it must be that $r = 0$. ■

Remark 2.2: We conventionally take $\deg(0) = -\infty$ for the sake of the formula $\deg(fg) = \deg f + \deg g$ and taking $-\infty + k = 0$ for any k.

⊛ **Example 2.4**: Consider $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Let $I \subseteq \mathbb{Z}/n\mathbb{Z}$ and consider $\varphi^{-1}(I)$; this is an ideal of $\mathbb{Z}$ and so is principal ie $\varphi^{-1}(I) = (a)$ for some $a \in \mathbb{Z}$. Then, $I = (a + n\mathbb{Z}) \subseteq \mathbb{Z}/n\mathbb{Z}$.

⊛ **Example 2.5**: Let $R = \mathbb{Z}[x] = \{a_n x^n + \cdots + a_1 x + a_0 : a_i \in \mathbb{Z}\}$. Take $I = \{f(x) : f(0) \text{ even}\} \subsetneq \mathbb{Z}[x]$. We claim this an ideal. The subgroup property is clear. If $f(x) \in \mathbb{Z}[x]$ and $g(x) \in I$, then $f(0)g(0) =$ some integer $\cdot$ even integer $=$ even. Elements of I include 2, x, ... any polynomial with a_0 even. If I were principal, then there must exist some element in R dividing both 2 and x; the only possibilities are 1 and -1. This would imply, then, that $I = R$, which is not possible and so I not principal. We may say, however, that I is generated by 2 elements, $I = (2, x) = 2\mathbb{Z}[x] + x\mathbb{Z}[x]$.

⊛ **Example 2.6**: Let $R = \mathbb{F}[x, y]$. Consider $(x, y) = Rx + Ry = \{f : f(0, 0) = 0\}$ with typical element $xf(x, y) + yg(x, y)$; these will not have constant terms.

↪**Proposition 2.3**: I is a prime ideal of R iff R/I has no zero divisors (namely an element $x \neq 0$ such that $xy = 0$ for some $y \neq 0$); such a ring is called an *integral domain*.

Proof. Given $a + I, b + I \in R/I$, $(a + I)(b + I) = 0 \Rightarrow ab + I = 0 \Rightarrow ab \in I$. By primality of I, then at least one of $a, b \in I$, so at least one of $a + I, b + I = 0$. ■

Remark 2.3: If R an integral domain, then it satisfies the "cancellation law", namely $\forall\, a \neq 0, ax = ay \Rightarrow x = y$, since we may write $a(x - y) = 0$ hence it must be $x - y = 0 \Rightarrow x = y$.

↪**Theorem 2.4**: I is a maximal ideal $\Leftrightarrow$ R/I is a field.

Proof. ($\Rightarrow$) Let $a+I \in R/I$. If $a+I \neq 0$, then consider the ideal $Ra+I \supsetneq I$. By maximality of I, it must be that $Ra+I=R$. So, anything in R can be written as a "multiple" of a plus an element of I, so in particular $1 \in R$ may be written $1=ba+i$ for some $i \in I, b \in R$. Passing to the quotient, we find

$$1+I=(b+I)(a+I) \Rightarrow b+I=(a+I)^{-1} \in R/I,$$

so we indeed have multiplicative inverses.
($\Leftarrow$) Given $J \supsetneq I$, let $a \in J-I$. Then, $a+I \neq 0 \in R/I$, so there exists a b such that $ba+I=1+I$ since R/I a field, and hence $1 \in J$ so $J=R$ and thus I maximal. ■

§2.4 Quotients

⊛ **Example 2.7**: Let $R=\mathbb{Z}, I=(n)$, and consider

$$\begin{aligned} R/I=\mathbb{Z}/n\mathbb{Z} &= \{a+n\mathbb{Z} : a+\mathbb{Z}\} \\ &= \{0,1,2,\ldots,n-1\} \,(\mathrm{mod}\, n). \end{aligned}$$

Let $R=\mathbb{F}[x], I=(f(x))$, and consider

$$\begin{aligned} R/I=\mathbb{F}[x]/(f(x)) &= \{p(x)+f(x)\mathbb{F}[x]\} \\ &= \{p(x) : \deg p \leq d-1 \text{ where } d \coloneqq \deg f\}. \end{aligned}$$

Remark 2.4: In $R/I, a+I=b+I \leftrightarrow a-b \in I$. If $I=(d)$ principal, then $a+I=b+I \Leftrightarrow d \mid b-a$. For more general quotients (namely, more general ideals) this is a more difficult question.

⊛ **Example 2.8**: Let $R=\mathbb{Z}[x], I=(2,x)=\{f(x) : f(0) \text{ even}\}$, then $\mathbb{Z}[x]/I$ has precisely two elements, and indeed is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. To see this, consider the map

$$\varphi : \mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}, \qquad f(x) \mapsto f(0) \bmod 2,$$

a surjective homomorphism, with

$$\ker(\varphi)=\left\{f(x) : f(0) \underset{2}{\equiv} 0\right\}=\{f(x) : f(0) \text{ even}\}=I,$$

so by the isomorphism theorem, $\mathbb{Z}[x]/\ker(\varphi) \cong \mathrm{im}(\varphi) \Rightarrow \mathbb{Z}[x]/I \cong \mathbb{Z}/2\mathbb{Z}$.

⊛ **Example 2.9**: Let $R=\mathbb{F}[x,y]=\left\{\sum_{i,j=1}^{N} a_{i,j}x^iy^j : a_{i,j} \in \mathbb{F}\right\}$ and $I=(x,y)=\{f(x,y) : f(0,0)=0\}$. Then, $R/I \cong \mathbb{F}$ by the map $f(x,y)+I \mapsto f(0,0)$.

⊛ **Example 2.10**: Let $R = \mathbb{F}[x_1, ..., x_n]$ and $I = (f_1, ..., f_t)$, for $f_j(x_1, ..., x_n) \in R$. Then, consider R/I; this is hard. Let

$$V(I) := \{(x_1, ..., x_n) : f_i(x_1, ..., x_n) = 0 \text{ for all } i = 1, ..., t\}.$$

Then, we may identify $R/I \to$ functions on $V(I)$.

§2.5 Adjunction of Elements

↪**Theorem 2.5**: Given a ring R and $p(x) \in R[x]$, there exists a ring S containing both R and a root of $p(x)$.

Proof. Let $S = R[x]/(p(x))$, $R \to S$ by $a \mapsto a + (p(x))$. Let $\alpha = x + (p(x))$; then $p(\alpha) = p(x) + (p(x)) = 0 + (p(x))$. ■

⊛ **Example 2.11**: Let $R = \mathbb{R}$ and $p(x) = x^2 + 1$. Then, $\mathbb{R}[x]/\left(x^2 + 1\right) = \mathbb{C}$.