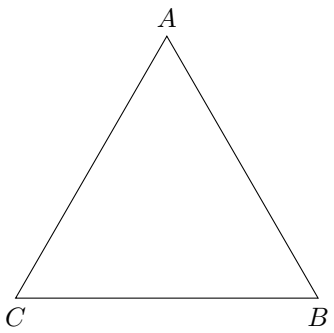
MAT347 Abstract Algebra

Jonah Chen

1 Groups

Groups are generally associated with symmetries. Consider the equilateral triangle:



We know that there are six symmetries of the triangle:

- Identity transformation (do nothing) denoted as id or e
- Two rotations ($A \to B \to C \to A$ and $A \to C \to B \to A$)
- Three reflections $A \leftrightarrow B$, $A \leftrightarrow C$, $B \leftrightarrow C$

Note that these symmetries preserve the structure of the triangle, hence the composition of two symmetries must also be a symmetry. Let

- ρ be the rotation $A \to B \to C \to A$
- σ be the reflections $B \leftrightarrow C$

Note that $\rho\sigma$ is the $A \leftrightarrow C$ reflection and $\sigma\rho$ is the $A \leftrightarrow B$ reflection. Hence they may not be commutative.

We also know that all symmetries can be reversed. α has an inverse α^{-1} such that $\alpha\alpha^{-1} = \alpha^{-1}\alpha = e$. These inspires the following definition:

Definition–: A **group** is a set G with a composition

$$G \times G \to G \tag{1}$$
$$(g, h) \mapsto g \cdot h \tag{2}$$

Satisfying:

- Associativity: $(g \cdot h) \cdot k = g \cdot (h \cdot k)$

- Identity: $\exists\, e \in G$ such that $g \cdot e = e \cdot g = g$ for all $g \in G$
- Inverse: $\forall\, g \in G$, $\exists\, g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$

Examples:

- $\mathbb{Z}$ with $+$ is a group. It is associative, $e = 0$ and $g^{-1} = -g$.
- $\mathbb{Z}/n\mathbb{Z}$ with addition modulo n.
- If F is a field, it implicitly has two group structures:
  - Additive group: $(F, +)$ is a group. It is associative, $e = 0$ and $g^{-1} = -g$.
  - Multiplicative group: $(F \setminus \{0\}, \times)$ is a group. It is associative, $e = 1$ and $g^{-1} = 1/g$.
- $GL(n, F)$ – "general linear group" contains all invertiable $n \times n$ matrices.
- $SL(n, F)$ – "special linear group" contains all invertiable $n \times n$ matrices with determinant 1.
- $SO(n, F)$ – "special orthogonal group" $= \{A \in SL(n, F) | A^t = A^{-1}\}$.

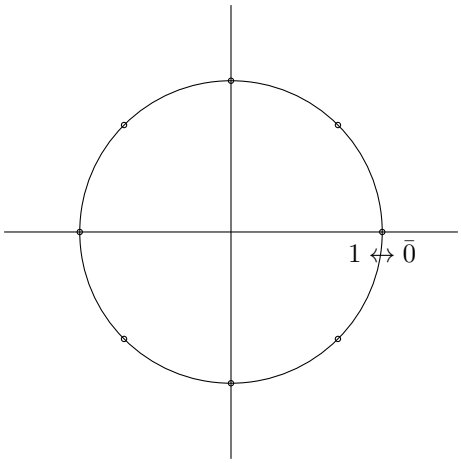
1.1 Cyclic Groups

One of the simplest groups is $\mathbb{Z}/n\mathbb{Z}$ for $n \in \mathbb{N}$ with the operation addition modulo n. This is known as the "cyclic group of order n" or C_n. i.e. for $n = 8$, $5 + 7 = 4 \pmod 8$, which we denote $\bar{5} + \bar{7} = \bar{4}$.

We know the inverse $\bar{k}^{-1} = \overline{n - k}$ for nonzero k or $\bar{0}^{-1} = \bar{0}$.

Another way to express the cyclic group is $\bar{k} \leftrightarrow e^{2\pi i k/n}$ with multiplication operation. Then,

$$\overline{k + n} = e^{2\pi i(k+n)/n} = e^{2\pi i k/n} e^{2\pi i n/n} = e^{2\pi i k/n} = \bar{k}. \tag{3}$$



Definition–Order: The **order** of a group G is its cardinality denoted $\mathrm{ord}(G)$ or $|G|$. It could be a finite or infinite ordinal. In particular, $|C_n| = n$.

1.2 Quaternion Group

The quaternion group $\mathbb{H} = \{\pm 1, \pm i, \pm j, \pm k\}$ is a group of order 8 with the multiplication operation. It has

Definition–Subgroup: A **subgroup** of a group G is a subset $H \subseteq G$ such that H is a group.

Definition–Coset: If G is a group and $H \leq G$, consider sets of the form

$$Hg = \{hg | h \in H\} \tag{4}$$

This is a **right coset** of H.

Theorem–Partitioning with Cosets: Consider Hg and Hg' for $g.g' \in G$. There are two cases:

- They might be disjoint: $Hg \cap Hg' = \emptyset$.
- They might intersect. Suppose $hg = h'g'$ for some $h, h' \in H$

$$h^{-1}hg = h^{-1}h'g' \tag{5}$$
$$g = h^{-1}h'g' \in Hg' \tag{6}$$

Similarly, $g' \in Hg$. Consider an arbitrary element of $kg \in Hg$ with $k \in H$. Then, $kg = kh^{-1}h'g' \in Hg'$ i.e. $Hg \leq Hg'$. Similarly, $Hg' \leq Hg$. Thus, $Hg = Hg'$.

The right cosets of H partition G. In particular,

$$G = \bigsqcup Hg_i \tag{7}$$

For fixed g, if $hg = h'g$ for $h, h' \in H$ then $hgg^{-1} = h'gg^{-1}$ so $h = h'$. So in Hg, every element can be matched with an element of H. So, $|Hg| = |H|$.

Theorem–Lagrange: If $|G| < \infty$ and $H \leq G$, then $|H| \Big| |G|$

Definition–Index: For $H \leq G$, the **index** of H in G is $[G : H] = |G|/|H|$.

If $|G| = 13$, the only subgroups or G are $\{e\}, G$.

If $G = \mathbb{Z}$ and $H = 2\mathbb{Z}$ (even numbers). Then $H + 0 = H$ is one coset, and $H + 1 =$ the odd integers is another coset. So, $\mathbb{Z} = (2\mathbb{Z}) \sqcup (2\mathbb{Z} + 1)$.

Same for Left Cosets Interaction of left and right cosets?

Consider the triangle group with rotations e, ρ, ρ^2 and reflections $\sigma_A, \sigma_B, \sigma_C$ Consider the subgroup $H = \{e, \sigma_A\}$.

$$He = \{e, \sigma_A\} \tag{8}$$
$$H\rho = \{\rho, \sigma_B\} \tag{9}$$
$$H\rho^2 = \{\rho^2, \sigma_C\} \tag{10}$$
$$eH = \{e, \sigma_A\} \tag{11}$$
$$\rho H = \{\rho, \sigma_C\} \tag{12}$$
$$\rho^2 H = \{\rho^2, \sigma_B\} \tag{13}$$

Note that the left and right cosets are different. They are the same if the group is commutative.

Definition–Action: An **action** of a group G on a set X is a map

$$G \times X \to X \tag{14}$$
$$(g, x) \mapsto gx \tag{15}$$

such that

$$(gh)x = g(hx) \tag{16}$$
$$ex = x \tag{17}$$

If G is a group, it acts on itself. This is called a "left translation" or "left regular action".

How about the right action $(g, x) \mapsto xg$. The second condition may not be true

$$(gh, x) = xgh \tag{18}$$
$$(g, (hx)) = (g, xh) = xhg \tag{19}$$

which is not true. Instead, let $(g, x) = xg^{-1}$. Then,

$$(gh, x) = x(gh)^{-1} = xh^{-1}g^{-1} \tag{20}$$
$$(g, (h, x)) = (g, xh^{-1}) = xh^{-1}g^{-1} \tag{21}$$

This is the definition of the right action.

There is a third action of G on itself by $(g, x) = gxg^{-1}$. This action is called conjugation.

Take the following example: Let $G = SO(3)$ and let $X = S^2$. G acts on X by rotation. Let $H = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}$ be the subgroup of rotations that fixes the z-axis.

H also acts on X ??

Definition–Orbit: If G acts on X, the **orbit** of $x \in X$ is the set $Gx = \{gx | g \in G\}$. i.e. the set of all points x is taken to by elements of G.

The orbits of $H \approx SO(2)$ on the sphere are the lines of latitude (and the north and south poles).

H fixes the north pole, thus every coset gH takes the north pole to a point. Suppose gH and $g'H$ are cosets such that $gHN = g'HN \implies gN = g'N \implies (g')^{-1}gN = N \implies (g')^{-1}g \in H \implies gH$... so the points ofn the sphere are in 1-1 correspondence with the left cosets of H.

Definition–Stabilizer: If G acts on X and $x \in X$, the "stabilizer" of x in G is $\{g \in G | gx = x\}$

Definition–Centralizer: If $A \subset G$, the **centralizer** of A in G is $C_G(A) = \{g \in G | ga = ag \forall a \in A\}$

- If G is abelian, then $C_G(A) = G$ for any A.
- In the triangle group, $C_G(\{\rho\}) = \{e, \rho, \rho^2\}$

Definition–Center: The **center** of G is $Z(G) = \{g \in G | gg' = g'g \forall g' \in G\} = C_G(G)$

Proposition: For any $A \subset G$, $C_G(A) \leq Z(G)$ (is a subgroup).

Consider the regular n-gon ($n \geq 3$), what are its rigid motion symmetries?

- There are always n rotations by $\frac{2\pi}{n}$ about the origin.
- When n is even, there are $n/2$ reflections in each pair of edges, and each pair of vertices. When n is odd, there are n reflections in each pair of (edge, vertex). There are always n reflections.
- Write ρ for clockwise rotation by $\frac{2\pi}{n}$. Fix one vertex and let σ be the reflection that fixes that vertex.
- Note that $\rho\sigma = \sigma\rho^{-1}$. To show this, it suffices to find where two of the vertices gets mapped.

Proposition: The symmetries are $e, \rho, \rho^2, \ldots, \rho^{n-1}, \sigma, \sigma\rho, \sigma\rho^2, \ldots, \sigma\rho^{n-1}$

Definition–dihedral group: The group of symmetries of the regular n-gon is D_{2n}, the **dihedral group** of order $2n$.

Given $H \leq G$ we write G/H as the set of left cosets

$$G/H = \{gH | g \in G\} \tag{22}$$
$$H \setminus G = \{Hg | g \in G\} \tag{23}$$

Both of these are called "G mod H". In general, the two are different.

Now we want to ask, is $H \setminus G$ a group?

- The most naive idea is to reuse multiplication in G, i.e. $Hg \cdot Hg' = Hgg'$, but it only sometimes works.
- This formula means: $hg \cdot h'g' = h''gg'$. For any $h, h' \in H, \exists h''$ s.t. this holds.
- Trick: $hg \cdot h'g' = hgh'eg' = hgh'(g^{-1}g)g' = h(ghg^{-1})gg'$. Now we can ask if $ghg^{-1} \in H$ (for every $h' \in H$)

Definition–Normal Subgroup: A subgroup $H \leq G$ is **normal** if $ghg^{-1} \in H \forall g \in G, h \in H$, which is abbreviated as $gHg^{-1} = H$. $H \trianglelefteq G$ means H is a normal subgroup of G

- Notice that if $gHg^{-1} = H$ then $gH = Hg$. So H is normal, the left and right cosets must be the same.

Definition–Quotient Group: If $H \trianglelefteq G$, then G/H is called the quotient group.

1.3 Homomorphisms

Definition–Homomorphism: If G, K are groups, a **homomorphism** is a map $\varphi : G \to K$ such that $\varphi(gg') = \varphi(g)\varphi(g') \, \forall g, g' \in G$.

Observations: IF $\varphi : G \to K$ is a homomorphism and $g \in G$, then

1. $\varphi(g) = \varphi(eg) = \varphi(e)\varphi(g)$, so $\varphi(e) = e$ (the identity element of K)
2. $e = \varphi(e) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$, so $\varphi(g^{-1}) = \varphi(g)^{-1}$

Examples

- $G = \mathbb{Z}$ and $\varphi : \mathbb{Z} \to \mathbb{Z}, \varphi(n) = 2n$ is a homomorphism, as $\varphi(n+m) = 2(n+m) = 2n + 2m = \varphi(n) + \varphi(m)$
- $G = \mathbb{Z}, K = \mathbb{R}$ and $\varphi : \mathbb{Z} \to \mathbb{R}, \varphi(n) = n$. This mapping is called an **inclusion** as $Z \subset \mathbb{R}$.
- If G is a group and $g_0 \in G$, then $C_{g_0} : G \to G, g \mapsto g_0 g g_0^{-1}$ is a homomorphism.
- A linear transformation $T : V \to W$ if V, W are vector spaces (the additive group).
- Note that $\varphi : g \mapsto g^{-1}$ is **only** a homomorphism if G is abelian.

Definition–Kernel/Image: If $\varphi : G \to G'$ is a homomorphism, then the **kernel** of φ is

$$\ker(\varphi) = \{g \in G | \varphi(g) = e\}. \tag{24}$$

The **image** of φ is

$$\mathrm{im}(\varphi) = \{\varphi(g) | g \in G\} \subseteq G' \tag{25}$$

Theorem–: $\ker(\varphi) \leq G$ and $\mathrm{im}(\varphi) \leq G'$ $\ker(\varphi) \trianglelefteq G$

Proof. Since $\varphi(e) = e$, $e \in \ker(\varphi)$, and $e \in \mathrm{im}(\varphi)$. So both are nonempty.
Suppose $g, h \in \ker(\varphi)$, $e = \varphi(e) = \varphi(hh^{-1}) = \varphi(h)\varphi(h^{-1}) \ldots$ □

- Suppose $N \trianglelefteq G$ and then define $G \to G/N, g \mapsto Ng$. We claim this is a homomorphism. Proof is simple $\varphi(gg') = Ngg'$, $\varphi(g)\varphi(g') = NgNg' = NgN(g^{-1}gg') = N(gNg^{-1})gg' = NNgg' = Ngg'$
- This map is called the (natural) **projection** of G onto G/N. Sometimes written $\Pi_{G/N}$ or $\mathrm{proj}_{G/N}$.
- $\mathrm{im}(\Pi_{G/N}) = G/N$ and $\ker(\Pi_{G/N}) = N$.
- Any homomorphism is related to this one, so this could be considered as the "generic homomorphism".

Definition–Isomorphism: If $\varphi : G \to H$ is a homomorphism, and $\ker(\varphi) = \{e\}$ then φ is injective. If $\varphi(G) = H$ then φ is surjective. Thinking of G and H as sets, there is an inverse $\varphi^{-1} : H \to G$ such that $\varphi^{-1} \circ \varphi = 1_G$ and $\varphi \circ \varphi^{-1} = 1_H$. It is easy to check that φ^{-1} is also a homomorphism.
In this case, φ is an **isomorphism**

- Suppose we have an injective homomorphism $\varphi : G \to H$ where $\ker(\varphi) = \{e\}$. Then, we can consider $\varphi : G \to \mathrm{im}(\varphi) < H$. Sometimes we say $\varphi : G \to H$ is an **isomorphism into** H, as opposed to an isomorphism **onto** H or between G and H.

Definition–Automorphism: If G is a group, an **automorphism** of G is an isomorphism $\varphi : G \to G$.

Examples:

- If $G = \mathbb{Z}, n \mapsto -n$ is the only automorphism apart from the identity.
- If G is abelian, $g \mapsto g^{-1}$ is an automorphism.
- If F is a field, and $G = GL(n, F)$ then $g \mapsto (g^t)^{-1}$ (transposed inverse) is an automorphism.
- If we fix $g_0 \in G$ then the conjugation $C_{g_0} : G \to G$ where $C_{g_0}(g) = g_0 g {g_0}^{-1}$ is an automorphism.

Definition–Automorphism Group: $\mathrm{Alt}(G)$ is the **group** of automorphisms of G.

Definition–Inner/Outer Automorphisms: The **inner automorphisms** of G are

$$\mathrm{Inn}(G) = \{\varphi \in \mathrm{Alt}(G) | \varphi = C_{g_0} \text{ for some } g_0 \in G\}. \tag{26}$$

If an element of $\mathrm{Alt}(G)$ that is not inner is **outer**.

- It is easy to show that $\mathrm{Inn}(G) \leq \mathrm{Alt}(G)$.
- Observe that if G is abelian, then $\mathrm{Inn}(G) = \{\mathrm{id}\}$
- In general, $\{\mathrm{id}\} \leq \mathrm{Inn}(G) \leq \mathrm{Alt}(G)$.

- The map

$$G \to \mathrm{Alt}(G) \tag{27}$$
$$g \to C_g \tag{28}$$

  is a homomorphism. Its image is $\mathrm{Inn}(G)$ and its kernel is Z_G (the center).

Definition–Fiber: If p is a projection, then $p^{-1}(x)$ is the **fiber** over x

- If $N \triangleleft G$, the projection $\pi : G \to G/N$ is a homomorphism. The fibers of π is the cosets $gN = Ng$, and they are all the same size.
- Suppose $\varphi : G \to H$ is a homomorphism, and $N = \ker(\varphi) \trianglelefteq G$. The fibers of φ is the cosets of G/N.
- We have $\varphi : G \to H$ and $\pi : G \to G/N$. Wouldn't it be nice if $G/N \to H$ "induced by φ" were a homomorphism? Well, it is.

Theorem–(First) Isomorphism: If $\varphi : G \to H$ is a homomorphism, and $N = \ker(\varphi)$, then there is a homomorphism $\bar{\varphi} : G/N \to H$ such that $\bar{\varphi} \circ \pi = \varphi$.
Moreover, $\ker(\bar{\varphi}) = \{eN\}$, the trivial subgroup of G/N, so $\bar{\varphi}$ is injective. So, $\bar{\varphi} : G/N \to \mathrm{im}(\varphi)$ is an **isomorphism**.

- This theorem suggests that you can construct an isomorphism from an arbitrary homomorphism. First, φ factors through G/N, then we can include it into H.

$$G \to^{\pi} G/N \to^{\bar{\varphi}} \mathrm{im}(\varphi) \to^{\text{inclusion}} H \tag{29}$$

Theorem–(Third) Isomorphism: $N \trianglelefteq G$ and $H \leq G$, then $N \leq H \implies N \trianglelefteq G$.

Proof. ???? □

Theorem–:

$$G/H \cong G/N \Big/ H/N \tag{30}$$

Proof. Define $\varphi : G \to G/N \Big/ H/N$ by

$$\varphi(g) = (gN)H/N \tag{31}$$

We need to show φ is a homomorphism. Let

$$\begin{aligned} \varphi(gg') &= gg'N\ H/N && (32)\\ &= gNg'N\ H/N && (33)\\ &= gN\ H/N \cdot g'N\ H/N && (34)\\ &= \varphi(g)\varphi(g') && (35)\\ & && (36) \end{aligned}$$

□

We will then ask what is $\ker(\varphi)$. Suppose $\varphi(g) = H/N$, so $gN\ H/N = H/N$. But g is a representation for gN, so gH/N for this to be in H/N we want $g \in H$ so $\ker(\varphi) = H$. An arbitrary element of $G/N \Big/ H/N$ is $gN\ H/N$ for some $g \in G$, so $\mathrm{im}(\varphi) = G/N \Big/ H/N$.

- $G = \mathbb{Z}, H = 3\mathbb{Z}, K = 4\mathbb{Z}$. By the second isomorphism theorem, $\mathbb{Z}/3\mathbb{Z} \cong 4\mathbb{Z}/12\mathbb{Z}$, and also $Z/4\mathbb{Z} \cong 3\mathbb{Z}/12\mathbb{Z}$.

Definition–Equivilence Class: Being in the same coset of a subgroup H is an equivalence relation. So, the large group is a disjoint union of equivalence classes (cosets) of H.

- The cosets of $\mathbb{Z}$ in $\mathbb{R}$ is $r + \mathbb{Z}$ for $r \in [0, 1)$.
- Homomorphism $\varphi : \mathbb{R} \to \mathbb{C}^\times, t \mapsto e^{2\pi i t}$. Then, $\ker(\varphi) = \mathbb{Z}$. Observe tat φ is **onto** the unit circle, by the first isomorphism theorem, $\mathbb{R}/\ker(\varphi) = \mathbb{R}/\mathbb{Z} \cong S^1$.
- $\mathbb{Z}^2 \triangleleft \mathbb{R}^2$

Theorem–Fourth Isomorphism Theorem/Lattice Theorem: Consider a lattice of subgroups with $N \trianglelefteq G$. In G/N, the subgroup lattice has the same structure as the subgroup lattice of G that contains N.
Specifically, if $N \trianglelefteq G$, and $N \trianglelefteq H < G$, we write $\bar{H} = H/N$. Including $\bar{G} = G/N$ and $\bar{N} = \bar{e} = N/N$. Then, the lattice of $\bar{H}$s in $\bar{G}$ has the same lattice structures as the part of the lattice for G consisting

of subgroups that are intermediate between N and G. Moreover,

$$H \leq K \iff \bar{H} \leq \bar{K} \tag{37}$$
$$H \trianglelefteq K \iff \bar{H} \trianglelefteq \bar{K} \tag{38}$$
$$[H : K] = [\bar{H} : \bar{K}] \text{ if } K \leq H \tag{39}$$
$$\overline{H \cap K} = \bar{H} \cap \bar{K} \tag{40}$$
$$\overline{\langle H, K \rangle} = \langle \bar{H}, \bar{K} \rangle \tag{41}$$

If G, G' are groups, consider the cartesian product $G \times G' = \{(g, g') | g \in G, g' \in G'\}$. Note that $|G \times G'| = |G||H|$. There is an obvious way to turn this into a group by

$$(g, g')(h, h') = (gh, g'h') \tag{42}$$
$$(g, g')^{-1} = (g^{-1}, g'^{-1})e = (e, e) \tag{43}$$

In $G \times G'$, the subset $G_0 =: \{(g, e) | g \in G\} \cong G$ is a subgroup. Likewise, $G_0' =: \{(e, g') | g' \in G'\} \cong G'$. Also notice that G_0 and G_0' commute. So, $(G \times G')/G_0 \cong G'$.

1.4 Symmetric Groups

Definition–Symmetric Group: The symmetric group S_n is the group of permutation of n elements, with composition as the operation.

- $|S_n| = n!$
- A cycle is a permutation that cycles through some subset of $\{1, \ldots, n\}$, denoted as

  $$(a_1\, a_2\, \ldots\, a_k), \quad k \leq n \text{ and } a_i \text{ are distinct.} \tag{44}$$

  Represents the permutation $a_1 \to a_2 \to \cdots \to a_k \to a_1$.
- Note that these are ambiguous, as $(a_1\, a_2\, \ldots\, a_k)$ is the same as $(a_2\, a_3\, \ldots\, a_k\, a_1)$. So by convention, we often start with the smallest number first so they are unique.
- k is the length of the cycle, it is also called a **k-cycle**.
- Every permutation can be written as a product of disjoint cycles. If given a permutation, we will start from 1 and write a cycle until we get back to 1. Then, we will start from the next number that hasn't been included yet and repeat until we get to the end.
- If $\sigma = (1\,3\,6)(4\,5)$, then $\sigma^{-1} = (4\,5)^{-1}(1\,3\,6)^{-1} = (4\,5)(1\,6\,3) = (1\,6\,3)(4\,5)$. We will order the cycles by their first element, and omit 1-cycles.
- Two **disjoint cycles** (i.e. without any numbers in common) will commute.
- If cycles are not disjoint, like $\sigma = (1\,4\,2)(2\,3\,5)(3\,4\,7) \in S_7$ will not commute.
  - $1 \to 4$
  - $4 \to 7$
  - $7 \to 3 \to 5$
  - $5 \to 2 \to 1$
  - $2 \to 3$
  - $3 \to 4 \to 2$

  So $\sigma = (1\,4\,7\,5)(2\,3)$.

- Any k-cycle is a product of 2-cycles. Thus, every element in the symmetric group can be written as a product of 2-cycles so S_n is generated by 2-cycles. For example, if $k = 4$ and $\sigma = (a\,b\,c\,d)$, then $\sigma = (a\,d)(a\,c)(a\,b)$.
- We can ask what is the minimum number of 2-cycles needed to generate any $\sigma \in S_n$. In general, this is a very difficult question to answer. However, the **parity** of the number of 2-cycles in a product equalling σ is well-defined.
- If $\sigma = (a_1\,b_1)(a_2\,b_2)\dots(a_k\,b_k)$ is a product of 2-cycles, then σ is **even** if k is even, and **odd** if k is odd.
- **Warning: a k-cycle is even if k is odd, and odd if k is even.**
- To make odd and even well defined, we need to know that the parity of a permutation is independent of the way we write the cycles.

  Proof. Given $\sigma \in S_n$ is a k-cycle. Define $\Delta = \prod_{1\le i<j\le n}(j-i)$. If $\tau \in S_n$, it acts on Δ with

  $$\tau \cdot \Delta = \prod_{1\le i<j\le n} (\tau(j) - \tau(i)). \tag{45}$$

  These two products are the same up to a factor of ± 1, you have to multiply by -1 for each pair $i < j$ for which $\tau(i) > \tau(j)$.

  We will consider how $(a\,b)$ with $a < b$ affect Δ. If neither i nor j is equal to a or b, the term is unaffected. Note that

  - If $i < a$, then $i < \tau(a) = b$ and $i < \tau(b) = a$. So $(i\,a)$ or $(i\,b)$ are unaffected.
  - Likewise, for $j > b$ then $(a\,j)$ or $(b\,j)$ are unaffected.

  The only pairs that will be affected are ones $(a\,i), (i\,b)$ with $a < i < b$ and $(a\,b)$. If $a < i < b$, then both $(a\,i)$ and $(i\,b)$ will change sign, so the product will be unaffected. $(a\,b)$ will change sign, so Δ will change sign under a transposition.

  If $\sigma \in S_n$, write it as any product of k transpositions. If $\sigma \cdot \Delta = \Delta$ then there must be an even number of transpositions. If $\sigma \cdot \Delta = -\Delta$ then there must be an odd number of transpositions. Thus, the parity of σ is independent of the way we write it. □

Definition–Sign: The sign of $\sigma \in S_n$ is

$$\operatorname{sgn}(\sigma) = (-1)^k, \tag{46}$$

if σ is a product of k transpositions.

- Note that $\operatorname{sgn}(\sigma\tau) = (-1)^k(-1)^l = (-1)^{k+l} = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$.
- Thus, $\operatorname{sgn} : S_n \to \{\pm 1\}$ is a homomorphism.
- $\ker(\operatorname{sgn}) = A_n \trianglelefteq S_n$ is the alternating group of k elements which contains all the even permutations. Note that

  $$S_n/A_n \cong \{\pm 1\} \quad [S_n : A_n] = 2 \quad |A_n| = \frac{n!}{2} \tag{47}$$

- for $n > 5$, A_n has no normal subgroups. What are the possible cycle types in A_5? There is $(a\,b\,c\,d\,e), (a\,b)(c\,d), (a\,b\,c)$
- Let $\sigma \in S_n$ with $a \to b \to c \to \cdots$, and suppose $\tau \in S_n$ takes $a \to a', b \to b', c \to c', \dots$. Consider the conjugation $\tau\sigma\tau^{-1}$.

  $$\tau\sigma\tau^{-1}(a') = \tau\sigma(a) = \tau(b) = b' \tag{48}$$
  $$\tau\sigma\tau^{-1}(b') = \tau\sigma(b) = \tau(c) = c' \tag{49}$$
  $$\tag{50}$$

  So $\tau\sigma\tau^{-1}$ takes $a' \to b' \to c' \to \cdots$. Conjugating by τ "relabels" what σ by replacing a with a', ...

1.5 Simple Group

One way we study groups is to write it as a chain of normal subgroups $G_0 = \{e\} \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_r = G$, where G_{i+1}/G is a simple group $\forall i = 0, \ldots, r-1$. A decomposition like this is called a **Jordan-Holder Series** (composition series), and the quotients are called the **composition factors**. However, the same G may have different composition series.

> **Theorem–Jordan-Holder**: Any two Jordan-Holder series for G have the same length. Moreover, the composition factors are the same (but perhaps in different orders).

Example: Suppose H, K are both normal subgroups of G. Apply 2nd isomorphism theorem. Note, $H \subseteq Norm_G(K) = G$ and $K \subseteq Norm_G(H) = G$. Thus, $HK/K \cong H/H \cap K$ and $HK/H \cong K/H \cap K$. In this example there are two composition series

$$\{e\} \triangleleft H \cap K \triangleleft H \triangleleft HK \triangleleft G \tag{51}$$
$$\{e\} \triangleleft H \cap K \triangleleft K \triangleleft HK \triangleleft G \tag{52}$$

Every group has a Jordan-Holder series. In genera, a group G is not determined by its Jordan-Holder series. However, if G is simple, then its Jordan-Holder series is $\{e\} \triangleleft G$.

> **Definition–Solvable**: If the composition factor G_{i+1}/G_i of G are all **abelian**, we say G is **solvable**.

If G acts on a set X, then each $g \in G$ permutes the element of X. So there is a map $G \to S_X$ (the symmetric group of X). It is easy to show that this map is a homomorphism. So, we will allow ourselves to go between group actions and Homomorphisms into S_X.

Suppose $H \leq G$ and let $X = G/H$ be the coset space. So, G acts on X by left multiplication $g(xH) \mapsto gxH$. If $n = [G : H] = |X|$, the action amounts to a homomorphism $\varphi : G \to S_n$.

Our first observation is that G acts **transitively**. For any $x, y \in X$, $\exists\, g \in G$ s.t. $gx = y$. i.e. the orbit of any $x \in X$ is X.

What is $\ker \varphi$? We know that if $h \in \ker \varphi$, that $hxH = xH$. Then consider $h', h'' \in H$ then

$$hxh' = xh'' \tag{53}$$
$$hx = xh''h'^{-1} \tag{54}$$
$$h = xh''h'^{-1}x^{-1} \tag{55}$$
$$\ker \varphi = \bigcap_{x \in G} xHx^{-1} \tag{56}$$

If $H = \{e\}$, then $G/H = G$, so $\ker \varphi = \{e\}$. then φ is injective. By the first isomorphism theorem, $G \cong \operatorname{im} \varphi = S_n$.

> **Theorem–Cayley**: Any group G with $|G| = n$ is isomorphic to a subgroup of S_n.
>
> *Proof.* We already proved it! □

Another example is to let G act on itself by conjugation. In this case, φ with $g \cdot x = gxg^{-1} = C_g(x)$. This is not a transitive action unless G is trivial. The orbits of conjugation are the **conjugacy classes** of G. They are disjoint (because conjugacy is an equivalence relation).

Note that $geg^{-1} = e$, $\forall g$. If $z \in Z(G)$, then $gzt^{-1} = zgg^{-1} = z \forall g$, then the conjugacy classes contain a single element.

If G is abelian, $Z(G) = G$ and every element is its own conjugacy class.

Because conjugacy is an equivalence relation, G is a disjoint union of all conjugacy classes.

If $Z(G) = \{e, z_1, \ldots, z_k\}$ and $g_1, \ldots, g_m$ are representatives from the non-central conjugacy classes. Let's write $C(g_i) = \{gg_ig^{-1} | g \in G\}$. So,

$$G = Z(G) \sqcup \left(\bigsqcup C(g_i) \right) \tag{57}$$

so

$$|G| = |Z(G)| + \sum_i |C(g_i)| \tag{58}$$

This is called the **Class Equation**.

Theorem–Orbit-Stabilizer: If G acts on X, for each $x \in X$, write $G \cdot x$ for its orbit. Then,

$$|G \cdot x| = [G : G_x] = [G : \mathrm{Stab}(x)] \tag{59}$$

The point is that two things in the same coset of G_x has the same effect on x.

Under conjugation,

$$\mathrm{Stab}(x) = G_x = \{g \in G | gxg^{-1} = x\} = Z(x), \tag{60}$$

the centralizer of x. So the class equation can be rewritten as

$$|G| = |Z(G)| + \sum_i [G : Z(g_i)] \tag{61}$$

Definition–p-group: Suppose p is prime, G is a **p-group** if $|G| = p^k$ for some $k \geq 1$.

Theorem–: If G is a non-trivial p-group, then it has a non-trivial center.

Proof. Suppose $|G| = 1$. Then

$$|G| = |Z(G)| + \sum_i [G : Z(g_i)] \tag{62}$$

Claim $Z(g_i) < G$, otherwise $g_i \in Z(G)$. By Lagrange's theorem $|Z(g_i)| \mid |G| = p^k$. So $|Z(g_i)| = p^l$ for some $l < k$. Then,

$$p^k = |G| = |Z| + \sum_i [G : Z(g_i)] \tag{63}$$

$$\tag{64}$$

Since $|Z| = 1$, the RHS is not divisible by p so this is a contradiction. □

Corollary: Suppose p is prime. If $|G| = p^2$, then G is abelian.

Proof. We know $Z(G)$ is a non-trivial subgroup so $1 \neq |Z(G)| \Big| p^2$. So $|Z(G)| = p$ or p^2. If $|Z(G)| = p^2$, then G is abelian by definition. If $|Z(G)| = p$, then $|G/Z(G)| = p$ hence $G/Z(G) \cong C_p$. So $x \notin Z(G)$, then $G/Z(G) = \{\bar{e}, \bar{x}, \bar{x}^2, \dots \bar{x}^{p-1}\}$ where $\bar{x} =: xZ(G)$. Also, $\bar{x}^p = \bar{e} \in G/Z(G)$. Note that $\text{ord}(x)$ is either p or p^2.

- If $|\langle x \rangle| = p^2$ so $\langle x \rangle = G$ and G is cyclic hence abelian.
- If $\text{ord}(p)$, then $G = \bigcup_{k=0}^{p-1} x^k Z(G)$. Recall $|Z(G)| = p$, so $Z(G)$ is cyclic. Then,

$$Z(G) = \{e, z, z^2, \dots, z^{p-1}\} \tag{65}$$

so

$$G = \{x^i z^j | 0 \leq i, j < p\} \tag{66}$$

These elements commute. $x^i z^j x^m z^n = x^i x^m z^j z^n = x^{i+m} z^{j+n}$

□

Note we need to be careful with the steps in this proof. Just because $\bar{x}^p = \bar{e}$ doesn't mean there is a representative $x \in \bar{x}$ that is order p.

- Now we consider the rotations of a tetrahedron. A easy way to think about this is to identify a "top" vertex, which is well defined (4 possibilities). Then, we fix the top and we have 3 rotations (like of the triangle). So, there are 12 rotations.
- Apart from e, there are two non-trivial rotations that fix any particular vertex. This only accounts for 8 rotations, and e, so we are missing 3 rotations.
- The other rotations does not fix any vertices and are like $(1\,2)(3\,4)$. Then, $2, 3, 4$ goes with 1 so we have 3 rotations. This accounts for all 12.
- In summary, we have e, and 8 rotations in the form $(a\,b\,c)$ and 3 rotations in the form $(a\,b)(c\,d)$. This is A_4.
- The rigid motions are S_4.

Proposition: A_5 is simple. $A_5 \triangleleft S_5$ with index 2, so $|A_5| = 60$.

Proof. We will enumerate the conjugacy classes of S_5

- $(a\,b\,c\,d\,e) \in A_5$
- $(a\,b\,c\,d) \notin A_5$
- $(a\,b\,c) \in A_5$
- $(a\,b\,c)(d\,e) \notin A_5$
- $(a\,b)(c\,d) \in A_5$
- $(a\,b) \notin A_5$
- $e \in A_5$

There are 24 elements in the conjugacy class of $(a\,b\,c\,d\,e)$. However, 24 does not divide 60 so it is not a conjugacy class of A_5.

Consider the centralizer $Z_{A_5}(a\,b\,c\,d\,e) \geq \langle (a\,b\,c\,d\,e)\rangle$ which has order 5. But $Z_{A_5}(a\,b\,c\,d\,e) \leq Z_{S_5}(a\,b\,c\,d\,e)$ so $Z_{A_5}(a\,b\,c\,d\,e) = \langle (a\,b\,c\,d\,e)\rangle$
So there are two A_5 conjugate classes of 5-cycles, each with 12 elements.
There are 20 3-cycles in S_5. Are they all conjugate in A_5? If $(a\,b\,c)$ is conjugate to $(x\,y\,z)$ by $\sigma \in S_5$, then it is also conjugate by $\sigma(d\,e)$ If $\sigma \notin A_5$ then $\sigma(d\,e) \in A_5$ so there is one conjugate class of 20 3-cycles.
There are 15 double transpositions.
If we have a normal subgroup, it is a union of the conjugacy classes, so if A_5 has a normal subgroup it must be a combination of $1 + 15, 20, 12, 12$ but there is no combination (apart from 1) that divides 60. Hence, A_5 is simple. □

2 Sylow Theorems

Theorem–: Suppose $|G| = p^\alpha n$ where $p \not| n$. Then, a subgroup $P \leq G$ is a Sylow p-subgroup if $|P| = p^\alpha$. We'll write $n_p(G)$ for the number of Sylow p-subgroups of G.

1. Sylow p-subgroups exist.
2. Suppose P is a Sylow p-subgroup of G and $Q \leq G$ s.t. $|Q| = p^r$ for some $r > 0$. Then, $\exists\, g \in G$ s.t. $gQg^{-1} \subseteq P$. In particular, all Sylow p-subgroups of G are conjugate.
3. $n_p(G) \equiv 1 \mod p$ and $n_p(G) = [G : \mathrm{Norm}_G(P)]$ for any Sylow p-subgroup. Hence $n_p(G)||G|$. It actually also divides $n = |G|/|P|$.

Before proving the theorem we will consider the following example: Let $G = S_3$. The Sylow 2 subgroups are $\{e, (1\,2)\}, \{e, (1\,3)\}, \{e, (2\,3)\}$ we know $n_2(S_3) = 3 \equiv 1 \mod 2$. The only Sylow 3 subgroup is A_3, so $n_3(S_3) = 1$.

Lemma 1: If G is abelian and $p \Big| |G|$, then G contains an element of order p.

Proof. If $|G| = p$ then G is cyclic and every non-trivial element has order p.
If $|G| > p$, and $x \in G$ with order $p^r m$ where $p \not| m$. If $r \neq 0$,then $x^{p^{r-1}m}$ has order p.
This reduces us to the case where $p \nmid \mathrm{ord}(x), \forall x \in G$. We will use induction.

- Assume the result is true for all groups smaller than G.
- If $p \nmid \mathrm{ord}(x) = |\langle x\rangle| < |G|$. As G is abelian, then $N =: \langle x\rangle \triangleleft G$.
- By induction G/N contains an element of order p.
- i.e. $\exists y = y_0 N \in G/N$ s.t. $y^p = e = N$. so $y_0^p \in N$
- We claim that $\langle y_0^p\rangle < \langle y_0\rangle$ since otherwise $y_0 \in N$ which has order 1.
- This means $p \mid |y_0|$ otherwise $\langle y_0^p\rangle = \langle y_0\rangle$. This is a contradiction.
- This means a suitable power of y_0 must have order p.

□

Lemma 2: If $P \in \mathrm{Syl}_p(G)$ and Q is a non-trivial p-subgroup of G. Then, $Q \cap \mathrm{Norm}_G(P) = Q \cap P$.

Proof. Let $H = Q \cap \mathrm{Norm}_G(P) \geq Q \cap P$. We need to show that $H \leq Q \cap P$. But $H \leq Q$ so we only need to show that $H \leq P$.

$H \leq N_G(P) \implies HP$ is a subgroup. The result will follow if we can argue that HP is a p-group. We know that

$$|HP| = \frac{|H||P|}{|H \cap P|} \tag{67}$$

Since $|H|, |P|, |H \cap P|$ are all powers of P. So $HP \geq P$ but $|HP|$ can't be bigger than $|P|$. $\square$

Proof that Sylow p-subgroup exists. We will use induction on $|G|$.

If $p \mid |Z(G)|$, we know by the lemma that $\exists z \in Z(G)$ with $|z| = p$. Let $N = \langle z \rangle$ is a normal subgroup as $N \leq Z(G)$. Then, G/N is a smaller group than G. By the induction hypothesis say G/N has a Sylow p-subgroup.

If $|G| = p^\alpha m, p \nmid m$ then $G/N = p^{\alpha-1}m$. So, it has a Sylow p-subgroup of order $p^{\alpha-1}$. By the lattice isomorphism theorem, the preimage of this group in G has order p^α, as required.

Assume $p \nmid |Z(G)|$. Let $g_1, \ldots, g_k$ be representatives of the non-central conjugacy classes of G. So,

$$|Z(G)| + \sum_{i=1}^{k} [G : C_G(g_i)] = |G|. \tag{68}$$

We know that $p \mid |G|$ but $p \nmid |Z(G)|$ meaning for some i, we know $p \nmid [G : C_G(g_i)]$. As g_i represents a non-central conjugacy class, then $C_G(g_i) < G$. We will use the induction hypothesis. Note that since $p \nmid [G : C_G(g_i)]$, then $p^\alpha \mid |C_G(g_i)|$. By the induction hypothesis, $C_G(g_i)$ has a Sylow p-subgroup of order p^α, it is also a Sylow p-subgroup of G. Thus, Sylow p-subgroups exist.

Fix a Sylow p-subgroup P_1 of G and enumerate all its distinct conjugates as $P_1, \ldots, P_r$. Let Q be any p-subgroup.

G acts on $\mathcal{S} = \{P_1, \ldots, P_r\}$, and Q also act on $\mathcal{S}$, but it may not have a single orbit. Decompose $\mathcal{S}$ into Q orbits,

$$S = \mathcal{O}_1 \sqcup \mathcal{O}_2 \sqcup \cdots \sqcup \mathcal{O}_s. \tag{69}$$

How big is $\mathcal{O}_k$? Relabel $P_1, \ldots P_k$ s.t. $\mathcal{O}_k = \{qP_kq^{-1} | q \in Q\}$. We know how to find the size of a conjugacy class. $|\mathcal{O}_k| = [Q : N_Q(P_k)]$. Note that $N_Q(P_k) = N_G(P_k) \cap Q$. The second lemma states $N_G(P_k) \cap Q = P_k \cap Q$.

For now, let $Q = P_1$. So, $\mathcal{O}_1 = \{qP_1q^{-1} | q \in P_1\} = P_1$.

$$|S| = r = \underbrace{|\mathcal{O}_1|}_{1} + \underbrace{\sum_{i=2}^{s} [P_1 : P_1 \cap P_i]}_{\text{divisible by } p} \tag{70}$$

If we know that if all Sylow p-subgroup are conjugate, then we know the number of Sylow p-subgroup is $1 \mod p$.

Let Q be any p-subgroup of G and suppose Q is not contained in any of the $P_1, \ldots P_r$. Then, $Q \cap P_i$ is a proper subgroup of Q. Then,

$$|\mathcal{O}_k| = [Q : P_k \cap Q] \tag{71}$$

is divisible by P. So, $p \mid |\mathcal{S}|$ so $p \mid |r$ but $r \equiv 1 \mod p$ so this is a contradiction.

Suppose $|G| = pq$, and $p < q$ prime. We know $n_q(G) = 1$, i.e. $\mathrm{Syl}(G) = \{Q\}$, then $Q \triangleleft G$. One possibilities is that G is cyclic. Often, $n_p(G) = 0$ unless $p \mid (q-1)$, then it is more complicated.

The significance os $q-1 =$ the number of units $\mod q$, which turns out to be the number of automorphisms of C_q. (multiply each element of C_q by a unit $u = (\mathbb{Z}/q\mathbb{Z})^x$.

So this is a homomorphism $C_p \to \mathrm{Aut}(C_q)$. We can use this homomorphism to make a group that is not abelian.

Definition–Finitely Generated: An abelian group G is **finitely generated** if there exists a finite set S such that $G = \langle S \rangle$.

Examples of finitely generated abelian groups are finite abelian groups, $\mathbb{Z}, \mathbb{Z}^r$ but not $\mathbb{R}, S^1, \mathbb{Q}$.

Theorem–Fundamental Theorem of Abelian Groups: If G is a finitely generated abelian group, then G is isomorphic to a product

$$G \cong \mathbb{Z}^r \times \prod_{i=1}^{s} C_{r_i} \tag{72}$$

where $r \in \mathbb{N}_0, n_i \in \mathbb{N}^{>1}$, and $n_{i+1} \mid n_i \forall i = 1, \ldots, s-1$. Note the following:

- $r = 0 \iff G$ is finite.
- G is cyclic $\iff r = 0 \wedge s = 1$

Moreover, this decomposition is unique up to isomorphism.

Proof. The proof will come easily from another theorem later. □

Definition–: In this decomposition, r is called the **free rank** of G or the **Betti number**Other Information of G. The n_i's are called the **invariant factors** of G.

Another version. Any finitely generated abelian group G can be written as

$$G = \mathbb{Z}^r \times \prod_{i=1}^{k} P_{p_i} \tag{73}$$

where $|G/\mathbb{Z}^r| = \prod_i p_i^{\alpha_i}$. Moreover, for each i,

$$P_{p_i} = C_{p_i^{\beta_1^i}} \times C_{p_i^{\beta_2^i}} \times \cdots \times C_{p_i^{\beta_{\alpha_i}^i}} \tag{74}$$

where $\beta_1^i \geq \beta_2^i \geq \cdots \geq \beta_{\alpha_i}^i$ and $\beta_1^i + \beta_2^i + \cdots + \beta_{\alpha_i}^i = \alpha_i$. The notation is awful, but idea is we can decompose G into its Sylow p-subgroups and then decompose each Sylow p-subgroup into its cyclic factors. This decomposition is unique up to isomorphism.

Definition–Elementary Divisors: The subgroups $C_{p_i^{\beta_1^i}}, \ldots, C_{p_i^{\beta_{\alpha_i}^i}}$ or sometimes their orders are called the **elementary divisors** of G.

Semidirect product of $\mathbb{R}^2 \rtimes SO(2)$. Translate first then rotate. e.g. $g = \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right)$ and $g' = \left(\begin{pmatrix} -1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \right)$. These are the motions of the plane that preserves lengths and angles.

Theorem–: Let G be a finite group and $G_0 = G$. then construct $G_1 = [G_0, G_0], \dots G_i = [G_{i-1}, G_{i-1}]$. This series will always terminate, and G is solvable iff $\exists r$ s.t. $G_r = \{e\}$.

Proof. Messy, but not hard. □

Definition–Upper Central Series: $Z_0 = \{e\}, Z_1(G)$ and $Z_1(G) = Z(G)$ then let Z_2 be a subgroup of G s.t. $Z_2(G)/Z_1(G) = Z(G/Z_1(G))$, $Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$. This series will always terminate with

$$\{e\} = Z_0 \triangleleft Z_1 \triangleleft Z_2 \triangleleft \cdots \triangleleft Z_r = G \tag{75}$$

Definition–Nilpotent: G is **nilpotent** if G is solvable and $Z_r(G) = G$.

Definition–Lower Central Series: $G^{(0)} = G, G^{(1)} = [G, G], G^{(2)} = [G^{(0)}, G^{(1)}], G^{(i)} = [G^{(0)}, G^{(i-1)}]$.

Theorem–: G is solvable iff $\exists r$ s.t. $G^{(r)} = \{e\}$.

We have developed the following understanding of groups in order of complexity:

1. Trivial group $\{e\}$
2. Cyclic group of prime order C_p
3. Cyclic group C_n
4. Abelian group
5. p-group
6. Nilpotent group
7. Solvable group

Definition–Characteristic: A proper subgroup $H < G$ is a **characteristic subgroup** if $\varphi(H) = H$ for all $\varphi \in \mathrm{Alt}(G)$. (Note normal subgroups are only required to satisfy this property for inner automorphisms).

Proposition: If H is normal in a characteristic subgroup of G, then $H \trianglelefteq G$. This is not true without the characteristic property.

2.1 Nilpotent Groups

Easy: p-groups are nilpotent.

(almost) easy: a product of nilpotent groups is nilpotent. (the pieces in the definition of nilpotence work "component-wise" in a product).

In particular, product of p-groups are nilpotent.

If P is a p-group and Q is a q-group, in $G = P \times Q$, $P = P \times \{e\} \in \mathrm{Syl}_p(G) \triangleleft G$ and $Q = \{e\} \times Q \in \mathrm{Syl}_q(G) \triangleleft G$. Analogously, $G = P_1 \times P_2 \times \cdots \times P_k$ is nilpotent iff P_i is a p_i-group, then the P_is are the Sylow p_i-subgroups of G, and each is normal (so it is the only p_i subgroup).

Theorem–: Suppose G is finite, then the following are equivalent:

1. G is nilpotent.
2. If $H < G$ is a proper subgroup, then $H < N_G(H)$ is also a proper subgroup.
3. If $p \mid |G|$ and $P \in \mathrm{Syl}_p(G)$, then P is normal. Hence, all Sylow p-subgroups are normal.
4. $G \cong P_1 \times \cdots \times P_k$ where $P_i \in \mathrm{Syl}_{p_i}(G)$ and $p_1, \cdots, p_k$ are distinct primes.

Proof (hint $1 \to 2$). If G is abelian, then the proof is trivial. So, we can assume G is not abelian. Otherwise, the proof of the theorem is trivial. □

Consider a finite field $\mathbb{F}$ and matrices over $\mathbb{F}$ with the form $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$. Suppose two matrices of this form,

$$\underbrace{\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}}_{g} \underbrace{\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}}_{h} = \begin{pmatrix} 1 & a+x & b+az+y \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{pmatrix} \tag{76}$$

$$hg = \begin{pmatrix} 1 & a+x & b+cx+y \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{pmatrix} \tag{77}$$

$$[g,h] = g^{-1}h^{-1}gh = \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{78}$$

If $G = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\}$, then $[G,G] = \left\{ \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}$, and $[G,[G,G]] = \{e\}$. This shows G is solvable. If we extend n to any number beyond 3, the same argument holds.

Theorem–Very hard ones:

1. (Burnside) If $|G| = p^a q^b$ and p, q are distinct primes, then G is solvable.
2. (Philip Hall) Suppose that for each prime p dividing $|G|$, with $|G| = p^a m$ so that $gcd(m,p) = 1$. Suppose $\exists H < G$ s.t. $|H| = m$ s.t. $G = PH$ where $P \in \mathrm{Syl}_p(G)$. If this holds for all p, then G is solvable.
3. (Feit–Thompson) If $|G|$ is odd, then G is solvable.
4. (Thompson) Suppose that for any $x, y \in G$, the subgroup they generate $\langle x, y \rangle$ is solvable. Then G is solvable.

Proof. The proofs of these theorems are hundreds of pages long. □

3 Rings

Rings are a difficult topic because there are very few results that holds for all rings. To learn about rings, we need to show many things for specific cases. There are some important differences

1. Rings need not have multiplicative inverses.
2. Rings need not be commutative.
3. Rings need not have multiplicative identities.

Definition–Ring: A ring R is an abelian group under addition, with additive identity 0. A ring also have multiplication, and multiplication is associative. Also, the left and right distributive law holds: for $x, y, z \in R$, $x(y+z) = xy + xz$ and $(x+y)z = xz + yz$. The ring may not have a multiplicative identity.

Examples:

- Any field is a ring.
- $\mathbb{Z}$
- The set of all matrices over a field.
- Polynomials of n variables over a field.
- $\mathbb{Z}/n\mathbb{Z}$ is a finite ring. It is not a field if n is not prime.
- If X is a set, then the set of functions on X with values in a field $\mathbb{F}$ is a commutative ring. with

$$(f+g)(x) = f(x) + g(x) \tag{79}$$
$$(f \cdot g)(x) = f(x)g(x) \tag{80}$$

- If X is a topological space, then the set of continuous functions on X is a ring.
- $C_c(X)$ (continuous functions with compact support) is a ring.

If R is a ring, then

1. $\forall r \in R, \quad 0 \cdot r = r \cdot 0 = 0.$
2. $\forall a, b \in R, \quad (-a) \cdot b = a \cdot (-b) = -(a \cdot b).$
3. $\forall a, b \in R, \quad (-a)(-b) = ab$
4. If R has a unit 1, then it is unique and $(-1)a = a(-1) = -a$ for all $a \in R$.

Exercise: Find an example of a "one-sided" identity: $1_L \cdot a = a \forall a$ but $a \cdot 1_L \neq a$ for some a.

Definition–Integral Domain: An **integral domain** is a commutative ring with unit, and no zero divisors. i.e. $\forall a, b \in R, \quad ab = 0 \implies a = 0 \vee b = 0.$

Proposition: **Cancellation law:** in an integral domain, if $ab = ac$ where $a \neq 0$, then $b = c$.

Proof. Suppose $ab = ac$ and $a \neq 0$ then $a(b-c) = 0$ as $a \neq 0, b - c = 0$ so $b = c$. □

Note that if R has zero divisors say $ab = 0$ where $a, b \neq 0$ we can write $ab = a0$ so if there were a cancellation law this will contradict the assumption that $b \neq 0$.

In $\mathbb{Z}/12\mathbb{Z}$ we have $3 \cdot 4 = 3 \cdot 8$ but $4 \neq 8$.

Theorem–: A finite integral domain must be a field.

Proof. The other axioms for a field is already satisfied. We only need to show that R has multiplicative inverses.
For $a \neq 0$ define a map $\Phi : R \to R$ where $\Phi(x) = ax$. Note this is not a homomorphism. The cancellation law implies Φ is injective, since R is finite Φ is also surjective. Hence, $\exists\ x \in R$ s.t. $ax = 1$ so $x = a^{-1}$. □

Theorem–Wedderburn: A finite division ring is a field.

Proof. Homework □

Definition–Unit: A unit in a ring R is an element u s.t. it has an multiplicative inverse v s.t. $uv = vu = 1$.

Definition–Group Ring: Suppose G is a finite group and $\mathbb{F}$ is a field. The group ring $\mathbb{F}[G]$ (our text writes FG) "group ring of G over $\mathbb{F}$" is

$$\mathbb{F}[G] = \{\sum_{g\in G} a_g \cdot g \mid a_g \in \mathbb{F}\} \tag{81}$$

formal linear combination of elements of G.
Multiplication is defined by extending group multiplication.

$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} a_h h\right) =: \sum_{(g,h)\in G^2} a_g b_h \cdot gh. \tag{82}$$

An equivalent, but quite different way of looking at it is to define $a : G \to F$ and $b : G \to F$ and define

$$a \cdot b = \sum_{hk=g} a(h)b(k) = \sum_{h\in G} a_h \cdot b_{h^{-1}g}. \tag{83}$$

The set of all such possible functions from $G \to F$ is the same as the previous definition.
As an exercise, find a ring isomorphism between these two definitions.

If $n = |G|$ take an n-dimensional vector space over $\mathbb{F}$ and pick a basis, and label the basis with elements of G and then define multiplication by the first definition.

We can also use a ring for the coefficient rather than a field. We can also have an infinite group (but only with finite linear combinations)

Example 1 ()

If $|G| = n < \infty$ consider $\mathbb{F}[G]$ and let $r = \sum_{g\in G} 1 \cdot g$.
If $h \in G$, regard it as $1 \cdot h \in \mathbb{F}[G]$. Then, $h \cdot r = \sum_{g\in G} h \cdot g = r$.

Definition–Subring: If R is a ring, a subset $S \subseteq R$ is a **subring** if the restriction to S of the ring operation from R make S into a ring. i.e.

- $0 \in S$
- S must be closed under addition and multiplication.

- If $a \in S$, then $-a \in S$.

Another way to say this is that S is an additive subgroup of R that is closed under multiplication (the same multiplication as R).

- $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ are subrings
- $n\mathbb{Z} \subset \mathbb{Z}$. Note that $n\mathbb{Z}$ does not have (multiplicative) identity unless $n = 1$.

Recall the hamiltonian quaternion $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$, and an obvious subring is the quaternions with integer coefficients, called the "naive quaternions". The better subring called the Hurwitz quaternions is $\{a + bi + cj + dk + \frac{n}{2}(1 + i + j + k) | a, b, c, d, n \in \mathbb{Z}\}$. Observe that

$$\frac{1+i+j+k}{2} \cdot \frac{1-i-j-k}{2} = \frac{1}{4}(1 - (-1) - (-1) - (-1)) = 1. \tag{84}$$

If $D \in \mathbb{Z}$ is square-free, recall $\mathbb{Q}[\sqrt{D}] = \{a + b\sqrt{D} | a, b \in Q\}$ is a quadratic field. There is an obvious subring $\{a + b\sqrt{D} | a, b \in Z\}$, but it turns out that there is a better choice.

If $D \equiv 1 \pmod 4$ let $\omega = (1 + \sqrt{D})/2$ otherwise $\omega = \sqrt{D}$. In $Q[\sqrt{D}]$, the "ring of integers" is $\mathbb{Z}[\omega] = \{a + b\omega | a, b \in \mathbb{Z}\}$. This is a ring

$$(a + b\omega)(c + d\omega) = ac + (ad + bc)\omega + bd\omega^2 \tag{85}$$

$$\omega^2 = \frac{1}{4}\left(1 + 2\sqrt{D} + D\right) \tag{86}$$

$$= \frac{1}{4}\left(1 + 2\sqrt{D} + D\right) \tag{87}$$

$$= \frac{1}{4}\left(1 + 2\sqrt{D} + 1 + 4k\right) \tag{88}$$

$$= \frac{1 + \sqrt{D}}{2} + k = k + \omega \in \mathbb{Z}[\omega]. \tag{89}$$

These rings are called "ring of integers" because in many respects they play the same role that $\mathbb{Z}$ does in $\mathbb{Q}$. In $\mathbb{Q}[i]$, the $N(a + bi) = (a + bi)\overline{(a + bi)} = a^2 + b^2 = |a + bi|^2$. In $\mathbb{Q}[\sqrt{D}]$ define the norm analogously $N(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2$. We claim that $N(a + b\sqrt{D}) \neq 0$ unless $a = b = 0$, as if it were then $a^2 = Db^2$, so $D = \frac{a^2}{b^2}$, which is impossible since D is square-free.

Easy: N is "multiplicative":

$$N((a + b\sqrt{D})(c + d\sqrt{D})) = N(a + b\sqrt{D})(c + d\sqrt{D}) \tag{90}$$

So N is a group homomorphism from $\mathbb{Q}[\sqrt{D}]^\times \to \mathbb{Q}^\times$. Note this is **not** a ring homomorphism as it does not respect addition.

Easy: $N : \mathbb{Z}[\omega] \to \mathbb{Z}$. Very easy if $D \not\equiv 1 \pmod 4$. If $D \equiv 1 \pmod 4$, then

$$N(a + b\omega) = \left(a + b\frac{1 + \sqrt{D}}{2}\right)\left(a + b\frac{1 - \sqrt{D}}{2}\right) \tag{91}$$

$$= a^2 + ab\left(\frac{1 + \sqrt{D}}{2} + \frac{1 - \sqrt{D}}{2}\right) + b^2\frac{1 - D}{4} \tag{92}$$

$$= a^2 + ab + b^2\frac{1 - D}{4} \tag{93}$$

As $D \equiv 1 \pmod 4$, $1 - D \equiv 0 \pmod 4$, so $N(a + b\omega)$ is an integer.

FACT: $\mathbb{Z}[\omega]$ is the set of all elements of $\mathbb{Q}[\sqrt{D}]$ whose norms are in $\mathbb{Z}$, i.e. $\mathbb{Z}[\omega] = N^{-1}(\mathbb{Z})$. It is always true that $\mathbb{Z}[D] \subseteq N^{-1}(\mathbb{Z})$, but they are not equal if $D \equiv 1 \pmod 4$. The proof is a **challenge**.

Note this fact is true for the Hurwitz quaternions.

If $x = a + b\omega$ is in the ring of integers, then so is $\bar{x} =: a - b\omega$. We know $N(x) = x\bar{x}$. If $N(x) = 1 = x\bar{x}$, then x is a unit as $x^{-1} = \bar{x}$. Even if $N(x) = -1$, then $x^{-1} = -\bar{x}$.

The set of units in the ring of integers is $N^{-1}(\pm 1) = \{x \in \mathbb{Z}[\omega] \mid N(x) = \pm 1\}$.

Definition–Polynomial: Suppose R is a commutative ring with identity. Define the polynomial ring

$$R[x] = \{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \mid a_i \in R\}, \tag{94}$$

with addition and multiplication defined in the usual way.
If R is also a field, then $R[x]$ is a vector space over R.
If $a_n \neq 0$, it is the "leading coefficient" and $\deg(a_0 + a_1 x + \cdots + a_n x^n) = n$. Some people define $\deg(0) = -\infty$. Then, for $f, g \in R[x]$, and R has no zero divisors then $\deg(fg) = \deg(f) + \deg(g)$.

If R is an integral domain, then so is $R[x]$.

If G is a non-trivial finite group, and R be any ring then $R[G]$ always has zero divisors.

If $1 \in R$ choose $e \neq g \in G$ and if $|g| = n$, observe that $(e - g)(e + g + g^2 + \cdots + g^{n-1}) = 0$.

Definition–Ring Homomorphism: A **ring homomorphism** $\varphi : R \to S$ is a map that respects addition and multiplication. That is, if $a, b \in R$ then

$$\varphi(a + b) = \varphi(a) + \varphi(b) \tag{95}$$
$$\varphi(ab) = \varphi(a)\varphi(b). \tag{96}$$

Some books requires that φ takes units to units, but we will not make this requirement.

Proposition: If $\varphi : R \to S$ then $\ker(\varphi) \subseteq R$ is a subring of R, and $\mathrm{im}(\varphi) \subseteq S$ is a subring of S.

Proof. trivial. □

The kernel of φ has an interesting property. Let $K = \ker(\varphi)$. Then, if $k \in K, r \in R$ then $\varphi(rk) = \varphi(r)\varphi(k) = \varphi(r)0 = 0$, and $\varphi(kr) = \varphi(k)\varphi(r) = 0\varphi(r) = 0$.

Suppose $N \subseteq R$. As additive groups $N \trianglelefteq R$ so we can construct R/N. To turn this into a ring, we need to define multiplication, and we can do this by defining

$$(r + N)(r' + N) = rr' + N \tag{97}$$

We need to ensure that this is well defined. Suppose $r = s + n, r' = s' + n'$ with $n, n' \in N$. Then,

$$(s + N)(s' + N) = ss' + N = (r - n + N)(r' - n' + N) = rr' - nr' - rn' + nn' + N \tag{98}$$

we require this to be equal to $rr' + N$. Hence, we require $nr' - rn' \in N$ which is true if nr' and rn' are both in N. So, the multiplication on R/N is well defined if $RN \subseteq N$ and $NR \subseteq N$

Definition–Ideal: A subring $N \subseteq R$ is an **ideal** if $RN \subseteq N$ and $NR \subseteq N$. In this case, R/N is a ring with the multiplication defined above.

3.1 Ideals

For this section, we will always assume the ring has at least one unit.

Definition–Ideal: a In a ring R, a subring I is

- a **left ideal** if $\forall r \in R,\ \forall i \in I,\ ri \in I$.
- a **right ideal** if $\forall r \in R,\ \forall i \in I,\ ir \in I$.
- a **(two-sided) ideal** if it is both a left and right ideal.

Recall the kernel of a ring homomorphism is a two-sided ideal. If I is a two-sided ideal, then R/I is a ring. If I is a left ideal, then R/I is a left module over R/I. If I is a right ideal, then R/I is a right module over R/I.

Example 2 ()

If R is the space of $\mathbb{F}$-valued functions on X, the evaluation map at $x \in X$ is

$$\varphi_x(f) = f(x) \in \mathbb{F} \tag{99}$$
$$\varphi_x : R \to \mathbb{F} \tag{100}$$

$\ker(\varphi_x) = \{f \in R \mid f(x) = 0\}$ is the ideal of all functions that vanish at x. This also works for more restrictive functions (i.e. continuous, differentiable, etc.)

Theorem–First Isomorphism: If $\varphi : R \to S$ is a ring homomorphism, and $I = \ker(\varphi)$ then $R/I \cong \mathrm{im}(\varphi)$.
If I is a two-sided ideal in R, then $\varphi : R \to R/I, r \mapsto r + I$ is a ring homomorphism with kernel I.

If $A \subseteq R$, then we can define the **ideal generated by** A denoted (A). If A is a singleton $\{a\}$, we denote (a), and if A is a finite set $\{a_1, \ldots, a_n\}$, we denote $(a_1, \ldots, a_n)$.

$$(A) = \bigcap_{\substack{A \subseteq I \subseteq R \\ I \text{ is an ideal}}} I \tag{101}$$

The same definition can be used for left and right ideal.

Definition–Maximal Ideal: An ideal M is a **maximal ideal** if there is no **proper** ideal I s.t. $M \subset I \subset R$ and $M \neq I$.

It is easy to show that

- An ideal M is proper *i.e.* $M \neq R$ iff $1 \notin M$.
- The left ideal generated by a is $Ra = \{ra \mid r \in R\}$.
- The right ideal generated by a is $aR = \{ar \mid r \in R\}$.

Note that the two-sided ideal generated by a is not always equal to $\{ras \mid r, s \in R\}$. Certainly (a) contains these, but this set is not always closed under addition. So, $(a) = RaR = \{\sum_{i=1}^{n} r_i a s_i \mid \forall i, r_i, s_i \in R\}$.

Proposition: If $1 \in R$ then any proper ideal is contained in a maximal ideal.

Proof. Suppose I is a proper ideal, and consider all proper ideals containing I ordered by inclusion. If C is a chain of such ideals, let $M = \bigcup_{J \in C} J$. If we can show M is a proper ideal then it is an upper bound for C and zorn's lemma implies M is maximal.
Suppose M is not a proper ideal, then $1 \in M$ so $1 \in J$ for some $J \in C$ which means J is not proper. This is a contradiction so M is a proper ideal. □

The second, third, and fourth isomorphism theorems all have ring analogues.

Proposition: If R is commutative, then an ideal M is maximal iff R/M is a field.

Proof. Use the fourth isomorphism theorem with the fact that fields have no proper ideals. □

Example 3 ()

Evaluation map $\varphi : \mathcal{F}(X) \to \mathbb{F}, f \mapsto f(x)$ then $M/\ker(\varphi) \cong \mathbb{F}$. Note that if $\mathbb{F}$ is an algebraically closed field, $\mathcal{F}(X)$ is a polynomial ring, then these are the only maximal ideals.

Assume R is a commutative ring with 1. In $\mathbb{Z}$, if $a/b = c/d \iff ad = bc$. We want to mimic this in R, the problem is if b is a zero divisor, then $a/b \cdot c/d = ac/bd$.

Start by specifying a set of potential denominators. Suppose $D \subseteq R$ s.t.

- $0 \notin D$
- D contains no zero divisors
- D is closed under multiplication

Note we do not assume D is closed under addition.

In the traditional construction of $\mathbb{Q}$ from $\mathbb{Z}$, we let $D = \mathbb{Z} \setminus \{0\}$.

If $d \neq 0$, we can let $D = \{d, d^2, d^3, \ldots\}$. or $D = \{1, d, d^2, d^3, \ldots\}$.

We consider pairs $(r, d) \in R \times D$ (which corresponds to r/d) and we can define addition and multiplication as follows

$$(r, d) + (r', d') = (rd' + dr', dd') \tag{102}$$
$$(r, d)(r', d') = (rr', dd') \tag{103}$$

We must also define an equivalence relation as follows

$$(r, d) \sim (r', d') \iff rd' = dr' \tag{104}$$

To confirm it is an equivalence relation, we must verify it is symmetric and transitive.

$$(r, d) \sim (r', d') \iff rd' = dr' \iff r'd = d'r \iff (r', d') \sim (r, d) \tag{105}$$

Suppose $(a, b) \sim (c, d) \wedge (c, d) \sim (r, s)$ then $ad - bc = 0$ and $cs - dr = 0$. Consider

$$d(as - br) = ads - brs \tag{106}$$
$$= ads - bcs + bcs - bdr \tag{107}$$
$$= (ad - bc)s + b(cs - dr) = 0 \tag{108}$$

because d is not a zero divisor, then $as - br = 0$ so $(a, b) \sim (r, s)$.

The definitions of addition and multiplication respect the equivalence relation (tedious to check), so they are well defined. Therefore, we can regard the set of equivalence classes $Q = (R \times D)/\sim$ as a ring.

The set $\{(dr, d) \mid d \in D, r \in R\} \cong R$. Also, Q contains $(1, d) \forall d \in D$.

Q contains (a copy of) R and in Q, every $d \in D$ is invertible. So Q is called the ring of fractions relative to D.

If $D = R \setminus \{0\}$ (which requires D to have no zero divisors) then Q is a field, called the "quotient field of R". If $R = \mathbb{Z}$, then $Q = \mathbb{Q}$.

Example 4 ()

Suppose $R = \mathbb{Z}$, and $D = 2\mathbb{Z} \setminus \{0\}$. Then $Q = \mathbb{Q}$ because $r/s = 2r/2s$.

In general, $Q \ni d/d = 1$, and is the smallest ring with these properties in the following sense:

If $\varphi : R \to S$ is an injective ring homomorphism into a ring S with the required properties, then φ extends to Q.

Fix $d \in \mathbb{Z}, d \neq 0$ let $D = \{d, d^2, d^3, \ldots\}$. Then $Q = \mathbb{Z}/D$. Construct $Q = \{r/d^k \mid r \in \mathbb{Z}, k \geq 0\}$. (it does not matter if we include 1 or not because $dr/d = r/1$.) These two examples show that we can choose different sets of D and get the same Q.

Theorem–Chinese Remainder: Inspiration: Note that $105 = 3 \cdot 5 \cdot 7$. If you have an unspecified number of soldiers, you can line them up in 3s but you may have some left over. You can also line them up in 5s but you may have some left over. You can also line them up in 7s but you may have some left over. If you know how many are left over, can you determine how many soldiers you have left over if you line them up in 105s? We can use the Chinese Remainder Theorem to answer this question.

Chinese Remainder Theorem: In a commutative ring R, with identity; two ideals A, B are called co-maximal if $A + B = R$. If $A_1, \ldots, A_m$ are ideals in R and

$$\varphi : R \to R/A_1 \times \cdots \times R/A_m \tag{109}$$
$$r \mapsto (r + A_1, \ldots, r + A_m) \tag{110}$$

Then $\ker \varphi = \bigcap_{i=1}^{m} A_i$ and

$$\bar{\varphi} : R/\ker \varphi \to R/A_1 \times \cdots \times R/A_m \tag{111}$$

is a ring homomorphism. If the A_is are pairwise co-maximal, then $\bar{\varphi}$ is an isomorphism and $\bigcap A_i = A_1 \cdot A_2 \cdot \cdots \cdot A_m$ where $\cdot$ is the ring product.

Proof. For surjectivity, we will prove by induction. First, consider $m = 2$. We assumed that the ideals are co-maximal so $A_1 + A_2 = R$ so $a + b = 1$ for some $a \in A_1, b \in A_2$.
Given $(s + A_1, t + A_2) \in R/A_1 \times R/A_2$, Note that

$$ta + sb + A_1 = sb + A_1 = sa + sb + A_1 = s + A_1 \tag{112}$$
$$ta + sb + A_2 = ta + A_2 = ta + tb + A_2 = t + A_2 \tag{113}$$

so $\varphi(ta + sb) = (s + A_1, t + A_2)$
For the inductive case, suppose $m \geq 3$ and assume the statement is true for $m - 1$.
Finally, we want to show $\cap A_i = \prod A_i$ □

Consider the chinese remainder theorem in $R = \mathbb{F}[x]$, where $\mathbb{F}$ is a field. Suppose $P_i(x) \in \mathbb{F}[x]$ for $i = 1, \ldots, k$

are pairwise relatively prime i.e. P_i, P_j have no roots in common, even in the algebraic closure of $\mathbb{F}$. This means that the ideals $(P_i(x))$ are pairwise co-maximal. Suppose $A_i(x) \in R$ so that $\deg(A_i) < \deg(P_i)$ for $i = 1, \ldots, k$ then CRT $\implies$ if $P(x) = \prod P_i(x)$ then $\exists Q(x) \in R$ s.t. $Q(x) = A_i(x) \mod P_i, \forall i$.

There is a unique such Q satisfying the congruences where $\deg Q < \deg P$.

In this context, we can find Q explicitly. Let

$$Q_i = \frac{P(x)}{P_i(x)} = \prod_{j \neq i} P_j(x) \tag{114}$$

What is the partial fraction decomposition of

$$\frac{1}{P(x)} = \frac{1}{\prod P_i(x)} = \sum_i \frac{S_i(x)}{P_i(x)} \tag{115}$$

where $\deg(S_i) < \deg(P_i)$. So

$$\frac{1}{P(x)} = \sum \frac{S_i(x)}{P_i(x)} = \sum \frac{S_i(x) Q_i(x)}{P(x)} \tag{116}$$

$$1 = \sum S_i(x) Q_i(x) \tag{117}$$

This is like a partition of unity. Consider the sum

$$\sum_i A_i(x) S_i(x) Q_i(x) = A_j(x) + \sum_{i \neq j} (A_i(x) - A_j(x)) S_i(x) Q_i(x) \tag{118}$$

Lagrange Interpolation: Given distinct $x_1, \cdots, x_k \in \mathbb{F}$, and $a_1, \ldots, a_k \in \mathbb{F}$ we can find a $Q(x) \in \mathbb{F}[x]$ s.t. $Q(x_i) = a_i, \forall i$ we can find a unique such Q with $\deg(Q) < k$.

Let $P_i(x) = (x - a_i)$, and $P = \prod P_i$ and $Q_i = P/P_i$ Then,

$$\frac{1}{P(x)} = \frac{1}{\prod (x - x_i)} = \sum \frac{1}{(x - x_i) Q_i(x_i)} = \frac{1}{P(x)} \sum \frac{Q_i(x)}{Q_i(x_i)} \tag{119}$$

So,

$$1 = \sum \frac{Q_i(x)}{Q_i(x_i)} \tag{120}$$

and

$$Q(x) = \sum_{i=1}^{k} \frac{a_i Q_i(x)}{Q_i(x_i)} \tag{121}$$

This work because for x_i, the i term goes to a_i and the $j \neq i$ term is 0.