MA3K4 Introduction to group theory :: Lecture notes

Lecturer: Gareth Tracey

November 28, 2023

Contents

Week 1, lecture 1 starts here

1 Introduction

Definition 1.0.1. A *group* is a pair $(G, \circ)$ where G is a set and $\circ : G \times G \to G$ is a binary operation satisfying

1. Associativity: $(g \circ h) \circ k = g \circ (h \circ k)\ \forall g, h, k \in G$,
2. Identity: $\exists$ an element in G, denoted 1_G, such that $1_G \circ g = g \circ 1_G = g\ \forall g \in G$,
3. Inverses: $\forall g \in G$, $\exists$ an element in G, denoted g^{-1}, such that $g \circ g^{-1} = g^{-1} \circ g = 1_G$.

Remark. Implicit in parts 1 and 2 of above definition are

1. An identity element in an associative binary operation is unique, justifying the notation and the 'the' before 'identity'
2. Similarly, inverses are unique in an associative binary operation, so we say *the* inverse of g

The number of elements in a group $(G, \circ)$ is called the order of G, denoted $|G|$.

Example 1.0.2. Let $G = \mathbb{Z}$. Then

1. If we define $\circ : G \times G \to G$ by $g \circ h = g + h$ for $g, h \in \mathbb{Z}$ then we know $(G, \circ)$ is a group and $1_G = 0,\ g^{-1} = -g\ \forall g \in G$.
2. For the same set, if we define $g \circ h = g \times h$ then $(G, \circ)$ is not a group for lack of inverses for $g \in \mathbb{Z} \backslash \{\pm 1\}$.

Remark.

1. You may have been given a fourth axiom, closure, in previously seen definitions of a group. The reason we omit that here is because it's implied by definition of binary operation.
2. If $(G, \circ)$ is a group, $\circ$ is often called the *group operation*.
3. Given clear context, we will streamline our notation and simply write G in place of $(G, \circ)$ and gh in place of $g \circ h$.

Definition 1.0.3. Let G be a group.

1. If $g, h \in G : gh = hg$ then g and h *commute*.
2. If g and h commute $\forall g, h \in G$ then G is *abelian*.

Example 1.0.4. $(\mathbb{Z}, +)$ is abelian.

Exercise 1.0.5 (Commuting elements in groups)**.** Let G be a group.

1. Suppose $g^2 = 1_G\ \forall g \in G$. Show that G is abelian.

   Proof. Note that this implies $\forall g, h \in G,\ (gh)^{-1} = gh$, but $(gh)^{-1} = h^{-1}g^{-1} = hg$, so $gh = hg$. □

2. Suppose $g^3 = 1_G \ \forall g \in G$. Show that hgh^{-1} and g commute $\forall g, h \in G$.

   Proof. One has $g^2h = g^{-1}h^{-2} = (h^2g)^{-1} = h^2gh^2g \Rightarrow gh^2g = hg^2h \Rightarrow hgh^2g = h^2g^2h$. Now consider $(gh)^{-1}$, which equals h^2g^2 but also $ghgh$. Hence $ghgh^{-1} = ghgh^2 = h^2g^2h = hgh^2g = hgh^{-1}g$, as desired. □

Next, we are going to look at two infinite families of examples of groups: 1. Symmetric groups and 2. Linear groups.

1.1 Symmetric group

Definition 1.1.1. Let X be a set, and define

$$\mathrm{Sym}(X) = \{f : f : X \to X \text{ is a bijection}\}$$

Define $\circ : \mathrm{Sym}(X) \times \mathrm{Sym}(X) \to \mathrm{Sym}(X)$ to be the usual composition of functions. Then $(\mathrm{Sym}(X), \circ)$ is a group, called the *symmetric group* on X. An element of $\mathrm{Sym}(X)$ is called a *permutation*.

Remark (Sanity check)**.** 1. Associativity is clear by inheritance

2. $1_G = \mathrm{id}_X : x \mapsto x$

3. For $f \in \mathrm{Sym}(X)$, $x \in X$, choose a unique $y_x \in X$ such that $f(y_x) = x$. Define $g : X \to X$ by $g(x) = y_x$, then g is a inverse for f.

We introduce cycle notation as a more compact way of writing permutations down.

Week 1, lecture 2 starts here

Definition 1.1.2 (Cycle notation)**.** Let X be a set.

1. Let $a_1, \dots, a_n \in X$ be distinct. The permutation $f = (a_1, \dots, a_n) \in \mathrm{Sym}(X)$ is defined to be $f(a_i) = a_{i+1}$ for $1 \leq i \leq n-1$, $f(a_n) = a_1$, and $f(b) = b$ for $b \notin \{a_1, \dots, a_n\}$. We call f a *cycle of length* n (or an n-cycle).

2. Two cycles $(a_1, \dots, a_r)$, $(b_1, \dots, b_s)$ are *disjoint* if $\{a_1, \dots, a_r\} \cap \{b_1, \dots, b_s\} = \varnothing$.

3. The *empty cycle*, written $()$, is the identity map which is also $1_{\mathrm{Sym}(X)}$.

Remark (Important points about cycles)**.** 1. Perhaps a tautology, but the empty cycle is thought of as a cycle (of length 0).

2. Recall that the group operation is composition of functions. So $fg : X \to X$ means do g first and then f. e.g. $X = \{1, 2, 3, 4, 5\}$, so $(3, 4, 1, 2)(4, 5) = (1, 2, 3, 4, 5)$.

3. Cycle notation is not unique in the following sense: two distinct m-tuples of elements in a set X can represent the same cycle, e.g. $(1, 2, 3, 4, 5) = (3, 4, 5, 1, 2)$.

Theorem 1.1.3. Let X be a finite set. Then

1. $|\mathrm{Sym}(X)| = |X|!$,

2. Every element $F \in \mathrm{Sym}(X)$ can be written as product of disjoint cycles. Moreover, the decomposition is unique in the sense that if $F = f_1 \cdots f_r = g_1 \cdots g_s$ where f_i, g_i are disjoint cycles of length > 1, then $r = s$ and $\{f_1, \ldots, f_r\} = \{g_1, \ldots, g_r\}$.

Proof (nonexaminable). 1. Write $X = \{x_1, \ldots, x_r\}$ where $n = |X|$ and define

$$X(n) := \{(a_1, \ldots, a_n) : a_i \in X, a_i \neq a_j \text{ for } i \neq j\}.$$

Define a bijection $\theta : \mathrm{Sym}(X) \to X(n)$ by $\theta(f) = (f(x_1), \ldots, f(x_n))$. for $f \in \mathrm{Sym}(X)$, observe

(a) θ is well-defined, since f is a bijection, so $f(x_i) \neq f(x_j)$ for $i \neq j$.

(b) In the same way, θ is injective. Indeed, if $\theta(f) = \theta(g)$ then $f(x_i) = g(x_i)$ $\forall i$ by definition of θ, so $f = g$.

(c) If $(a_1, \ldots, a_n) \in X(n)$, then define $f : X \to X$ by $f(x_i) = a_i$ for $1 \leq i \leq n$. Clearly, $f \in \mathrm{Sym}(X)$ and $\theta(f) = (a_1, \ldots, a_n)$, so θ is surjective.

It follows that $|\mathrm{Sym}(X)| = |X(n)| = n!$.

2. Let $f \in \mathrm{Sym}(X)$. If $f = \mathrm{id}_X$ then $f = ()$ so it's a cycle. Now suppose f is not id_X. Let $Y = \{x \in X : f(x) \neq x\}$. Note that since $|\mathrm{Sym}(X)|$ is finite by 1., $\exists n \in \mathbb{N}$ such that $f^n = \mathrm{id}_X$.

In particular, if we fix $a_1 \in Y$, then we may define $m_1 := \min\{m \in \mathbb{N} : f^m(a_1) = a_1\}$ since the set is nonempty. Now, for $2 \leq i \leq m_1$, define $a_i := f(a_{i-1})$. If $Y = \{a_1, \ldots, a_{m_1}\}$, then by definition of cycle, one has $f = (a_1, \ldots, a_m)$.

Now suppose $Y \backslash \{a_1, \ldots, a_{m_1}\} \neq \varnothing$. Choose $a_{m_1+1} \in Y \backslash \{a_1, \ldots, a_{m_1}\}$, and define $m_2 := \min\{m \in \mathbb{N} : f^m(a_{m_1+1}) = a_{m_1+1}\}$. For $m_1 + 2 \leq i \leq m_2$, again define $a_i := f(a_{i-1})$, then if $Y = \{a_1, \ldots, a_{m_1}, a_{m_1+1}, \ldots, a_{m_2}\}$, one has $f = (a_1, \ldots, a_m)(a_{m+1}, \ldots, a_{m_2})$. If not, we continue inductively. Since X is finite, this must terminate, and when it does f will be a product of disjoint cycles. The uniqueness follows from the algorithm immediately.

□

1.2 Linear group

Definition 1.2.1. F is a field and $n \in \mathbb{N}$. We define

$$GL_n(F) := \{A : A \text{ an invertible } n \times n \text{ matrix over } F\},$$

a group with matrix multiplication as operation. This is called *general linear group* of dimension n over F.

Week 1, lecture 3 starts here

Remark (Useful things from Algebra I, II for studying general linear groups). 1. Each field F has an additive and multiplicative identity 0_F and 1_F. Given clear context, they will be denoted simply 0 and 1 respectively.

2. An $n \times n$ matrix A over F is invertible iff $\det A \neq 0$ iff rows (or columns) of A are linearly independent.

3. If F is a finite field, then $|F| = p^f$ for some prime p and $f \in \mathbb{N}$. Moreover, for each prime p and each $f \in \mathbb{N}$, $\exists!$ a field (up to isomorphism) $F : |F| = p^f$. p is called the *characteristic* of F, and satisfies that $p\alpha = 0 \ \forall \alpha \in F$.

4. If F is a field then $F^\times := F\backslash\{0\}$ is a group with multiplication as group operation inherited from F.

Exercise 1.2.2. 1. Let X be a set. Show that $\mathrm{Sym}(X)$ is abelian iff $|X| \leq 2$.

2. Let F be a field. Show that $GL_n(F)$ is abelian iff $n = 1$.

Theorem 1.2.3. Let F be a finite field with $|F| = q$. Then $|GL_n(F)| = q^{\binom{n}{2}} \displaystyle\prod_{i=1}^{n}(q^i - 1)$.

Proof (nonexaminable). See sheet 1. ☐

1.3 Order of elements

Definition 1.3.1. The *order* of $g \in G$, denoted $|g|$, is defined $|g| := \min\{n \in \mathbb{N} : g^n = 1_G\}$. If the set is $\varnothing$ then $|g| := \infty$.

Example 1.3.2. 1. Let X be a set and let $f = (a_1, \dots, a_m) \in \mathrm{Sym}(X)$. Then $|f| = m$.

2. Let F be a finite field of order p^f where p prime, $G = GL_2(F)$, and $\alpha, \beta \in F^\times$. Observe that
$$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha+\beta \\ 0 & 1. \end{pmatrix}$$
So if $g = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ then $g^n = \begin{pmatrix} 1 & n\alpha \\ 0 & 1 \end{pmatrix}$, so $|g| \mid p$ (we'll see later about this implication), so $|g| = p$.

   Also,
$$g^n = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}^n = \begin{pmatrix} \alpha^n & 0 \\ 0 & \beta^n. \end{pmatrix}$$
So $|g| = \mathrm{lcm}\ (m, k)$ where $m = |\alpha|$ and $k = |\beta|$ as elements of $F^\times$.

Remark. 1. For $g \in G$, $(g^n)^{-1} = \left(g^{-1}\right)^n$, so we write $g^{-n} := \left(g^{-1}\right)^n$. In particular, $\left|g^{-1}\right| = |g|$.

2. If $g \in G$, $n = |g|$ and $n \mid l$, then $g^l = 1$.

Lemma 1.3.3. Let $a, b \in G$ of finite order. Then

1. If $l \in \mathbb{N}$, then $a^l = 1$ iff $|a| \mid l$.

2. Let $m \in \mathbb{N}$, then $|a^m| = \dfrac{|a|}{\gcd(|a|, m)}$.

3. If a, b commute then $|ab| \mid \mathrm{lcm}\ (|a|, |b|)$.

4. If a, b commute and $a^i = b^j \ \forall i, j \in \mathbb{N}$ only when they are both 1 (i.e. $\langle a \rangle \cap \langle b \rangle = \{1\}$) then $|ab| = \mathrm{lcm}\ (|a|, |b|)$.

Proof. 1. $\Leftarrow$ is mentioned. $\Rightarrow$: suppose $a^l = 1$. By Euclidean division, we can write $l = q|a|+r$ for some $r \in [0, |a|)$. Then $1 = a^l = a^{q|a|+r} = a^r$, which contradicts minimality of $|a|$.

2. Suppose first that $m \mid |a|$. Then one can write $|a| = ms$, so $a^{ml} = 1 \Leftrightarrow |a| \mid ml$ by 1 $\Leftrightarrow \dfrac{|a|}{m} \mid l$. Hence the least positive integer $l : a^{ml} = 1$ is $\dfrac{|a|}{m}$.

   Now let $k = \gcd(|a|, m)$. We write $m = ks$, then $a^{m\frac{|a|}{k}} = a^{|a|s} = 1$, and by 1 one has $|a^m| \mid \frac{|a|}{k}$. To complete the proof it suffices to show that $\frac{|a|}{k} \leq |a^m|$.

   Week 2, lecture 1 starts here

   By Bézout's lemma, $\exists s, t \in \mathbb{Z} : k = s|a| + tm$, so $a^k = a^{s|a|+tm} = (a^{|a|})^s a^{tm} = a^{tm}$. Then $a^{tm|a^m|} = ((a^m)^{|a^m|}))^t = 1^t = 1$. This implies $|a^{tm}| \mid a^m$ by 1. So $\frac{|a|}{k} = |a^k| = |a^t m| \mid |a^m|$.

3. Let $l := \text{lcm } (|a|, |b|)$. Then $(ab)^l = a^l b^l = 1 \times 1 = 1$, so by 1. $|ab| \mid l$.

4. Let $k := |ab|$. Then $k \mid l$, but also, $1 = (ab)^k = a^k b^k$ so $a^k = \left(b^{-1}\right)^k$ and by assumption both sides are 1. So $|a|, |b| \mid k$, so $l \mid k$, hence $k = l$.

$\square$

Exercise 1.3.4. 1. Let $h, g \in G$. Show that $\left|hgh^{-1}\right| = |g|$.

2. Let $l, m, n > 2 \in \mathbb{N}$. Show that $\exists G$ with $a, b \in G : |a| = l,\ |b| = m,\ |ab| = n$. Also:

   (a) Show that G can be finite.

   (b) Show that one can replace $l, m, n > 2$ by $l, m, n > 1$.

   Key hint: A 2×2 matrix over $\mathbb{C}$ with distinct eigenvalues is diagonalisable. Now exploit result of 1st exercise.

1.4 Subgroup and coset

Definition 1.4.1. A nonempty $H \subseteq G$ is a *subgroup* of G, denoted $H \leq G$, if

1. $1_G \in H$
2. $h \in H \Rightarrow h^{-1} \in H$
3. $h_1, h_2 \in H \Rightarrow h_1 h_2 \in H$

Definition 1.4.2. For a group G and $g \in G$, define $\langle g \rangle := \{g^n : n \in \mathbb{Z}\}$ which is called the *cyclic subgroup of G generated by g*. If $G = \langle g \rangle$ then G is *cyclic* and g is a *generator* for G.

Lemma 1.4.3. $H \subseteq G$ where H nonempty. $H \leq G \Leftrightarrow h_1 h_2 \in H \Rightarrow h_1 h_2^{-1} \in H$

Proof. $\Rightarrow$ $h_1, h_2 \in H \Rightarrow h_2^{-1} \in H \Rightarrow h_1 h_2^{-1} \in H$.

$\Leftarrow$
1. $H \neq \varnothing \Rightarrow h \in H \Rightarrow hh^{-1} \in H \Rightarrow 1_G \in H$
2. $h \in H \Rightarrow 1_G h^{-1} = h^{-1} \in H$
3. $h_1, h_2 \in H \Rightarrow h_2^{-1} \in H \Rightarrow h_1 (h_2^{-1})^{-1} h_1 h_2 \in H$

$\square$

Example 1.4.4. Let $G = GL_2(F)$ and

$$H = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} : \alpha, \beta \in F^\times \right\} \subseteq G. \qquad \text{sometimes called diagonal subgroup}$$

We want to show this is indeed a subgroup. Let $h_i = \begin{pmatrix} \alpha_i & 0 \\ 0 & \beta_i \end{pmatrix} \in H$ where $i = 1, 2$. Then

$$h_1 h_2 = \begin{pmatrix} \alpha_1 & 0 \\ 0 & \beta_2 \end{pmatrix} \begin{pmatrix} \alpha_2^{-1} & 0 \\ 0 & \beta_2^{-1} \end{pmatrix} = \begin{pmatrix} \alpha_1 \alpha_2^{-1} & 0 \\ 0 & \beta_1 \beta_2^{-1} \end{pmatrix} \in H.$$

Definition 1.4.5. Let $A \subseteq G$ be nonempty. The *subgroup of G generated by A*, denoted $\langle A \rangle$, is

$$\{a_1^{\varepsilon_1} \cdots a_m^{\varepsilon_m} : m \in \mathbb{N},\ a_i \in A,\ \varepsilon_i = \{\pm 1\}\}.$$

Notation. If $A = \{g_1, \ldots, g_t\}$ then we often write $\langle A \rangle$ as $\langle g_1, \ldots, g_t \rangle$.

Week 2, lecture 2 starts here

Exercise 1.4.6. Let G be a group and $A \subseteq$ nonempty.

1. Use Lemma 1.4.3 to show that $\langle A \rangle$ is indeed a subgroup of G.
2. Write $A = \{g_1, \ldots, g_s\}$ and suppose $g_i g_j = g_j g_i$ $\forall i, j = 1, \ldots, s$. Show that $|\langle A \rangle| \leq \prod_{i=1}^{s} |g_i|$.
3. Suppose $g^p = 1$ $\forall g \in G$ and $G = \langle x, y \rangle$ for some $x, y \in G$.
   (a) Show that if $p = 2$, $|G| \leq 4$.
   (b) Show that if $p = 3$, $|G| \leq 3^4$.
   (c) Fields-medal-worth: If $p = 5$, is G finite?

Definition 1.4.7. The *left coset* of $H \leq G$ with respect to $g \in G$ is the set $gH := \{gh : h \in H\}$. The *right coset* is defined similarly.

gH is not a subgroup unless $g \in H$ since in general the identity is not there.

Lemma 1.4.8. Let $H \leq G$ and $g, k \in G$. The following are equivalent:

1. $k \in gH$
2. $kH = gH$
3. $g^{-1}k \in H$

Proof. First note that if $h \in H$ then $hH = H$ by virtue of the fact $H \leq G$.
Now $k \in gH \Rightarrow k = gh$ for some $h \in H \Rightarrow kH = ghH = gH$, so 1 implies 2. The other two implications are almost identical. □

Lemma 1.4.9. Let $H \leq G$. For $g_1, g_2 \in G$, say that $g_1 \sim_H g_2 \Leftrightarrow g_1 H = g_2 H$. Then $\sim_H$ is an equivalence relation.

Proof. The three conditions reflexivity, symmetry and transitivity follow immediately from definition. □

Corollary 1.4.10. Let $H \leq G$.

1. If $g_1, g_2 \in G$, then either $g_1H = g_2H$ or $g_1H \cap g_2H = \varnothing$.
2. The set $\{gH : g \in G\}$ of left cosets is a partition of G, i.e. if g_iH for $i \in I$ are distinct left cosets of H in G then
$$G = \bigsqcup_{i \in I} g_iH.$$

Proof. $\{gH : g \in G\}$ is precisely the set of equivalence classes under $\sim_H$, so the results follow immediately. □

Theorem 1.4.11 (Lagrange's)**.** Let G be a finite group and $H \leq G$. Then $|H| \mid |G|$.

Proof. Let $g_1H, \ldots, g_tH$ be distinct left cosets of H in G. By Corollary 1.4.10,
$$|G| = \left| \bigsqcup_{i=1}^{t} g_iH \right| = \sum_{i=1}^{t} |g_iH|,$$
and one also has $|gH| = |H| \ \forall g \in G$ since $gH \to H$ defined by $gh \mapsto h$ is a bijection. Hence $|G| = t|H|$. □

Definition 1.4.12. 1. As in the context of above, we write $G/H := \{gH : g \in G\}$.

2. $|G/H|$ is called *index* of H in G, denoted $|G : H|$. By Lagrange's theorem if G is finite then $|G : H| = \frac{|G|}{|H|}$.

Corollary 1.4.13. If G is finite and $g \in G$, then $|g| \mid |G|$.

Proof. This follows from the fact $|\langle g \rangle| = |g|$ and Lagrange's theorem. □

1.5 Normal subgroup and quotient group

In general G/H is not a group, which is the motivation of this section.

Lemma 1.5.1. Let $H \leq G,\ g \in G$. Then $gHg^{-1} = \left\{ghg^{-1} : h \in H\right\} \leq G$.

Proof. We use Lemma 1.4.3. Clearly $gHg^{-1} \neq \varnothing$ since $1_G \in gHg^{-1}$. Now let $x = gh_1g^{-1},\ y = gh_2g^{-1}$ where $h_1, h_2 \in H$. Note that $h_1h_2 \in H$ since $H \leq G$. Then $y^{-1} = gh_2^{-1}g^{-1}$ so
$$xy^{-1} = gh_1g^{-1}gh_2^{-1}g^{-1} = gh_1h_2^{-1}g^{-1} \in gHg^{-1}.$$
□

Definition 1.5.2. 1. $H \leq G$ is *normal* in G if $gHg^{-1} = H \ \forall h \in H$, denoted $N \trianglelefteq G$.

2. The *normaliser* of $H \leq G$ is defined as
$$N_G(H) := \{g \in G : gHg^{-1} = H\}.$$

Exercise 1.5.3. 1. If $H \leq G$, show that $N_G(H) \leq G$.

2. $\{1_G\}, G$ are always normal.

Definition 1.5.4. G is *simple* if $\{1_G\}$ and G are the only normal subgroups of G.

Example 1.5.5.
- $\mathbb{Z}/p\mathbb{Z}$ for any prime p (by Lagrange's)
- A_n for $n \geq 5$

Notation. $AB := \{ab : a \in A, b \in B\}$ where $A, B \subseteq G$. It's a subset but not a subgroup of G in general, even if $A, B \leq G$.

Lemma 1.5.6. Let $N \trianglelefteq G$ and $g, h \in G$. Then $(gN)(hN) = ghN$.

Proof. $\subseteq$: Let $x = gn_1 \in gN,\ y = hn_2 \in hN$ where $n_{1,2} \in N$. Then

$$xy = gn_1hn_2 = ghh^{-1}n_1hn_2 \in ghN$$

since $h^{-1}n_1h \in N$ by definition of a normal subgroup.

$\supseteq$: Let $x = ghn \in ghN$ where $n \in N$. Then

$$x = (g1_G)(hn) \in (gN)(hN).$$

□

Definition 1.5.7. Let $N \trianglelefteq G$.

1. The *natural binary operation* on G/N is $\circ : G/N \times G/N \to G/N$ given by $(gN) \circ (hN) = ghN$.
2. $(G/N, \circ)$ is a group, called the *quotient of G by N*.

Checking this is indeed a group is left as an exercise.

1.6 Homomorphism

Definition 1.6.1.
1. A map $\theta : G \to H$ is a *homomorphism* if $\theta(g_1g_2) = \theta(g_1)\theta(g_2)\ \forall \theta_{1,2} \in G$.
2. A bijective homomorphism is an *isomorphism*. If for G, H, $\exists \theta : G \to H$ an isomorphism, then G and H are *isomorphic*, denoted $G \cong H$.
3. Let $\theta : G \to H$ be a homomorphism. The *kernel* of θ, denoted $\ker\theta$, is defined to be $\{g \in G : \theta(g) = 1_H\}$, which is a subgroup of G. The *image* of θ, denoted $\operatorname{im}\theta$, is defined to be $\{\theta(g) : g \in G\}$.

Example 1.6.2. Let F be a field, $G = GL_n(F)$ and $H = F^\times$. Then $\det G \to H$ is a (surjective) homomorphism, since $\det AB = \det A \det B\ \forall A, B \in GL_n(F)$. Also

$$\ker\det = \{A \in GL_n(F) : \det A = 1_F\} =: SL_n(F).$$

Theorem 1.6.3 (1st isomorphism theorem)**.** Let $\theta : G \to H$ be an homomorphism. Then

1. $\ker\theta \trianglelefteq G$.
2. $\operatorname{im}\theta \leq H$.

3. $G/\ker\theta \cong \operatorname{im}\theta$.

Theorem 1.6.4 (2nd isomorphism theorem)**.** Let $H \leq G$ and $N \trianglelefteq G$. Then

1. $HN = NH \leq G$.
2. $H \cap N \trianglelefteq H$.
3. $HN/N \cong H/(H \cap N)$.

Theorem 1.6.5 (3rd isomorphism theorem)**.** Let $N, K \trianglelefteq G : N \leq K$. Then

$$K/N \trianglelefteq G/N \quad \text{and} \quad (G/N)/(K/N) \cong G/K.$$

Theorem 1.6.6 (Correspondence (or 4th isomorphism) theorem)**.** Let $N \trianglelefteq G$. Then the map

$$f : \{J : N \leq J \leq G\} \to \{X : X \leq G/N\}$$

given by

$$J \mapsto J/N$$

is a bijection.

Proof. Let $A := \{J : N \leq J \leq G\}$ and $B := \{X : X \leq G/N\}$. Clearly $J/N \leq G/N$.
Suppose $J_{1,2} \in A$ and $f(J_1) = f(J_2)$, and let $x \in J_1$. Then

$$xN \in f(J_1) = f(J_2) = J_2/N,$$

so $xN = yN$ for some $y \in J_2$. Since $x \in xN$, $x = yn \in J_2$ for some $n \in N$. It follows that $J_1 \subseteq J_2$, and symmetrically $J_2 \subseteq J_1$. Hence f is injective.
Let $X \in B$ and set $Y = \{y \in G : yN \in X\}$. One can see that $Y \leq G$ since $y_{1,2}N \in X \Rightarrow (y_1N)(y_2N)^{-1} \in X \Rightarrow y_1y_2^{-1}N \in X$, so $y_1y_2^{-1} \in Y$ by definition, hence $Y \leq G$. Since $N \leq Y$ ($nN = N = 1_{G/N} \in X\ \forall n \in N$) one has $y \in A$. Since $f(Y) = X$, f is surjective. $\square$

Week 3, lecture 1 starts here

2 Group action

2.1 Permutation group

Definition 2.1.1. Let X be a set. $G \leq \operatorname{Sym}(X)$ is called a *permutation group* on X.

Definition 2.1.2.

1. Let $g \in \operatorname{Sym}(X)$. The *support* of g is defined

$$\operatorname{supp}(g) := \{x \in X : g(x) \neq x\} \subseteq X.$$

2. Let $G \leq \operatorname{Sym}(X)$. The *support* of G is defined

$$\operatorname{supp}(G) := \{x \in X : g(x) \neq x \text{ for some } g \in G\} \subseteq X.$$

Example 2.1.3.

1. $\operatorname{supp}(\operatorname{Sym}(X)) = X$.
2. $\operatorname{supp}(\{1_G\}) = \varnothing$.

3. $X = \{1,2,3,4,5,6\}$ and $g = (1,5,6)$. Then $\mathrm{supp}(g) = \{1,5,6\}$.
4. $X = \{1,2,3,4,5\}$ and $g = (1,2)(3,5)$. Then $\mathrm{supp}(g) = \{1,2,3,5\}$.

Remark. As the above examples show, one can read off the support of $g \in \mathrm{Sym}(X)$ from its decomposition as a product of disjoint cycles. More precisely, if $f \in \mathrm{Sym}(X)$, $f = f_1 \dots f_m$ is such decomposition where $f_i = \left(a_{i_1}, \dots, a_{i_{t_i}}\right)$. Then

$$\mathrm{supp}(f) = \{a_{i_j} : 1 \le i \le m,\ 1 \le j \le t_i\}.$$

Exercise 2.1.4. Let $H, G \le \mathrm{Sym}(X)$.

1. Show that $H \le G \Rightarrow \mathrm{supp}(H) \subseteq \mathrm{supp}(G)$.
2. Deduce that $\mathrm{supp}(H) \cap \mathrm{supp}(G) \Rightarrow H \cap G = \{1_{\mathrm{Sym}(X)}\}$.
3. Is the converse of above true?

   No, counterexample: $X = \{1,2,3\}$, $G = \langle (1,2) \rangle$, $H = \langle (2,3) \rangle$.
4. What if $gh = hg\ \forall g \in G, h \in H$?

Theorem 2.1.5. 1. Disjoint cycles commute.

2. Let $f \in \mathrm{Sym}(X)$ and $f = f_1 \dots f_m$ as a product of disjoint cycles f_i. If $m = 1$ then $|f|$ is length of f_1. If $m \ge 2$ then $|f| = \mathrm{lcm}\left(|f_1|, \dots, |f_m|\right)$.
3. If $f = (a_1, \dots, f_r) \in \mathrm{Sym}(X)$ is a cycle and $g \in \mathrm{Sym}(X)$, then ${}^g f := gfg^{-1} = (g(a_1), \dots, g(a_r))$.

Proof (nonexaminable). 1. Let $f = (a_1, \dots, a_r)$, $g = (b_1, \dots, b_s)$ be disjoint cycles. One needs to prove $(f \circ g)(x) = (g \circ f)(x)\ \forall x \in X$.

   Suppose $x \in \{a_1, \dots, a_r\}$, which implies $x \ne b_i$ by assumption. So $g(x) = x$ by definition of cycles, hence $f(g(x)) = f(x)$. Also, again by definition, $f(x) \in \{a_1, \dots, a_r\}$, so $f(x) \ne b_i$, hence $g(f(x)) = f(x)$. The argument for case $x \notin \{a_1, \dots, a_r\}$ is symmetric.

2. The case $m = 1$ is seen before in section 1.3. We prove the claim by induction on m. Suppose $m \ge 2$ and all precedents are true. Let $g = f_1 \dots f_{m-1}$. We now need three things to finish the proof:

   (a) Write $f_i = (a_{i_1}, \dots, a_{i_{t_i}})$. Then $\mathrm{supp}(g) = \{a_{i_j} : 1 \le i \le m-1,\ 1 \le j \le t_i\}$ and $\mathrm{supp}(f_m) = \{a_{m_j} : 1 \le j \le t_m\}$. By assumption $\mathrm{supp}(g) \cap \mathrm{supp}(f_m) = \varnothing$, so $\langle g \rangle \cap \langle f_m \rangle = \{1_{\mathrm{Sym}(X)}\}$ by exercise above.

   (b) g and f_m commute by 1.

   (c) $|g| = \mathrm{lcm}\left(|f_1|, \dots, |f_{m-1}|\right)$ by inductive hypothesis.

   By Lemma 1.3.3.4 one has the desired.

3. Let $b_i := g(a_i)$ and observe that $(gfg^{-1})(b_i) = gfg^{-1}(g(a_i)) = g(f(a_i)) = g(a_{i+1}) = b_{i+1}$. Now let $x \in X \backslash \{b_1, \dots, b_m\}$. Then $g^{-1}(x) \in X \backslash \{g^{-1}(b_1), \dots, g^{-1}(b_m)\}$ since g is a bijection, i.e. $g^{-1}(x) \in X \backslash \{a_1, \dots, a_m\}$, so $f(g^{-1}(x)) = g^{-1}(x)$, and $gfg^{-1}(x) = g(g^{-1}(x)) = x$.

$\square$

Week 3, lecture 2 starts here

Recall that a subgroup of G generated by a nonempty $A \subseteq G$ is defined to be

$$\langle A \rangle := \{a_1^{\varepsilon_1} \cdots a_m^{\varepsilon_m} : m \in \mathbb{N},\ \varepsilon_i \in \{\pm 1\},\ a_i \in A\}.$$

Exercise 2.1.6. Let $A \subseteq G$ be nonempty.

1. Show that
$$\langle A \rangle = \bigcap_{A \subseteq H \leq G} H.$$
In particular, if $H \leq G$ and $A \subseteq H$ then $\langle A \rangle \leq H$.

2. Recall that given $H \leq G$, $N_G(H) := \{g \in G : gHg^{-1} = H\}$. Suppose $g \in G$ and $gag^{-1} \in \langle A \rangle\ \forall a \in A$. Show that $g \in N_G(\langle A \rangle)$. (One only needs to check element in generating set instead of the whole subgroup for normaliser.)

Definition 2.1.7. Let $n \in \mathbb{N}$, $n \geq 3$ and set $X := \{1, \ldots, n\}$. Define $\sigma, \tau \in \mathrm{Sym}(X)$ by $\sigma := (1, 2, \ldots, n)$ and $\tau = \prod_{i=1}^{\lfloor n/2 \rfloor}(i, n-i+1) = (1, n)(2, n-1) \cdots$. The *dihedral group of order* $2n$ is the permutation group on X defined by $D_{2n} := \langle \sigma, \tau \rangle$.

This is the rigorous (algebraic) definition of D_{2n}, but it can also be thought of group of symmetries of a regular n-gon.

Example 2.1.8.
1. $n = 8,\ \sigma = (1, 2, 3, 4, 5, 6, 7, 8),\ \tau = (1, 8)(2, 7)(3, 6)(4, 5)$.
2. $n = 7,\ \sigma = (1, 2, 3, 4, 5, 6, 7),\ \tau = (1, 7)(2, 6)(3, 5)$.

Theorem 2.1.9. Let $n \in \mathbb{N},\ n \geq 3$.

1. $|D_{2n}| = 2n$.
2. $N := \langle \sigma \rangle \trianglelefteq D_{2n}$ and $|N| = n$.

Proof.
1. See sheet 2.
2. First note that $\tau\sigma\tau^{-1} = (\tau(1), \ldots, \tau(n)) = (n, n-1, \ldots, 1) = \sigma^{-1}$ by Theorem 2.1.5.3 and definition of τ. Also clearly $\sigma\sigma\sigma^{-1} = \sigma$. Now if $A := \{\sigma\}$ then we have shown ${}^{\tau}\sigma, {}^{\sigma}\sigma \in \langle A \rangle$, so by Exercise 2.1.6.2, $\tau, \sigma \in N_{D_{2n}}(\langle A \rangle)$. Hence $\langle \{\tau, \sigma\} \rangle = D_{2n} \subseteq N_{D_{2n}}(\langle A \rangle)$, i.e. $\langle A \rangle \trianglelefteq D_{2n}$. Also $|N| = |\langle \sigma \rangle| = |\sigma| = n$.

$\square$

Definition 2.1.10. Let X be a finite set.

1. Let $f \in \mathrm{Sym}(X)$ and write $f = f_1 \cdots f_m$ as product of disjoint cycles. f is *even* if the number of cycles of even length in $\{f_1, \ldots, f_m\}$ is even. Otherwise f is *odd*.
2. The *alternating group on* X, denoted $\mathrm{Alt}(X)$, is defined $\{f : f \in \mathrm{Sym}(X) \text{ even}\}$.

Example 2.1.11. $(1, 2, 3, 4) \in S_4$ is odd, $(1, 2)(3, 4, 5) \in S_5$ is odd, $(1, 2)(3, 4, 5, 6) \in S_6$ is even.

Proposition 2.1.12. $\mathrm{Alt}(X) \leq \mathrm{Sym}(X)$ and $[\mathrm{Sym}(X) : \mathrm{Alt}(X)] = 2$, i.e. $|\mathrm{Alt}(X)| = \frac{|X|!}{2}$.

Proof. See sheet 2. $\square$

Proposition 2.1.13. If X, Y are finite sets with $|X| = |Y|$, then $\mathrm{Sym}(X) \cong \mathrm{Sym}(Y)$.

Proof. Let $\beta : X \to Y$ be a bijection. Define $\theta : \mathrm{Sym}(X) \to \mathrm{Sym}(Y)$ by $f \mapsto \beta f \beta^{-1}$. It's then clear that θ is an isomorphism. $\square$

Week 3, lecture 3 starts here

Recall that if $G = \langle B \rangle,\ H = \langle A \rangle$, then $H \trianglelefteq G \Leftrightarrow bab^{-1} \in H\ \forall a \in A, b \in B$.

2.2 Group action

Definition 2.2.1. Let G be a group and X a set. An *action* of G on X is a map $\cdot : G \times X \to X$ such that

1. $1_G \cdot x = x \quad \forall x \in X$
2. $(gh) \cdot x = g \cdot (h \cdot x) \quad \forall g, h \in G,\ x \in X$

We say G *acts on* X and X is a a G*-set*.

Example 2.2.2. 1. The action of G on itself by left multiplication: let $X := G$ and define $\cdot : G \times X \to X$ by $g \cdot x := gx,\ g \in G,\ x \in X$. Note that by definition of a group,

   (a) $1_G \cdot x = 1_G x = x \quad \forall x \in X$,

   (b) $(gh) \cdot x = (gh)x = g(hx) = g \cdot (h \cdot x) \quad \forall g, h \in G,\ x \in X$.

2. The action of G on itself by conjugation: again let $X := G$. Define $\cdot : G \times X \to X$ by $g \cdot x := gxg^{-1}$. Note that

   (a) $1_G \cdot x = 1_G x 1_G^{-1} = x \quad \forall x \in X$,

   (b) $(gh) \cdot x = (gh)x(gh)^{-1} = ghxh^{-1}g^{-1} = g \cdot \left(hxh^{-1}\right) = g \cdot (h \cdot x)$.

3. The action of G on the set of left cosets of $H \leq G$: let $X := G/H = \{gH : g \in G\}$ and define $\cdot : G \times X \to X$ by $g \cdot kH = gkH$. To see it's indeed an action is similar to 1.

Proposition 2.2.3. Let G be a group acting on a set X. Define $\phi : G \to \mathrm{Sym}(X)$ by $\phi(g)(x) := g \cdot x$. Then ϕ is a homomorphism. (Then $G/\ker\phi \cong H$ where $H \leq \mathrm{Sym}(X)$).

Proof. Let $g, h \in G$. ϕ is indeed a bijection by definition of an action. It suffices to show $\phi(gh) = \phi(g) \circ \phi(h)$. Let $x \in X$, then

$$\phi(gh)(x) = (gh) \cdot x = g \cdot (h \cdot x) = \phi(g)(\phi(h)(x)) = (\phi(g) \circ \phi(h))x.$$

$\square$

Definition 2.2.4. Let ϕ be the same map as above.

1. The *kernel of action* of G on X, denoted $\ker(G, X, \cdot)$, is defined to be

$$\ker(G, X, \cdot) = \ker\phi = \{g \in G : g \cdot x = x\ \forall x \in X\} \trianglelefteq G.$$

2. The *image* of the action, denoted $\mathrm{im}\,(G, X, \cdot)$, is defined to be $\mathrm{im}\,\phi \leq \mathrm{Sym}(X)$.

3. The action is *trivial* if $\ker(G, X, \cdot) = G$ and *faithful* if $\ker(G, X, \cdot) = \{1_G\}$.

Example 2.2.5 (The same ones from 2.2.2)**.** 1. $\ker(G, X, \cdot) = \{1_G\}$, a faithful action.

2. $\ker(G, X, \cdot) = \{g \in G : gxg^{-1} = x \ \forall x \in X\} = Z(G)$. The action is trivial iff G is abelian.

3. Observe that the action is trivial $\Leftrightarrow gxH = xH \ \forall g, x \in G \Leftrightarrow H = G$, i.e. it's nontrivial as long as H is proper. This is useful: let G be a nonabelian finite simple group. We claim G cannot have a subgroup of index 3 (the case that index is 2 is obvious since if that's true then it has a nontrivial proper normal subgroup, so not simple).

   Proof. Suppose $|G : H| = 3$. G acts on $X := G/H$ and by the above H is proper, so $K := \ker(G, X, \cdot) \trianglelefteq G$ is proper. But G is simple so $K = \{1_G\}$ and one can then say $G \cong G/K \cong$ some subgroup of S_3. Since it's nonabelian it must be the whole group. But S_3 is not simple, a contradiction. □

Week 4, lecture 1 starts here

Remark. We saw last time that Proposition 2.2.3 is particularly useful when G is a finite simple group and H is a subgroup of G such that $|G : H| = n$, in that it implies that G is isomorphic to a subgroup of S_n. This leads to the following more general result.

Proposition 2.2.6. Let G be a group acting faithfully on a set X. Then G is isomorphic to a subgroup of $\mathrm{Sym}(X)$.

Proof. This follows immediately from the definition of faithful and the 1st isomorphism theorem. □

Definition 2.2.7. Let G be a group acting on a set X and $x \in X$.

1. The *orbit* of x is $\mathrm{orb}_G(x) := \{g \cdot x : g \in G\}$.
2. The *stabiliser* of x is $\mathrm{stab}_G(x) := \{g \in G : g \cdot x = x\}$.

Proposition 2.2.8. 1. $\mathrm{stab}_G(x) \leq G$.

2. $\ker(G, X, \cdot) = \bigcap_{x \in X} \mathrm{stab}_G(x)$.

Proof. See sheet 2 Q8. □

Example 2.2.9 (From 2.2.2.2)**.** Fix $x \in X = G$. One has

$$\mathrm{orb}_G(x) = \{gxg^{-1} : g \in G\},$$

called the *conjugacy class* of x in G, sometimes denoted ${}^G x$. Also

$$\mathrm{stab}_G(x) = \{g \in G : gxg^{-1} = x\},$$

called the *centraliser* of x in G, sometimes denoted $C_G(x)$.

Theorem 2.2.10 (Orbit-stabiliser)**.** Let G be a finite group acting on a set X and $x \in X$. Then

$$|G : \mathrm{stab}_G(x)| = |\mathrm{orb}_G(x)|,$$

or alternatively

$$|G| = |\mathrm{stab}_G(x)||\mathrm{orb}_G(x)|.$$

Proof. Let $S = \mathrm{stab}_G(x)$. Recall $G/S = \{gS : g \in G\}$ and $|G : S| = |G/S|$. Define

$$f : G/S \to \mathrm{orb}_G(x) \text{ by } gS \mapsto g \cdot x.$$

It suffices to show f is bijective.

1. f is well-defined and injective: $gS = kS \Leftrightarrow k^{-1}g \in S \Leftrightarrow k^{-1}g \cdot x = x \Leftrightarrow g \cdot x = k \cdot x \Leftrightarrow f(gS) = f(kS)$;
2. For $g \cdot x \in \mathrm{orb}_G(x)$ then $f(gS) = g \cdot x$, so f is surjective.

$\square$

Corollary 2.2.11. 1. For $x, y \in X$, either $\mathrm{orb}_G(x) = \mathrm{orb}_G(y)$ or $\mathrm{orb}_G(x) \cap \mathrm{orb}_G(y) = \varnothing$.

2. $\{\mathrm{orb}_G(x) : x \in X\}$ is a partition of X.
3. $|\mathrm{orb}_G(x)|$ divides $|G|$.

Proof. 1, 2. Define a relation on X $x \sim y$ if $y = g \cdot x$. It follows from the definition of an action that $\sim$ is an equivalence relation and the equivalence classes are $\{\mathrm{orb}_G(x) : x \in X\}$.

3. Immediate from the theorem.

$\square$

Theorem 2.2.12 (Cayley's)**.** Let G be a finite group. Then G is isomorphic to a subgroup of $\mathrm{Sym}(X)$ for some set X.

Proof. By Example 2.2.2.1, G acts on itself by left multiplication, and $\ker(G, X, \cdot) = \{1_G\}$, i.e. the action is faithful. The result then follows from Proposition 2.2.6. $\square$

Theorem 2.2.13. Let p be prime and G a group of order p^n where $n \in \mathbb{N}^+$. Then $|Z(G)| > 1$.

Proof. Observe that

$$g \in Z(G) \Leftrightarrow gxg^{-1} = x \ \forall x \in G \Leftrightarrow xgx^{-1} = g \Leftrightarrow |\mathrm{orb}_G(g)| = 1.$$

Week 4, lecture 2 starts here

Let $\mathrm{orb}_G(x_1), \ldots, \mathrm{orb}_G(x_t)$ be the orbits of G in its action by conjugation on $X = G$ (Example 2.2.2.2). Assume WLOG that $|\mathrm{orb}_G(x_i)| = 1$ for $1 \leq i \leq s$ and $|\mathrm{orb}_G(x_i)| > 1$ for $s < i \leq t$. By the observation above, one then has $Z(G) = \{x_1, \ldots, x_s\}$ and in particular, $|Z(G)| = s$. If $s < i \leq t$, then $|\mathrm{orb}_G(x)| = p^{a_i}$ for some $a_i \in \mathbb{N}$ by Corollary 2.2.11.3. Now, by Corollary 2.2.11.2,

$$|G| = |X| = \sum_{i=1}^{t} |\mathrm{orb}_G(x_i)| = s + \sum_{i=s+1}^{t} p^{a_i} = p^n,$$

so $|Z(G)| = s \equiv 0 \bmod p$, hence $|Z(G)| \neq 1$. $\square$

Remark. Many groups we shall see in the course will have a trivial centre, e.g. S_n for $n \geq 3$ and D_{2n} for $n \geq 3$. Also, a nonabelian finite simple group is not of order p^n.

Corollary 2.2.14. Let p be prime and G a group.

1. $|G| = p^2 \Rightarrow G$ is abelian.

2. $|G| = p^3 \Rightarrow$ either G is abelian or $|Z(G)| = p$.

Proof. We need two facts:

1. All groups of order p are cyclic (immediate from Lagrange).

2. If G is nonabelian then $G/Z(G)$ is not cyclic (see sheet 2 Q1).

It follows that if G is nonabelian then $|G/Z(G)| \neq p$ for a prime p. Now Theorem 2.2.13 implies

1. $|G| = p^2 \Rightarrow |Z(G)| = p^2 \Rightarrow Z(G) = G \Rightarrow G$ is abelian.

2. $|G| = p^3 \Rightarrow |Z(G)| = p$ or p^3 and the desired result is clear.

□

Theorem 2.2.15 (Cauchy's)**.** Let G be a finite group and p a prime divisor of $|G|$. Then G has an element of order p. Furthermore, number of elements of order p is congruent to -1 mod p.

Proof. Define

$$X := \{(g_1, \dots, g_p) \in G^p : g_1 \cdots g_r = 1_G\}.$$

Note that

$$\begin{aligned} x = (g_1, \dots, g_p) \in X \Rightarrow 1_G &= g_1 \cdots g_p \\ &\Rightarrow g_i^{-1} \cdots g_1^{-1} 1_G g_1 \cdots g_i = g_i^{-1} \cdots g_1^{-1} g_1 \cdots g_p g_1 \cdots g_i \\ &\Rightarrow 1_G = g_{i+1} \cdots g_p g_1 \cdots g_i \\ &\Rightarrow (g_{i+1}, \dots, g_p, g_1, \dots, g_i) \in X. \end{aligned}$$

Now define

$$C := \langle \sigma \rangle \leq S_p \text{ where } \sigma = (1, 2, \dots, p)$$

and the action

$$\cdot : C \times X \to X \text{ by } \sigma^i \cdot (g_1, \dots, g_p) := (g_{i+1}, \dots, g_p, g_1, \dots, g_i).$$

(Check $\cdot$ is indeed an action.) Now

1. If $g \in G$ and $g^p = 1_G$ then $(g, \dots, g) \in X$, and $\sigma^i \cdot (g, \dots, g) = (g, \dots, g)$ $\forall i$, i.e. $|\mathrm{orb}_C((g, \dots, g))| = 1$.

2. We claim that the converse is true: if x satisfies $|\mathrm{orb}_C(x)| = 1$ then $x = (g, \dots, g)$ for some $g \in G : g^p = 1_G$. Indeed, say $x = (g_1, \dots, g_p)$. It suffices to show $g_1 = g_i$ $\forall i$. By the orbit-stabiliser theorem, $|\mathrm{orb}_C(x)| = 1$ implies $\mathrm{stab}_C(x) = C$, i.e. $\forall i$,

$$(g_1, \dots, g_p) = \sigma^{i-1}(g_1, \dots, g_p) = (g_i, \dots, g_p, g_1, \dots, g_{i-1}),$$

which gives the desired.

3. Note that if $(g_1, \dots, g_p) \in X$ then $g_p = (g_1 \cdots g_{p-1})^{-1}$. We claim $|X| = |G|^{p-1}$. Indeed, define $f : X \to G^{p-1}$ by $(g_1, \dots, g_p) \mapsto (g_1, \dots, g_{p-1})$. It suffices to show that f is bijective since then $|X| = |G^{p-1}| = |G|^{p-1}$. To see f is injective, note that

$$\begin{aligned} f((g_1, \dots, g_p)) = f((h_1, \dots, h_p)) &\Rightarrow g_i = h_i \text{ for } 1 \leq i \leq p-1 \\ &\Rightarrow g_p = (g_1 \cdots g_{p-1})^{-1} = (h_1 \cdots h_{p-1})^{-1} = h_p \\ &\Rightarrow (g_1, \dots, g_p) = (h_1, \dots, h_p). \end{aligned}$$

To see f is surjective, note that for every $(x_1, \dots, x_{p-1}) \in G^{p-1}$ one can set $x_p := (x_1 \cdots x_{p-1})^{-1}$, then $(x_1, \dots, x_p) \in X$ and it satisfies $f((x_1, \dots, x_p)) = (x_1, \dots, x_{p-1})$.

By Corollary 2.2.11.3, all orbits not of size 1 have size p. Let s be number of distinct orbits of size 1, t be number of distinct orbits of size p and r be number of elements of order p in G. By parts 1 and 2, $s = 1 + r$ where 1 corresponds to the trivial element $(1_G, \dots, 1_G)$. One can then write $|G|^{p-1} = |X| = 1 + r + pt$, and since $p \mid |G|$, $r \equiv -1 \mod p$. In particular, $r > 0$. □

Week 4, lecture 3 starts here

Tool 2.2.16 (Analysing element orders in a finite group)**.** Let $E_p(G) := \{x \in G : |x| = p\}$ where p prime. Then

1. $|E_p(G)| \equiv -1 \mod p$ (Cauchy's theorem)
2. $|E_p(G)| \leq |G : C_G(x)|\ \forall x \in G$ by 1.3.4.1 and the orbit-stabiliser theorem.
3. If $r \neq p$ is a prime and G has no element of order pr, then $|C_G(x)|$ is not divisible by r for $x \in E_p(G)$ by Lemma 1.3.3.4 and Cauchy's theorem.

Example 2.2.17. Let G be of order 48 with no elements of order 6. We claim $|E_3(G)| \geq 17$.

Proof. Let $x \in E_3(G)$. Tool 2.2.16.3 implies $|C_G(x)|$ is not divisible by 2. Since $|C_G(x)| \mid 48$, it must be $|C_G(x)| = 3$. Then by Tool 2.2.16.2 $|E_3(G)| \geq 16$, and since $|E_3(G)| \equiv -1 \mod 3$, $|E_3(G)| \geq 17$. □

Proposition 2.2.18. Let G, H, X be as in Example 2.2.2.3 and $K \leq G$. Then $|KH| = \frac{|K||H|}{|K \cap H|}$.

Proof. Since G acts on X and $K \leq G, K$ acts on X as well. Let $x = H \in X$. Then

$$\text{stab}_K(x) = \{k \in K : kH = H\} = \{k \in K : k \in H\} = K \cap H,$$

and

$$|K : K \cap H| = |\text{orb}_K(x)| = |\{kH : k \in K\}|.$$

On the other hand,

$$|KH| = \left| \bigcap_{k \in K} kH \right| = |\{kH : k \in K\}||H| = |K : K \cap H||H|.$$

□

Corollary 2.2.19. Let G, H, K as above. Then

$$|G : H \cap K| \leq |G : H||G : K|.$$

Proof.
$$\frac{|H||K|}{|H\cap K|} = |KH| \leq |G| = \frac{|G|^2}{|G|},$$
and rearranging gives the desired. □

2.3 Fixed point

Definition 2.3.1. Let G be a group acting on a set X and $g \in G$.

1. An element $x \in X$ is a *fixed point* of g if $g \cdot x = x$. The set of fixed points of g is denoted $\mathrm{fix}_X(g) := \{x \in X : g \cdot x = x\}$.
2. g is *fixed point free* if $\mathrm{fix}_X(g) = \varnothing$.

Lemma 2.3.2 (not Burnside's[1])**.** Let G be a finite group acting a finite set X. Then
$$|\{\mathrm{orb}_G(x) : x \in X\}| =: r = \frac{1}{|G|}\sum_{g\in G} |\mathrm{fix}_X(g)|.$$

Informally, the number of orbits = the average number of fixed points.

Proof. We will use Corollary 2.2.11.1 and 2. Let
$$\Lambda = \{(g,x) : g \in G, x \in X, g\cdot x = x\}.$$

We count $|\Lambda|$ in two different ways (double-counting method to show equality).

1. $$|\Lambda| = \sum_{g\in G} |\mathrm{fix}_X(g)|.$$
2. $$\begin{aligned} |\Lambda| &= \sum_{x\in X} |\{g \in G : g\cdot x = x\}| = \sum_{x\in X} |\mathrm{stab}_G(x)| = \sum_{x\in X} \frac{|G|}{|\mathrm{orb}_G(x)|} \\ &= \sum_{i=1}^{r} \sum_{y\in \mathrm{orb}_G(x_i)} \frac{|G|}{|\mathrm{orb}_G(y)|} = \sum_{i=1}^{r} \sum_{y\in \mathrm{orb}_G(x_i)} \frac{|G|}{|\mathrm{orb}_G(x_i)|} \\ &= \sum_{i=1}^{r} |\mathrm{orb}_G(x_i)| \frac{|G|}{|\mathrm{orb}_G(x_i)|} = r|G| \end{aligned}$$
   where $\mathrm{orb}_G(x_1), \ldots, \mathrm{orb}_G(x_r)$ are distinct orbits.

□

Corollary 2.3.3. Let G, X and r be as in above lemma. Suppose $|X| > 1$ and $r = 1$. Then G has a fixed point free element.

[1] William Burnside (1852–1927) was known as a pioneer in the systematic study of finite groups and indeed stated and proved this lemma, but later people found out this equality was known in as early as 1845 to Cauchy, so it's *a lemma that is not Burnside's*.

Proof. By definition one has $|\mathrm{fix}_X(1_G)| = |X|$. Now

$$1 = \frac{1}{|G|}\sum_{g\in G}|\mathrm{fix}_X(g)| = \frac{1}{|G|}\left(|\mathrm{fix}_X(1_G)| + \sum_{g\neq 1_G}|\mathrm{fix}_X(g)|\right).$$

So if G doesn't have any fixed point free element then $|\mathrm{fix}_X(g)| \geq 1\ \forall g \in G$ and

$$1 \geq \frac{1}{|G|}(|X| + |G| - 1) > \frac{|G|}{|G|} = 1,$$

a contradiction. $\square$

Week 5, lecture 1 starts here

3 Sylow theorems

Remark (Philosophy)**.** In chapter 1, we saw Lagrange's theorem. Question: does the converse hold? i.e., if $l \mid |G|$, does G necessarily have a subgroup of order l?

1. A counterexample would be A_4 with $|A_4| = 12$, which does not have a subgroup of order 6 (use Tool 2.2.16.3).
2. In general, let G be a finite simple group of even order > 2. Then G has no subgroup of order $|G|/2$.

Sylow theorems will prove that a partial converse holds by restricting l.

Notation. For the remainder of the chapter, we fix a finite group G and a prime divisor p of $|G|$. Also, we write $|G|_p$ for the p-part of $|G|$, i.e. writing $|G| = p^n m$ where $p \nmid m$ we have $|G|_p = p^n$.

Definition 3.0.1. Let $H \leq G$.

1. H is a *p-subgroup* of G if $|H|$ is a power of p.
2. H is a *Sylow p-subgroup* of G if $|H| = |G|_p$.
3. The set of all Sylow p-subgroups of G is denoted $\mathrm{Syl}_p(G)$.

Example 3.0.2.

1. $G = S_4$ has order 24. Then $|G|_2 = 2^3$, $|G|_3 = 3$. One has $\langle(1,2,3)\rangle \in \mathrm{Syl}_3(G)$ and $D_8 = \langle(1,2,3,4),(1,4)(2,3)\rangle \in \mathrm{Syl}_2(G)$. Also $\langle(1,2)\rangle$ is a 2-subgroup but not a Sylow 2-subgroup.
2. $G = C_n$. Then for each divisor d or n, G has a unique subgroup of order d. In particular, if $p \mid n$, then $|\mathrm{Syl}_p(G)| = 1$. See sheet 2 Q3.
3. $G = GL_2(F)$ where F is a field of order p. Then by Theorem 1.2.3, $|G| = p^{\binom{2}{2}}\prod_{i=1}^{2}(p^i - 1) = p(p-1)(p^2-1)$. One has $x = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \in G$ with order p. Hence $\langle x\rangle \in \mathrm{Syl}_p(G)$. More generally, $|GL_n(F)|_p = p^{\binom{n}{2}}$ and $U(n,F)$ (the set of upper triangular matrices with 1 on the diagonal) is a Sylow p-subgroup.

Theorem 3.0.3 (Sylow theorems)**.** Let G be a finite group with p a prime divisor of $|G|$.

1. (Existence) $\mathrm{Syl}_p(G) \neq \varnothing$.
2. (Conjugacy) All Sylow p-subgroups are conjugate in G.
3. (Containment) Every p-subgroup of G is contained in a Sylow p-subgroup.
4. (Number) $|\mathrm{Syl}_p(G)| \equiv 1 \bmod p$.

3.1 Wielandt's proof of Sylow theorems 1 & 4

Lemma 3.1.1. Let p be prime and $n, m \in \mathbb{N}^+$ with $\gcd(m, p) = 1$. Then

1. $p \mid \binom{p}{i}$ for $1 \le i \le p-1$.
2. $\binom{p^n m}{p^n} \equiv m \bmod p$.

Proof. 1. Fix $1 \le i \le p-1$. Then

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p(p-1)\cdots(p-i+1)}{i(i-1)\cdots 1}.$$

Now let $a := (p-1)\cdots(p-i+1),\ b = i!$. Then

$$\binom{p}{i} = \frac{pa}{b} \Rightarrow pa = b\binom{p}{i} \Rightarrow p \mid b\binom{p}{i},$$

but clearly $\gcd(p, b) = 1$, hence $p \mid \binom{p}{i}$.

2. Let $F := \mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$ with usual addition and multiplication modulo p. Consider the polynomial $(1+x)^p \in F[x]$.

Week 5, lecture 2 starts here

By binomial theorem,

$$(1+x)^p = \sum_{i=1}^{p} \binom{p}{i} x^i = 1 + x^p \in F[x].$$

Then

$$(1+x)^{p^2} = ((1+x)^p)^p = (1+x^p)^p = 1 + x^{p^2}.$$

Inductively,

$$(1+x)^{p^n} = 1 + x^{p^n}.$$

Even more generally,

$$(1+x)^{p^n m} = \left((1+x)^{p^n}\right)^m = \left(1 + x^{p^n}\right)^m.$$

Binomial theorem then gives us the equality

$$\sum_{i=0}^{p^n m} \binom{p^n m}{i} x^i = \sum_{i=0}^{m} \binom{m}{i} x^{p^n i}.$$

Comparing coefficients of $x^{p^n i}$ gives

$$\binom{p^n m}{p^n i} = \binom{m}{i}$$

and in particular for $i = 1$,

$$\binom{p^n m}{p^n} = m \in F.$$

Translating this back to $\mathbb{Z}$ one has the desired.

□

Proposition 3.1.2. Sylow theorem 4. In particular, Sylow theorem 1.

Proof. As usual, write $|G| = p^n m$ where $p \nmid m$ and $p^n =: |G|_p$. Let $X := \{S \subseteq G : |S| = |G|_p\}$. Define $\cdot G \times X \to X$ by $g \cdot S := gS = \{gs : s \in S\}$. This is indeed an action: see sheet 2 Q12. Let $\mathrm{orb}_G(S_i)$ be t distinct orbits in X. By Corollary 2.2.11.2 and Lemma 3.1.1.2,

$$\binom{p^n m}{p^n} = |X| = \sum_{i=1}^{t} |\mathrm{orb}_G(s_i)| \equiv m \bmod p.$$

This means at least one $|\mathrm{orb}_G(s_i)|$ is not divisible by p. WLOG, suppose $p \nmid |\mathrm{orb}_G(S_i)|$ for $1 \le i \le r$ and $p \mid |\mathrm{orb}_G(S_i)|$ for $r < i \le t$. We claim:

1. Fix $i = 1, \dots, r$ and denote S_i by S for convenience. Then $\exists x \in G : \mathrm{stab}_G(xS) = xS$ and in particular $xS \in \mathrm{Syl}_p(G)$. Indeed, let $s \in S$ and set $x = s^{-1}$, $T := xS$. We want to show $\mathrm{stab}_G(T) = T$. First note that $1_G = xx^{-1} = xs \in T$. Hence $g \in \mathrm{stab}_G(T) \Rightarrow gT \Rightarrow g = g1_G \in gT = T$, so $\mathrm{stab}_G(T) \subseteq T$. Also, $T \in \mathrm{orb}_G(S)$, so $\mathrm{orb}_G(T) = \mathrm{orb}_G(S)$. Hence

   $$p \nmid |\mathrm{orb}_G(T)| = \frac{|G|}{|\mathrm{stab}_G(T)|} = \frac{p^n m}{|\mathrm{stab}_G(T)|}.$$

   This implies $p^n \mid |\mathrm{stab}_G(T)|$ by Lagrange's theorem. But by construction, $|T| = p^n$, so it must be that $\mathrm{stab}_G(T) = T$.

2. $r = |\mathrm{Syl}_p(G)|$. Indeed, for $i = 1, \dots, r$ we can take $T_i = x_i S_i \in \mathrm{orb}_G(S_i)$ such that $T_i = \mathrm{stab}_G(T_i)$ by previous claim. Now define

   $$\begin{aligned} f : \{\mathrm{orb}_G(T_1), \dots, \mathrm{orb}_G(T_r)\} &\to \mathrm{Syl}_p(G) \\ \mathrm{orb}_G(T_i) &\mapsto T_i \end{aligned}$$

   f is well-defined since $\mathrm{orb}_G(T_i)$ are distinct by construction and $T_i \in \mathrm{Syl}_p(G)$ by first claim. Since T_i are distinct, f is injective. Now let $P \in \mathrm{Syl}_p(G)$. Then $P \in X$, and

   $$\mathrm{stab}_G(P) = \{g \in G : gP = P\} = P,$$

   so $|\mathrm{orb}_G(P)| = m$ which by definition is not divisible by p. Hence for some $i = 1, \dots, r$, $\mathrm{orb}_G(P) = \mathrm{orb}_G(T_i)$, so $P \in \mathrm{orb}_G(T_i)$, i.e. $P = gT_i$ for some $g \in G$. But $g = g1_G \in gT_i = P$ and since $g^{-1} \in P$, $T_i = g^{-1}P = P$. This proves f is surjective, hence bijective, hence the claim.

Therefore,

$$rm + 0 = \sum_{i=1}^{r} |\mathrm{orb}_G(T_i)| + \sum_{i=r+1}^{t} |\mathrm{orb}_G(S_i)| = |X| \equiv m \bmod p$$

and since $\gcd(m, p) = 1$, we can do cancellation and have $r \equiv 1 \bmod p$. ☐

Week 5, lecture 3 starts here

3.2 Proofs of Sylow theorems 2 & 3

Remark (Easy but useful facts)**.** Let G be finite and p a prime divisor of $|G|$. Then

1. $p \in \mathrm{Syl}_p(G), g \in G \Rightarrow gPg^{-1} \in \mathrm{Syl}_p(G)$.
2. If $|G|$ is a power of p then $\mathrm{Syl}_p(G) = \{G\}$.
3. By definition, a p-subgroup Q of G is a Sylow p-subgroup iff $p \nmid |G : Q|$.

Proposition 3.2.1. Let G, p be as above and $P \in \mathrm{Syl}_p(G)$, $H \leq G$. Then $\exists g \in G : H \cap gPg^{-1} \in \mathrm{Syl}_p(H)$.

Proof. Let $X = G/P = \{gP : g \in G\}$. Then H acts on X by left multiplication (since G does) (Example 2.2.2.3). Consider the orbits and stabilisers. Fix $xP \in X$ where $x \in G$, then

$$\begin{aligned}\mathrm{stab}_H(xP) &= \{h \in H : hxP = xP\} = \{h \in H : x^{-1}hxP = P\} \\ &= \{h \in H : x^{-1}hx \in P\} = \{h \in H : h \in xPx^{-1}\} = H \cap xPx^{-1}.\end{aligned}$$

As usual, let $\mathrm{orb}_H(x_1P), \dots, \mathrm{orb}_H(x_tP)$ be distinct orbits and write $|G| = p^n m$ where $p \nmid m$. We have

$$p \nmid m = |X| = \sum_{i=1}^{t} |\mathrm{orb}_H(x_iP)| = \sum_{i=1}^{t} \left|H : \left(H \cap x_iPx_i^{-1}\right)\right|$$

so $p \nmid \left|H : \left(H \cap x_iPx_i^{-1}\right)\right|$ for some i. We claim $g := x_i$ satisfies the desired. Indeed, $H \cap gPg^{-1} \leq gPg^{-1}$, so by Lagrange's theorem it's a p-subgroup of H, hence by 3rd remark above it's a Sylow p-subgroup of H. ☐

Corollary 3.2.2. Sylow theorems 2 and 3.

Proof.

2. Let $H, P \in \mathrm{Syl}_p(G)$. Then $\exists g \in G : H \cap gPg^{-1} \in \mathrm{Syl}_p(H) = \{H\}$ by previous proposition and the 2nd remark above. So $H = H \cap gPg^{-1}$, in particular $H \subseteq gPg^{-1}$, but by assumption $|H| = |gPg^{-1}|$ so $H = gPg^{-1}$.
3. Let $H \leq G$ be a p-subgroup and $P \in \mathrm{Syl}_p(G)$. Then by exactly the same argument as above, $H \subseteq gPg^{-1} \in \mathrm{Syl}_p(G)$.

☐

3.3 Consequences of Sylow theorems

Recall that if $H \leq G$ then $H \leq N_G(H) = \{g \in G : gHg^{-1} = H\}$.

Corollary 3.3.1. Let G, p be as above and $P \in \mathrm{Syl}_p(G)$.

1. $|\mathrm{Syl}_p(G)| = |G : N_G(P)|$.
2. $\mathrm{Syl}_p(G) \mid |G : P|$.
3. $P \trianglelefteq G \Leftrightarrow |\mathrm{Syl}_p(G)| = 1$.

Proof. Let G acts on $X := \mathrm{Syl}_p(G)$ by conjugation (see sheet 2 Q15 that this is indeed an action).

1. By Sylow theorem 2, $\mathrm{Syl}_p(G)$ is explicitly $\{gPg^{-1} : g \in G\}$ which by definition is $\mathrm{orb}_G(P)$. Now $\mathrm{stab}_G(P) = \{g \in G : gPg^{-1} = P\} = N_G(P)$. The desired result then follows from orbit-stabiliser theorem.
2. By Lagrange's theorem and part 1, $P \leq N_G(P) \Rightarrow |P| \mid |N_G(P)| \Rightarrow |G : N_G(P)| \mid |G : P| \Rightarrow |\mathrm{Syl}_p(G)| \mid |G : P|$.
3. We have $P \trianglelefteq G \Leftrightarrow \{gPg^{-1} : g \in G\} = \{P\} \Leftrightarrow \mathrm{Syl}_p(G) = \{P\} \Leftrightarrow |\mathrm{Syl}_p(G)| = 1$.

□

Corollary 3.3.2. Let G, p be as above and

$$F_p(G) := \{x \in G : x \neq 1_G,\ |x| = p^n\}.$$

Then

1. $$F_p(G) = \bigcup_{P \in \mathrm{Syl}_p(G)} P \backslash \{1_G\}$$
2. $|F_p(G)| \geq |G|_p - 1$ with equality iff $|\mathrm{Syl}_p(G)| = 1$ (i.e. there is a normal Sylow p-subgroup).
3. If $|G|_p = p$, then $|F_p(G)| = |\mathrm{Syl}_p(G)|(p-1)$.

Week 6, lecture 1 starts here

Proof. 1. Let

$$x \in \bigcup_{P \in \mathrm{Syl}_p(G)} P \backslash \{1_G\}.$$

Then $|x| = p^n$ by Lagrange's, and since $x \neq 1$ one has $x \in F_p(G)$. We haven't used Sylow yet. Now let $x \in F_p(G)$. Then $\langle x \rangle$ is a p-subgroup since its order is $|x|$, so $\langle x \rangle$ is contained in a Sylow p-subgroup. The desired is then clear

2, 3. See sheet 3 Q10, 11 respectively.

□

Example 3.3.3 (Applying 3.3.1 and 3.3.2). 1. Prove that a group of order 30 is not simple.

Proof. Suppose $|G| = 30$ and G is simple. Note $|G| = 2 \times 3 \times 5$. By Corollary 3.3.1.2 and Sylow theorem 4, $|\mathrm{Syl}_5(G)| \mid 6$ and $|\mathrm{Syl}_5(G)| \equiv 1 \bmod 5$, i.e. $|\mathrm{Syl}_5(G)| = 1$ or 6. If it's 1 then by Corollary 3.3.1.3 G is not simple with P normal, a contradiction; so $|\mathrm{Syl}_5(G)| = 6$. Similarly, $|\mathrm{Syl}_3(G)| = 10$. Now Corollary 3.3.2.3 says $|F_5(G)| = 6 \times 4 = 24$ and $|F_3(G)| = 10 \times 2 = 20$, but we only have 30 elements. Hence G must be not simple. $\square$

2. Prove that a group of order 132 is not simple.

   Proof. Suppose $|G| = 132 = 11 \times 2^2 \times 3$ and G is simple. Then similarly, $|\mathrm{Syl}_{11}(G)| \mid 12$ and $|\mathrm{Syl}_{11}(G)| \equiv 1 \bmod 11$, i.e. $|\mathrm{Syl}_{11}(G)| = 1$ or 12. But again G has no normal subgroup, so $|\mathrm{Syl}_{11}(G)| = 12$. Similarly, $|\mathrm{Syl}_3(G)| = 4$ or 22. Again, $|F_{11}(G)| = 12 \times 10 = 120$ and $|F_3(G)| \geq 4 \times 2 = 8$. Now,

   $$F_2(G) \subseteq G \backslash F_{11}(G) \sqcup F_3(G) \sqcup \{1_G\},$$

   so

   $$|F_2(G)| \leq 132 - 120 - 8 - 1 = 3.$$

   Corollary 3.3.2.2 says $|F_2(G)| \geq 2^2 - 1 = 3$, so $|F_2(G)| = 3$, hence there is a normal Sylow p-subgroup, a contradiction with G being simple. $\square$

3.4 2 applications of Sylow theorems

In this section, we'll look at a game with 2 versions.

- Version 1: Prove that a group G of order $*$ is not simple. The 3 strategies are

  1. Immediately apply Corollary 3.3.1.2 and Sylow theorem 4 to try to get a contradiction. We usually start with the largest p.

     e.g. $* = 20 = 2^2 \times 5$. Then $|\mathrm{Syl}_5(G)| = 1$, an immediate contradiction.
  2. The $F_p(G)$-strategy: for each p such that $|G|_p = p$, use Corollary 3.3.2.3 to get a lower bound on $|F_p(G)|$. Since

     $$|G| < \sum_{p \| G|} |F_p(G)|,$$

     we either get an immediate contradiction or we should further use Corollary 3.3.2.3 to get one.

     e.g. Example 3.3.3.

     Week 6, lecture 2 starts here

  3. The homomorphism strategy: again begin by considering possibilities for $|\mathrm{Syl}_p(G)|$. Note that if we choose a p such that $|G : N_G(P)| = |\mathrm{Syl}_p(G)| = m > 1$ for $P \in \mathrm{Syl}_p(G)$ (Corollary 3.3.1), then $\ker(G, \mathrm{Syl}_p(G), \cdot) \subseteq \mathrm{stab}_G(P) = N_G(P) \subsetneqq G$ is proper. Since we assume (for contradiction) that G is simple, $\ker(G, \mathrm{Syl}_p(G), \cdot) = \{1_G\}$ because otherwise it would be a nontrivial, proper normal subgroup. Hence by Proposition 2.2.6, $G \cong$ some subgroup of $\mathrm{Sym}(X)$ and in particular $|G| \mid m!$. We would then get a contradiction hopefully.

     e.g. $* = 48 = 2^4 \times 3$. Then $|\mathrm{Syl}_2(G)| = 3$. So $G \cong$ a subgroup of $(\mathrm{Sym}(\mathrm{Syl}_2(G)) \cong S_3)$ and in particular $48 \mid 6$, which is absurd.

- Version 2: Prove that a finite group G with given properties (usually conjugacy classes of elements of prime order) is simple. Essentially, use the following corollary.

Corollary 3.4.1. Let $N \trianglelefteq G$ a finite group and p a prime divisor of $|G|$. Then

1. $x \in N \Rightarrow \{gxg^{-1} : g \in G\} \subseteq N$.
2. $p \nmid |G : N| \Rightarrow \mathrm{Syl}_p(N) = \mathrm{Syl}_p(G)$ and $F_p(N) = F_p(G)$.

Proof. 1. Immediate from definition.

2. By the 2nd isomorphism theorem, for a $P \in \mathrm{Syl}_p(G)$, $P/(P \cap N) \cong PN/N \leq G/N$. So $|PN/N| \mid |P|$, hence by Lagrange's, PN/P is a p-subgroup of G/N. But $p \nmid |G : N|$, so $PN/N = \{1_{G/N}\}$, i.e. $PN = N$, so $P \leq N$. So $|N|_p = |G|_p$, hence $\mathrm{Syl}_p(G) \subseteq \mathrm{Syl}_p(N)$. The other inclusion is clear.

   Now $F_p(G) = \bigcup_{P \in \mathrm{Syl}_p(G)} P \backslash \{1_G\} = \bigcup_{P \in \mathrm{Syl}_p(N)} P \backslash \{1_G\} = F_p(N)$.

□

Theorem 3.4.2. A_5 is simple.

Proof. We need 4 facts about $G = A_5$ to start with:

1. $|G| = 60 = 2^2 \times 3 \times 5$.
2. G has 24 elements of order 5, the 5-cycles.
3. G has 20 elements of order 3, the 3-cycles.
4. G has 15 elements of order 2, precisely of the form $(a, b)(c, d)$ where $a, b, c, d \in \{1, \dots, 5\}$ are distinct and all such elements are conjugate.

Week 6, lecture 3 starts here

Suppose G is not simple and let $N \trianglelefteq G$.

1°: $p \mid |N|$ for some $p \in \{3, 5\}$. Then since $|G|_p = p$, $p \nmid |G : N|$. So $F_p(G) = F_p(N)$. Hence

- $p = 5 \Rightarrow |N| \geq |F_5(N)| + 1 \geq 25$
- $p = 3 \Rightarrow |N| \geq |F_3(N)| + 1 \geq 21$

so Lagrange's implies $|N| = 30$, i.e. both 3 and 5 divide $|N|$. But again by Corollary 3.4.1

$$|N| \geq |F_3(N)| + |F_5(N)| + 1 \geq 45,$$

a contradiction.

2°: Neither 3 nor 5 divides $|N|$, then $|N| \mid 4$, so by Cauchy's it contains an element of order 2. Hence N contains all elements of order 2, so $15 \leq |N| \mid 4$, a contradiction.

□

Lemma 3.4.3. Let X be the set of 3-cycles in $G = A_n$ for $n \geq 3$. Then $G = \langle X \rangle$, and if $n \geq 5$ then all 3-cycles are conjugate.

Proof. By sheet 2 Q7, every element of A_n can be written as a product of an even number of transpositions. Hence it suffices to prove that $(a,b)(c,d)$ can be written as a product of 3-cycles.

1°: $(a,b) = (c,d)$, then $(a,b)(c,d) = 1 = (1,2,3)^3$.

2°: $|\{a,b\} \cap \{c,d\}| = 1$. WLOG $a = c$. Then $(a,b)(c,d) = (a,b)(a,d) = (a,d,b)$.

3°: $\{a,b\} \cap \{c,d\} = \varnothing$, then $(a,b)(c,d) = (a,b,c)(b,c,d)$.

Now G acts on X by conjugation. It suffices to show $\mathrm{orb}_G((1,2,3)) = X$. So let $(a,b,c) \in X$ with a,b,c distinct. We want to find $g \in G : g(1,2,3)g^{-1} = (a,b,c)$.

1°: $\{1,2,3\} \cap \{a,b,c\} = \varnothing$. Set $g = (1,2)(1,a)(2,b)(3,c)$. We add $(1,2)$ just to make g even, and it doesn't effect since disjoint cycles commute and $(1,2)(a,b,c)(1,2)^{-1} = (a,b,c)(1,2)(1,2)^{-1} = (a,b,c)$.

2°, 3°: Similar.

□

Lemma 3.4.4. Let $n \geq 5$ and $\sigma \in A_n$. Then $\exists$ a conjugate $\sigma' \neq \sigma$ and some $i \in \{1,\ldots,n\}$ such that $\sigma(i) = \sigma'(i)$.

Proof. Let r be the length of the longest cycle in σ. WLOG, we can write $\sigma = (1,2,\ldots,r)\pi$ for some $\pi \in S_n$ with π disjoint from $(1,\ldots,r)$ and being a product of cycles of length $\leq r$.

1°: $r \geq 3$. Then set $g = (3,4,5)$ and $\sigma' = g\sigma g^{-1} = g(1,\ldots,r)g^{-1}g\pi g^{-1} = (1,2,4,\ldots)g\pi g^{-1}$. So $\sigma(1) = \sigma'(1) = 2$ but $\sigma(2) = 3 \neq 4 = \sigma'(2)$.

2°: $r \leq 2$. Left as an exercise.

□

Remark.

1. Recall if $N \trianglelefteq G$ and $H \leq G$ then $H \cap N \trianglelefteq H$ (2nd isomorphism theorem).
2. Exercise: if $i \in \{1,\ldots,n\}$ then $\mathrm{stab}_{A_n}(i) \cong A_{n-1}$.

Theorem 3.4.5. A_n is simple for $n \geq 5$.

Proof. Suppose $G = A_n$ is not simple and let $N \trianglelefteq G$. We prove by induction on n with base case $n = 5$. By lemma above, for $1 \neq \sigma \in N$, $\exists i \in \{1,\ldots,n\}$ and $g\sigma g^{-1} \neq \sigma$:

$$\left(g\sigma g^{-1}\right)^{-1}(\sigma)(i) = i,$$

so

$$1 \neq \left(g\sigma g^{-1}\right)^{-1}(\sigma) \in N \cap \mathrm{stab}_G(i) \trianglelefteq \mathrm{stab}_G(i).$$

So by induction hypothesis which says $\mathrm{stab}_G(i) \cong A_{n-1}$ is simple, $N \cap \mathrm{stab}_G(i)$ can only be the whole group $\mathrm{stab}_G(i)$. So $\mathrm{stab}_G(i) \leq N$, hence N contains a 3-cycle. But then by previous lemmas, N contains all 3-cycles. But A_n is generated by 3-cycles, so $A_n \leq N$. Hence $A_n = N$, a contradiction. □

Week 7, lecture 1 starts here

4 Classifying groups of small order

4.1 Semidirect product

Definition 4.1.1. Let H, K be groups. Define a binary operation $\cdot : (H\times K)\times(H\times K) \to H\times K$ by $(h_1, k_1) \cdot (h_2, k_2) = (h_1h_2, k_1k_2)$. Then $(H \times K, \cdot)$ is a group, called the *direct product* of H and K, denoted usually simply $H \times K$.

Remark. 1. One can generalise this definition to product of more than 2 groups.

2. The identity of $G_1 \times \cdots \times G_t$ is $(1_{G_1}, \ldots, 1_{G_t})$, and $(g_1, \ldots, g_t)^{-1} = \left(g_1^{-1}, \ldots, g_t^{-1}\right)$.

3. $H \times K \cong K \times H$.

Lemma 4.1.2. Let $H, K \trianglelefteq G$ with $H \cap K = \{1_G\}$ and $G = HK$. Then

1. $hk = kh\ \forall h \in H, k \in K$.

2. $G \cong H \times K$.

Proof. 1. Let $h \in H, k \in K$. Note $hk = kh \Leftrightarrow hkh^{-1}k^{-1} = 1$. Since $H \trianglelefteq G$, $kh^{-1}k^{-1} \in H$, so $hkh^{-1}k^{-1} \in H$. By symmetry of H and K, $hkh^{-1}k^{-1} \in K$ as well, so $hkh^{-1}k^{-1} = 1$ as desired.

2. Define $\varphi : H \times K \to HK = G$ by $(h, k) \mapsto hk$. Sanity check: if $(h_1, k_1), (h_2, k_2) \in H \times K$ then $\varphi((h_1, k_1)(h_2, k_2)) = \varphi((h_1h_2, k_1k_2)) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \varphi((h_1, k_1))\varphi((h_2, k_2))$. It immediately follows from assumption that φ is surjective. Now if $(h, k) \in \ker\varphi$ then $h = k^{-1} \in H \cap K = \{1\}$, so $h = k = 1$ and $hk = 1$, i.e. $\ker\varphi = \{1\}$ which implies φ is injective.

$\square$

Remark. The hypotheses of this lemma are not too bad to work with. Lagrange's theorem allows us to study $H \cap K$, Proposition 2.2.18 allows to study HK, and Sylow theorems say a lot about normality.

Definition 4.1.3. An isomorphism $\phi : G \to G$ is an *automorphism* of G. The set $\mathrm{Aut}(G) := \{\phi : \phi \text{ an automorphism}\}$ is a group under composition, called the *automorphism group* of G.

Example 4.1.4. 1. $\mathrm{id} : G \to G$ is an automorphism.

2. If $G = C_p$ where p is prime, then $f_e : G \to G : x_i \mapsto x^{ie} \in \mathrm{Aut}(G)$ for $1 \le e \le p - 1$. Furthermore, this is in fact all the automorphisms and $\mathrm{Aut}(C_p) \cong C_{p-1}$ (see sheet 4 Q8).

3. If $K \trianglelefteq G$ and $g \in G$, then $c_g : K \to K : x \mapsto gxg^{-1} \in \mathrm{Aut}(K)$.

Definition 4.1.5. Let H, K be groups and $\phi : H \to \mathrm{Aut}(K)$ a homomorphism. For $h \in H$, write ϕ_h in place of $\phi(h)$. Define a binary operation $* : (H \times K) \times (H \times K) \to H \times K$ by $(h_1, k_1) * (h_2, k_2) = \left(h_1h_2, \phi_{h_2^{-1}}(k_1)k_2\right)$. Then $(H \times K, *)$ is a group, called the *semidirect product* of H and K with respect to ϕ, denoted $H \ltimes_\phi K$.

Remark (Defence of the definition)**.** This is not as weird as it looks. If $x, y \in G$ then $xy = yc_{y^{-1}}(x)$ where c_y is as in Example 4.1.4.3 above. Also, this really is a generalisation of the direct product. To see this, define ϕ_h to be $\mathrm{id}_K\ \forall h \in H$.

Week 7, lecture 2 starts here

Example 4.1.6. 1. Inversion homomorphism: let $H = \langle x \rangle$ with $|x| = 2$ and K be abelian. Define $\phi : H \to \mathrm{Aut}(K)$ by $\phi_{1_H} = \mathrm{id}_K$ and $\phi_x(k) = k^{-1}$.

Check ϕ_x is an automorphism: indeed $\phi_x \in \mathrm{Aut}(K)$ since it's clearly bijective and as K is abelian, $\phi_x(k_1k_2) = k_2^{-1}k_1^{-1} = k_1^{-1}k_2^{-1} = \phi_x(k_1)\phi_x(k_2)$.

Check ϕ is a homomorphism, i.e. $\phi_{h_1h_2} = \phi_{h_1} \circ \phi_{h_2}\ \forall h_1, h_2 \in H$, which is not difficult to show.

2. Conjugation homomorphism: let G be finite and $K \trianglelefteq G, H \leq G$. Define ϕ by $\phi_h(k) = hkh^{-1}$. Again it's not difficult to do the two sanity checks.

Lemma 4.1.7 (General form of Lemma 4.1.2)**.** If $H \leq G, K \trianglelefteq G$ with $H \cap K = \{1_G\}$ and $G = HK$, then $G \cong H \ltimes_\phi K$ where ϕ is conjugation homomorphism.

Proof. Again it suffices to show $f : H \ltimes_\phi K \to G : f((h,k)) = hk$ is an isomorphism. Let $(h_1, k_1), (h_2, k_2) \in H \ltimes_\phi K$, then

$$\begin{aligned} f((h_1,k_1)(h_2,k_2)) &= f((h_1h_2, \phi_{h_2^{-1}}(k_1)k_2)) = h_1h_2\phi_{h_2^{-1}}(k_1)k_2 \\ &= h_1h_2(h_2^{-1}k_1h_2)k_2 = h_1k_1h_2k_2 = f((h_1,k_1))f((h_2,k_2)). \end{aligned}$$

To show f is bijective is similar to proof of Lemma 4.1.2. ☐

Example 4.1.8 (Dihedral groups as semidirect products)**.** Recall Definition 2.1.7, write $G = D_{2n} = \langle \sigma, \tau \rangle$, and let $C_2 \cong H := \langle \tau \rangle \leq G,\ C_n \cong K := \langle \sigma \rangle \trianglelefteq G$. Proposition 2.2.18 says

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{2 \times n}{1} = 2n = |G|$$

since if $H \cap K \neq \{1\}$ then it would have to be H since $|H| = 2$. Thus $G = HK$, so by previous lemma $G \cong H \ltimes_\phi K$ where ϕ is conjugation homomorphism.

Note that

$$\phi_\tau(\sigma) = \tau\sigma\tau^{-1} = (\tau(1), \tau(2), \ldots, \tau(n)) = (n, n-1, \ldots, 1) = \sigma^{-1}$$

and in general $\phi_\tau(\sigma^i) = \sigma^{-i}$, so ϕ is also inversion homomorphism.

Lemma 4.1.9 (Generalising example above)**.** Let G be nonabelian and finite. If

- G has a cyclic subgroup K of order $\frac{|G|}{2} =: n$,
- $G \backslash K$ has an element x of order 2, and
- the only $i \in \{1, \ldots, n-1\} : i^2 \equiv 1 \bmod n$ are 1 and $n-1$, (†)

then $G \cong D_{2n}$.

Proof. First note that † is satisfied when $n = 6,\ n = p$ or $n = p^2$ where p is prime.

Week 7, lecture 3 starts here

Set $H = \langle x \rangle \leq G$ and note that $K \trianglelefteq G$ since $[G : K] = 2$, $H \cap K = \{1_G\}$ since $x \in G \backslash K$ and

$$|HK| = \frac{|H||K|}{|H \cap K|} = 2n = |G|,$$

so $G = HK$. Recall Lemma 4.1.7, assumptions of which are all satisfied. It remains to show that conjugation homomorphism ϕ is equal to inversion homomorphism here by example above, i.e. showing $\phi_x(k) = k^{-1}\ \forall k \in K$. Since K is cyclic of order n, one can write $K = \langle y \rangle$ with $|y| = n$. By exercises below, it suffices to show $\phi_x(y) = y^{-1}$. Note that $xyx^{-1} \in \langle y \rangle$ since $K \trianglelefteq G$, i.e. $xyx^{-1} = y^i$ for some $i \in \{1, \dots, n-1\}$. Since $\phi_{1_H} = \mathrm{id}_K$, one has

$$y = \phi_{1_H}(y) = \phi_{x^2}(y) = (\phi_x \circ \phi_x)(y) = \phi_x(\phi_x(y)) = \phi_x(y^i) = \phi_x(y)^i = (xyx^{-1})^n,$$

so $y = y^{i^2}$, i.e. $y^{i^2-1} = 1_G$. By Lemma 1.3.3, $n \mid i^2 - 1$, i.e. $i^2 \equiv 1 \bmod n$, so by assumption $i = 1$ or $n - 1$. One now has that $\phi_x(y) = y$ or y^{-1}, but if $xyx^{-1} = y$ then $xkx^{-1} = k\ \forall k \in K$, i.e. ϕ is trivial homomorphism, which implies $G = H \ltimes_\phi K \cong H \times K \cong C_2 \times C_n$ is abelian, contradicting assumption. So $\phi_x(y) = y^{-1}$, inversion homomorphism. $\square$

Exercise 4.1.10.

1. If $H = \langle A \rangle$, $K = \langle B \rangle$, show $hkh^{-1} = k\ \forall h \in H, k \in K \Leftrightarrow aba^{-1} = b\ \forall a \in A, b \in B$.
2. If $H = \langle x \rangle$ with $|x| = 2$ and $K = \langle B \rangle$ is abelian, show $xkx^{-1} = k^{-1}\ \forall k \in K \Leftrightarrow xbx^{-1} = b^{-1}\ \forall b \in B$.

4.2 Semidirect product of an abelian group and a cyclic group

In this section, we fix a finite group G with an abelian subgroup K of odd order $\frac{|G|}{2}$ (so we know it's normal) and let $H = \langle x \rangle \in \mathrm{Syl}_2(G)$ with $|x| = 2$ (as $|G| = 2\times$odd number).

Notation. For $v \in K$, write $[v, x] := vxv^{-1}x^{-1}$ (the commutator).

Lemma 4.2.1 (Fitting's)**.** Write $[K, x] := \langle [v, x] : v \in K \rangle$. One has

1. $xkx^{-1} = k^{-1}\ \forall k \in [K, x]$,
2. $K \cong [K, x] \times C_K(x)$,
3. $G \cong (H \ltimes_\phi [K, x]) \times C_K(x)$ where ϕ is inversion homomorphism.

Proof.

1. It suffices to show it for $k = [v, x]$, a generator of $[K, x]$. Since $|x| = 2$, one has

$$x[v, x]x^{-1} = xvxv^{-1}x^{-1}x^{-1} = xvx^{-1}v^{-1} = [v, x]^{-1}.$$

Week 8, lecture 1 starts here

2. First note that for $v, w \in K$,

$$\begin{aligned}[vw, x] &= (vw)x(vw)^{-1}x^{-1} = vwxw^{-1}v^{-1}x^{-1} \\ &= vw\left(xw^{-1}x^{-1}\right)\left(xv^{-1}x^{-1}\right) \\ &= [v, x][w, x],\end{aligned}$$

and $[v, x] = 1$ iff v and x commute, i.e. $v \in C_K(x)$.

Now define $f : K \to [K, x]$ by $f(k) = [k, x]$. f is a homomorphism with $\ker f = C_K(x)$ by above. We claim

(a) $C_K(x), [K, x] \trianglelefteq K$. This is trivial since K is abelian.

(b) $C_K(x) \cap [K, x] = \{1\}$. Indeed, if $a \in C_K(x) \cap [K, x]$, then $a = xax^{-1} = a^{-1}$ by part 1, so $|a| = 1$ or 2. But since $|K|$ is odd, by Lagrange's $|a|$ must be 1, so $a = 1$.

(c) $K = [K, x]C_K(x)$. Indeed, by 1st isomorphism theorem $|K| = |\mathrm{im}\, f||\ker f| = |[K, x]||C_K(x)|$, hence by 2.2.18 one has

$$|[K, x]C_K(x)| = \frac{|[K, x]||C_K(x)|}{|[K, x] \cap C_K(x)|} = |[K, x]||C_K(x)| = |K|.$$

So by Lemma 4.1.2 one has the desired.

3. Left as an exercise, see sheet 4 Q14.

□

4.3 Infinite families

4.3.1 Abelian groups

Theorem 4.3.1 (Fundamental theorem of finite abelian groups)**.** Let G be a finite abelian group of order n. Then $\exists$ divisors $d_1 \mid \cdots \mid d_t$ of n such that $G \cong C_{d_1} \times \cdots \times C_{d_t}$.

Proof. See MA251. □

Example 4.3.2. The abelian groups of order 8 are $C_8,\ C_2 \times C_4,\ C_2 \times C_2 \times C_2$.

4.3.2 Groups of order $p, p^2, 2p$ where p prime

Lemma 4.3.3. $|G| = p \Rightarrow G \cong C_p$.

Proof. Note that by Lagrange's, any $x \in G\backslash\{1\}$ has $|x| = p$, so $G = \langle x \rangle \cong C_p$. □

Lemma 4.3.4. $|G| = p^2 \Rightarrow G \cong C_{p^2}$ or $C_p \times C_p$.

Proof. This follows immediately from Corollary 2.2.14 and Theorem 4.3.1. □

Lemma 4.3.5. If p is odd, then $|G| = 2p \Rightarrow G \cong C_{2p}$ or D_{2p}.

Proof. If G is abelian then $G \cong C_{2p}$ by 4.3.1. If G is nonabelian and let $K \in \mathrm{Syl}_p(G),\ H = \langle x \rangle \in \mathrm{Syl}_2(G)$ where $|x| = 2$. Then

1. $|K| = \frac{|G|}{2} = p$, so $K \cong C_p$,
2. $x \in G\backslash K$,
3. If $i^2 \equiv 1 \mod p$ then $i \equiv \pm 1 \mod p$ since $\mathbb{Z}/p\mathbb{Z}$ is a field,

so by Lemma 4.1.9 one has $G \cong D_{2p}$. □

4.3.3 Groups of order $2p^2$ where p odd prime

Definition 4.3.6. Let $K = C_p \times C_p$, $H = C_2$ and $\phi : H \to \mathrm{Aut}(K)$ be inversion homomorphism. $H \ltimes_\phi K$ is called the *generalised dihedral group* of order $2p^2$ and denoted GD_{2p^2}.

Lemma 4.3.7. $|G| = 2p^2 \Rightarrow G \cong$ either $C_{2p^2},\ C_p \times C_{2p},\ GD_{2p^2},\ D_{2p^2}$ or $C_p \times D_{2p}$.

Proof.

1. If G is abelian then $G \cong C_{2p^2}$ or $C_p \times C_{2p}$ by 4.3.1.
2. If G is nonabelian, let $K \in \mathrm{Syl}_p(G)$ and $H = \langle x \rangle \in \mathrm{Syl}_2(G)$ where $|x| = 2$. Then $K \cong$ either C_{p^2} or $C_p \times C_p$.
   (a) If $K \cong C_{p^2}$ then similarly the three conditions of 4.1.9 are satisfied and $G \cong D_{2p^2}$.

   Week 8, lecture 2 starts here

   (b) If $K \cong C_p \times C_p$ then by Fitting's lemma, $G \cong (H \ltimes_\phi [K,x]) \times C_K(x)$ where ϕ is inversion homomorphism. By Lagrange's, $|C_K(x)|$ is either $1, p$ or p^2. But if $|C_K(x)| = p^2$ then $K = C_K(x)$, i.e. $kx = xk\ \forall k \in K$, contradicting G being abelian since it is generated by K and x.
      i. If $|C_K(x)| = 1$ then $C_K(x) = \{1\}$. By Fitting's lemma, $K \cong [K,x] \times C_K(x) \cong [K,x]$ and so $G \cong H \ltimes_\phi K \cong C_2 \ltimes_\phi (C_p \times C_p) \cong GD_{2p^2}$.
      ii. If $|C_K(x)| = p$ then $C_K(x) \cong C_p$ and so $[K,x] \cong C_p$, therefore $G \cong (H \ltimes_\phi [K,x]) \times C_K(x) \cong (C_2 \ltimes_\phi C_p) \times C_p \cong D_{2p} \times C_p$.

□

4.3.4 Groups of order pq where p, q prime with $p < q$ and $p \nmid (q-1)$

Lemma 4.3.8. Let p, q be as above. Then $|G| = pq \Rightarrow G \cong C_{pq}$.

Proof. By Sylow theorems, $|\mathrm{Syl}_q(G)| \equiv 1 \mod q$ and $|\mathrm{Syl}_q(G)| \mid \frac{|G|}{|G|_q} = p$. Since $q > p$ and $p \not\equiv 1 \mod q$, $|\mathrm{Syl}_q(G)| = 1$. Similarly, $|\mathrm{Syl}_p(G)| = 1$. Write $\mathrm{Syl}_p(G) = \{P\}$ and $\mathrm{Syl}_q(G) = \{Q\}$. Then $P, Q \trianglelefteq G$, $P \cap Q = \{1\}$ and $G = PQ$ since $|PQ| = \frac{|P||Q|}{|P \cap Q|} = pq = |G|$. So by Lemma 4.1.2 and Theorem 4.3.1, $G \cong P \times Q \cong C_p \times C_q \cong C_{pq}$. □

4.4 2 missing pieces

4.4.1 Groups of order 8

Definition 4.4.1. Let i, j, k be indeterminates and define

$$Q_8 := \{\pm 1, \pm i, \pm j, \pm k\} \subseteq \mathbb{R}[i,j,k].$$

Define binary operation $\cdot : Q_8 \times Q_8 \to Q_8$ by

1. $1 \cdot g = g \cdot 1 := g$ and $(-1) \cdot g = g \cdot (-1) := -g\ \forall g \in Q_8$.
2. $i \cdot j := k,\ j \cdot k := i,\ k \cdot i := j$.
3. $j \cdot i := -k,\ k \cdot j := -i,\ i \cdot k := -j$.

4. $(\pm 1)^2 = 1,\ g^2 := -1\ \forall g \in Q_8 \backslash \{\pm 1\}$.

$(Q_8, \cdot)$ is then a group with its full Cayley table determined, called the *quaternion group*.

Remark. 1. $Z(Q_8) = \{\pm 1\}$.

2. Q_8 has 1 element of order 2 (-1) and 6 elements of order 4 ($\pm i, \pm j, \pm k$).

3. $Q_8 = \langle i, j \rangle = \langle i, k \rangle = \langle j, k \rangle$.

Lemma 4.4.2. $|G| = 9 \Rightarrow G \cong$ either $C_8,\ C_2 \times C_4,\ C_2 \times C_2 \times C_2,\ D_8$ or Q_8.

Proof. 1. If G is abelian then by 4.3.1 $G \cong$ either $C_8,\ C_2 \times C_4$ or $C_2 \times C_2 \times C_2$.

2. If G is nonabelian, then of the 7 elements of order > 1, none has order 8 (since then G would be C_8) and at least one has order $\neq 2$ (since if all elements have order 2, G would be abelian), so by Lagrange's there must $\exists u \in G : |u| = 4$. Let $K = \langle u \rangle$ and $v \in G \backslash K$ with minimal order. One then has $G = \langle u, v \rangle$. We claim $vuv^{-1} = u^{-1}$. Indeed, $vuv^{-1} \in K = \{1, u, u^2, u^{-1}\}$ since $K \trianglelefteq G$. We know $|vuv^{-1}| = |u| = 4$ and $|u^2| = 2$, so vuv^{-1} is either u or u^{-1}. But if $vuv^{-1} = u$ then G would be abelian, a contradiction. Now

   (a) If $|v| = 2$ then conditions of Lemma 4.1.9 are satisfied, so $G \cong D_8$.

   (b) If $|v| = 4$, note that $G = K \sqcup vK$ and all elements of vK have order 4, so G has 1 element of order 2 (u^2) and 6 elements of order 4. It follows that $g^2 = u^2\ \forall g \in G : |g| = 4$, since g^2 has order 2 and u^2 is the only such element. Now if we see G as $\{1, u^2, u^{\pm 1}, v^{\pm 1}, (uv)^{\pm 1}\}$ we have $G \cong Q_8$.

$\square$

Week 8, lecture 3 starts here

4.4.2 Groups of order 12

Definition 4.4.3. Let $H = C_4 = \langle x \rangle$ where $|x| = 4$ and $K = C_3$. Define $\phi : H \to \mathrm{Aut}(K)$ by $\phi_{x^i}(k) = k^{(-1)^i}$. The group $H \ltimes_\phi K$ is called the *dicyclic group* or order 12, denoted Dic_{12}.

Lemma 4.4.4. $|G| = 12 \Rightarrow G \cong$ either $C_{12},\ C_2 \times C_6,\ \mathrm{Dic}_{12},\ A_4$ or D_{12}.

Proof. 1. If G is abelian then by 4.3.1 $G \cong$ either C_{12} or $C_2 \times C_6$.

2. If G is nonabelian, then

   (a) If G has an element a of order 6, let $K = \langle a \rangle$. Then all subgroups of K are normal (see sheet 3 Q9). Now

      i. If $G \backslash K$ has an element of order 2 then conditions of 4.1.9 hold, so $G \cong D_{12}$.

      ii. If $G \backslash K$ has no element of order 2, then let $P \in \mathrm{Syl}_2(G)$. We know $P \nleq K$by Lagrange's, so choose $x \in P \backslash K$. $|x|$ can only be 4 since it cannot be 1 or 2. Let $H = \langle x \rangle$ and $K_1 = \langle a^2 \rangle$. So $|H| = 4,\ |K_1| = 3$, and so conditions of 4.1.7 hold and $G \cong H \ltimes_\phi K_1$ where ϕ is conjugation homomorphism. We claim that in this case, ϕ is the same as the ϕ defined in and so that $G \cong \mathrm{Dic}_{12}$. Indeed, let $k \in \{a^2, a^{-2}\} \subseteq K_1$. Then $G = \langle x, k \rangle$ and xkx^{-1} is either k or k^{-1} since $K_1 \trianglelefteq G$. But $xkx^{-1} \neq k$ since G is nonabelian. So $\phi_x(k) = xkx^{-1} = k^{-1}$ and hence $\phi_{x^i}(k) = k^{(-1)^i}$ since ϕ is a homomorphism.

(b) If G has no element of order 6, then let $P = \langle x \rangle \in \mathrm{Syl}_3(G)$ where $|x| = 3$. By Sylow theorems, $|\mathrm{Syl}_3(G)| \in \{1, 4\}$. By 2.2.16.3, $|C_G(x)|$ is odd, and since $x \in C_G(x)$, $|C_G(x) = 3$ and $|F_3(G)| \geq |G : C_G(x)| = 4$. By 3.3.2.3, $|F_3(G)| = 2|\mathrm{Syl}_3(G)|$, so $|\mathrm{Syl}_3(G)| \geq 2$, hence $|\mathrm{Syl}_3(G)| = 4$ and $P \ntrianglelefteq G$. Now let G act on $X = G/P$ by left multiplication. By sheet 2 Q9, $\ker(G, X, \cdot) \leq P$. By Lagrange's, $\ker(G, X, \cdot)$ is either trivial or P, but kernels are normal, so $\ker(G, X, \cdot)$ is trivial and the action is faithful, so by 2.2.6, $G \cong$ a subgroup of S_4. The only subgroup of S_4 of order 12 is A_4.

□

4.5 Final theorem of the chapter

Theorem 4.5.1. The only simple group of order 60 is A_5.

Proof. Let G be a simple group of order $60 = 2^2 \times 3 \times 5$. We claim:

1. If $H \lneq G$ then $|H| \leq 12$.

   Indeed, since G is simple, G acts faithfully on $X = G/H$ (as $\ker(G, X, \cdot) \leq H \lneq G$), so by 2.2.6, $G \cong$ a subgroup of $S_{|G:H|}$ and hence $|G| \mid |G : H|!$. Since $|G| = 60$, $|G : H| \geq 5$, so $|H| \leq 12$, i.e. G has no subgroup of index 4 or less.

2. If $P_1, P_2 \in \mathrm{Syl}_2(G)$ and $P_1 \cap P_2 \neq \{1\}$, then $H = \langle P_1 \cup P_2 \rangle \Rightarrow |H| = 12$.

   Indeed, let $x \in P_1 \cap P_2 \backslash \{1\}$. Then $x \in Z(P_1) \cap Z(P_2)$ since $|P| = 4$ and all groups of order 4 are abelian. So $H = \langle P_1 \cup P_2 \rangle \leq C_G(x)$. Since G is simple, $Z(G) = \{1\}$, so $C_G(x) \lneq G$ and so $H \lneq G$. By claim 1 $|H| \leq 12$.

   Week 9, lecture 1 starts here

   Now, $4 \mid |H|$ since $|P_1| = 4$. Also, $|\mathrm{Syl}_2(H)| \equiv 1 \bmod 2$ by Sylow theorems, i.e. it's odd, and by 3.3.1 $|\mathrm{Syl}_2(H)| \mid |H|$, so $4 \times$ (an odd number) $\mid |H|$. But as $P_1, P_2 \leq H$, $|\mathrm{Syl}_2(H)| \geq 2$, so $|H| \geq 12$. We conclude that $|H| = 12$.

3. If $P_1 \cap P_2 = \{1\}\ \forall P_1 \neq P_2,\ P_1, P_2 \in \mathrm{Syl}_2(G)$ then $H = N_G(P)$ has order 12 $\forall P \in \mathrm{Syl}_2(G)$.

   Indeed, again $|\mathrm{Syl}_2(G)| = |G : N_G(P)|$ is odd, so $|\mathrm{Syl}_2(G)| \in \{1, 3, 5, 15\}$. It's not 1 since G is simple, it's not 3 by claim 1, so $|\mathrm{Syl}_2(G)| \in \{5, 15\}$. Suppose it's 15. Note that $|\mathrm{Syl}_5(G)| = 6$, and by 3.3.2, since $|G|_5 = 5$, $|F_5(G)| = 6 \times (4 - 1) = 24$. By the assumption that $P_i \backslash \{1\}$ are disjoint,

   $$|F_2(G)| = \left| \bigcup_{P \in \mathrm{Syl}_2(G)} P \backslash \{1\} \right| = 15 \times (4 - 1) = 45,$$

   so we have at least 69 elements in a group of order 60, an absurdity. Hence $|\mathrm{Syl}_2(G)| = 5$ and $|N_G(P)| = 12$. Combined with claim 2, this means G always has a subgroup of index 5.

Now let $H \leq G$ be a subgroup of index 5, then again by argument in proof of claim 1, $G \cong$ a subgroup of S_5, but the only subgroup of S_n of order $\frac{n!}{2}$ is A_n. □

5 Soluble group and Jordan–Hölder theorem

5.1 Composition series

Notation. $H \lneq G$ means H is a proper subgroup and $H \ntrianglelefteq G$ means H is a proper normal subgroup.

Definition 5.1.1. A *composition series* for a group G is a series

$$\{1_G\} = G_0 \ntrianglelefteq G_1 \ntrianglelefteq \cdots \ntrianglelefteq G_r = G$$

where the (finite) r is called *length* of the series, such that G_i/G_{i-1} is simple $\forall 1 \leq i \leq r$.

Example 5.1.2. 1. If $G = D_{2p}$ with the usual generators σ, τ, then

$$G_0 = \{1\},\ G_1 = \langle\sigma\rangle,\ G_2 = G$$

is a composition series since C_2 and C_p are simple.

2. If $G = S_n$ where $n \geq 5$ then

$$G_0 = \{1\},\ G_1 = A_n,\ G_2 = G$$

is a composition series.

3. If $G = D_8$ with $\sigma = (1,2,3,4)$ and $\tau = (1,4)(2,3)$, then

$$G_0 = \{1\},\ G_1 = \langle\sigma^2\rangle,\ G_2 = \langle\sigma^2,\tau\rangle,\ G_3 = G$$

is a composition series. We could have also set $G_2 = \langle\sigma\rangle$.

Theorem 5.1.3. Every finite group has a composition series.

Proof. By convention, the trivial group has the composition series $G_0 = G$ of length 0. We then proceed to prove by induction on $|G|$ and assume all groups of order $< |G|$ have a composition series.

Week 9, lecture 2 starts here

If G is simple then $G_0 = \{1\},\ G_1 = G$ is a composition series, so suppose G is not simple. Then $\exists N : \{1\} \neq N \neq G$ and $N \trianglelefteq G$. By inductive hypothesis, N and G/N both have a composition series, and one writes

$$\{1_G\} = N_0 \ntrianglelefteq N_1 \ntrianglelefteq \cdots \ntrianglelefteq N_r = N$$
$$\{1_{G/N}\} = \overline{G_0} \ntrianglelefteq \overline{G_1} \ntrianglelefteq \cdots \ntrianglelefteq \overline{G_s} = G/N$$

Now, by Theorem 1.6.6, $\exists X_i : N \leq X_i \leq G$ and $X_i/N = \overline{G_i}$ for all $i = 1, \ldots, s$. Also by Theorem 1.6.5, one has

$$\frac{X_i/N}{X_{i-1}/N} \cong \frac{X_i}{X_{i-1}},$$

which is simple. Now define

$$G_i := \begin{cases} N_i, & 1 \leq i \leq r \\ X_{i-r}, & r+1 \leq i \leq r+s \end{cases}$$

and note that $X_r = N$ since $\{1_{G/N}\} = N/N$, so

$$G_0 \subsetneq\!\!\trianglelefteq G_1 \subsetneq\!\!\trianglelefteq \cdots \subsetneq\!\!\trianglelefteq G_{r+s} = G$$

is a composition series. $\square$

Corollary 5.1.4 (Direct byproduct of proof but useful to write down)**.** Let G be a finite group, $N \trianglelefteq G$, and

$$\{1_G\} = N_0 \ntrianglelefteq N_1 \ntrianglelefteq \cdots \ntrianglelefteq N_r = N$$
$$\{1_{G/N}\} = N/N \ntrianglelefteq X_1/N \ntrianglelefteq \cdots \ntrianglelefteq X_s/N = G/N$$

be composition series for N and G/N where $N \leq X_i \leq G$, then

$$G_i := \begin{cases} N_i, & 1 \leq i \leq r \\ X_{i-r}, & r+1 \leq i \leq r+s \end{cases}$$

yields a composition series.

Example 5.1.5. Recall 5.1.2.3 in which we have two different composition series for D_8. But they are not that different after all: length is both 3 and all $G_i/G_{i-1} \cong C_2$ in both cases. Let's codify this.

Definition 5.1.6. Let

$$\{1_G\} = A_0 \ntrianglelefteq \cdots \ntrianglelefteq A_r = G \tag{I}$$
$$\{1_G\} = B_0 \ntrianglelefteq \cdots \ntrianglelefteq B_s = G \tag{II}$$

be 2 composition series for a group G. We say (I) and (II) are *equivalent* (and write (I) $\sim$ (II)) if $r = s$ and $\exists$ a bijection

$$f : \{A_i/A_{i-1} : 1 \leq i \leq r\} \to \{B_j/B_{j-1} : 1 \leq j \leq s\}$$

such that $A_i/A_{i-1} \cong f(A_i/A_{i-1})$.

Theorem 5.1.7 (Jordan–Hölder)**.** Any two composition series of a finite group are equivalent.

Proof. WLOG assume $r \leq s$ and do induction on r. Base case $r = 0$ is trivial so suppose $r > 0$ and statement is true for smaller r.

1° $A_{r-1} = B_{s-1}$ are the same group, then the two series are equivalent by inductive hypothesis.

2° $A_{r-1} \neq B_{s-1}$. The idea is to construct two new composition series to 'link' the current ones together. Let $D := A_{r-1} \cap B_{s-1}$. We claim $D \trianglelefteq A_{r-1}$ and $A_{r-1}/D \cong G/B_{s-1}$ (and symmetrically $D \trianglelefteq B_{s-1}$ and $B_{s-1}/D \cong G/A_{r-1}$). Indeed, note that by Theorem 1.6.4.2, since $A_{r-1} \trianglelefteq A_r = G$ so $A_{r-1} \cap B_{s-1} \trianglelefteq B_{s-1}$ and since $B_{s-1} \trianglelefteq B_s = G$ so $A_{r-1} \cap B_{s-1} \trianglelefteq A_{r-1}$. Again by 1.6.4.3,

$$\frac{A_{r-1}}{D} = \frac{A_{r-1}}{A_{r-1} \cap B_{s-1}} \cong \frac{A_{r-1}B_{s-1}}{B_{s-1}}.$$

proof to be continued...

$\square$

Week 9, lecture 3 starts here