Modern Algebra II

Notes on MATH 6320

Daniel Koizumi

April 12, 2022

Contents

1 January 13

A group G is called **cyclic** if $G = \langle a \rangle$ for some $a \in G$, in which case a is a **generator**. For instance,

$$(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$$

$$= \langle 2, 3 \rangle$$

A group that is cyclic is Abelian. Rubiks cube group $< S_{48}$. It is generated by six elements,

$$\langle T, Bottom, L, R, F, Back \rangle$$

The group is

$$\left(\left(\frac{\mathbb{Z}}{2} \right)^{11} \times \left(\frac{\mathbb{Z}}{3} \right)^{7} \right) \rtimes \left((A_8 \times A_{12}) \rtimes \frac{\mathbb{Z}}{2} \right)$$

A_8 and A_{12} are alternating groups, and $\rtimes$ denotes the semi-direct product, which we will define in the future.

If $H < G$ we saw $|G| = |H| \cdot (G : H)$. Any infinite cyclic group is isomorphic to $\mathbb{Z}$. Otherwise, a cyclic group G is isomorphic to $\frac{\mathbb{Z}}{|G|}$. We use additive notation for a group only if it is abelian. If n is a positive integer, $x \in G$,

$$n \cdot x = x + \ldots + x \ (n \text{ times})$$

Likewise,

$$(-n) \cdot x = -x - x - \ldots - x \ (n \text{ times})$$

Any Abelian group G is a $\mathbb{Z}$-module. If G is a finitely generated Abelian group, then the structure theorem for modules over a PID applies. We have

$$G \cong \mathbb{Z} \oplus \ldots \oplus \mathbb{Z} \oplus \frac{\mathbb{Z}}{m_1} \oplus \frac{\mathbb{Z}}{m_2} \oplus \ldots \oplus \frac{\mathbb{Z}}{m_k}$$

Multiplicative notation: If $x \in G$ and n is a positive integer, then

$$x^n = x \cdot x \cdot \ldots \cdot x$$

$$x^{-n} = x^{-1} \cdot \ldots \cdot x^{-1}$$

Proposition 1. 1. An infinite cyclic group has 2 possible generators, a and a^{-1}.

2. If $G = \langle a \rangle$ is a cyclic group of order n. Then $\langle a^m \rangle = G$ if and only if m is relatively prime to n.
3. If $G = \langle a \rangle = \langle b \rangle$, then $G \to G$ defined by $a \mapsto b$ is an automorphism.
4. If G is cyclic of order n, and $d|n$, then $H = \{x \in G : \text{order of } x \text{ divides } d\}$ is a subgroup of order d.

Proof. 1.

2.

3. The map is surjective, but since it is a map of finite sets, it is also injective.
4. H contains the identity. And $x \in H$ implies that $x^{-1} \in H$. If $x^d = 1$ and $y^d = 1$, then $(xy)^d = 1$, because G is abelian.

□

If $G = \langle x \rangle$, $x^n = 1$, $n = de$, then

$$H = \{x^m : x^{m \cdot d} = 1\}.$$

Note $x^{md} = 1$ if and only if $n = de | md$ if and only if $e | m$. Note that H is the subgroup defined by

$$\left\langle x^{\frac{n}{d}} \right\rangle$$

(Can be used to show that the multiplicative group of a finite field is cyclic.) Suppose $\varphi : G_1 \to G_2$ is a group homomorphism. Let $H_2 < G_2$. Then $\varphi^{-1}(H_2)$ is a subgroup of G_1. We have

$$\varphi^{-1}(\{e_2\}) < G_1$$

But this is the kernel of φ. In fact, it is a normal subgroup, which we denote $\ker \varphi \lhd G_1$. We say that a subgroup is normal if $gHg^{-1} = H$ for all $g \in G$. Recall $xH = \{xh : h \in H\}$. If A, B are subsets of a group G $AB = \{ab : a \in A, b \in B\}$. Set $K = \ker(G_1 \to G_2)$. If $k \in K$ and $g \in G_1$, then

$$\varphi(gkg^{-1}) = \varphi(g)\varphi(g^{-1}) = \varphi(e_1) = e_2.$$

Given $K \lhd G$, there is a canonical surjection $G \twoheadrightarrow \frac{G}{K}$ $g \mapsto gK$ which has kernel K. The group above is defined

$$\frac{G}{K} = \{gK : g \in G\}$$

We want to give this group its structure. So we define

$$(g_1K)(g_2K) = g_1g_2K$$

This is well defined (check this). It also makes $\frac{G}{K}$ a group. A group G acts on a set S if there is a group homomorphism $\pi : G \to \mathrm{Perm}(S)$. For each $g \in G$ we have $\pi_g : S \to S$ a bijection. Now note that the identity element of the group must be the identity of the permutation of the group. In other words,

$$\pi_{g_1g_2} = \pi_{g_1}\pi_{g_2}$$

For shorthand, we often write $\pi_g(x) = gx$ for $x \in S$.

Example. If $H < G$, then G acts on $\frac{G}{H}$ (the set of left cosets). It acts via

$$x \mapsto (gH \mapsto xgH)$$

The kernel of this homomorphism, call it π, is

$$\{x \in G \mid xgH = gH \ \forall \ g \in G\} \lhd G$$

If $x \in K$, then $g^{-1}xg \in H$ for all $g \in G$. In particular, it happens when $g = id$, so $x \in H$. So $K < H < G$. Since $K \lhd G$, we also have $K \lhd H$.

Proposition 2. Suppose G is a finite group and $H < G$ such that

$$p = (G : H)$$

is the smallest prime dividing $|G|$. Then $H \lhd G$.

Proof. We can define $G \xrightarrow{\pi} \mathrm{Perm}(\frac{G}{H})$. Note the latter group is the symmetric group on p symbols, which is of order $p!$. Then we can factor this map through and get

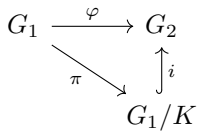
$$\frac{G}{K} \to \mathrm{Perm}(\frac{G}{H})$$

an injective map. So $(G : K)$ divides $p!$. But

$$(G : K) = (G : H)(H : K)$$

So $(G : H)(H : K)$ divides $p!$. Now $(G : H) = p$, so $(H : K)$ divides $(p-1)!$. Since p is the smallest integer dividing $|G|$, $(H : K) = 1$. Hence $H = K \lhd G$. □

Proposition 3. If $\varphi : G_1 \to G_2$ has kernel K, then φ factors through $\frac{G}{K}$, meaning there is a suitable map $i : \frac{G_1}{K}$ making the following diagram commute:



where i is an injective homomorphism, and π is the canonical surjection.

Proof. Given $gK \in \frac{G_1}{K}$, define

$$i(gK) = \varphi(g)$$

this is well defined, for given any other representative $hK = gK$, so that $g^{-1}h \in K$, we have

$$i(hK) = \varphi(h)$$

but $\varphi(g)^{-1}\varphi(h) = \varphi(g^{-1}h) = e_2$, so $\varphi(g) = \varphi(h)$. (Check this gives a homomorphism) □

Example. (Group Action) Suppose G is a group. We have

$$\mathrm{Aut}(G) \text{ (the group of automorphisms of } G)$$

We have a representation $G \mapsto \mathrm{Aut}(G) < \mathrm{Perm}(G)$ defined by $x \mapsto c_x \in \mathrm{Aut}(G)$ where c_x is the conjugation by x.

2 January 18

Suppose $K < H < G$ and $K \lhd G$ and $H \lhd G$. Then $\frac{G}{K}$ and $\frac{G}{H}$ are groups, and

$$\frac{G}{K} \to \frac{G}{H}$$

defined by $gK \mapsto gH$. With kernel $\{gK : gH = H\} = \{hK : h \in H\} = \frac{H}{K}$. Note that $K \lhd H$ so $\frac{H}{K}$ is a group. By the first isomorphism theorem

$$\frac{G/K}{H/K} \xrightarrow{\sim} \frac{G}{H}$$

Suppose $K \lhd G$. Then subgroups of $\frac{G}{K}$ correspond to subgroups of G that contain K. Likewise, normal subgroups of G/K correspond to normal subgroups of G that contain K. Recall: If A, B are subsets of G then

$$AB = \{ab \mid a \in A, b \in B\}$$

Let $S \subset G$. Then $N_S = \{x \in G \mid xSx^{-1} = S\} < G$ is a subgroup of G, called **normalizer** of S in G. Define

$$Z_S = \{x \in G \mid xsx^{-1} = s \forall s \in S\} < G$$

is the centralizer of S in G.

Z_G is the center of the group G. If $H < G$ then $H < N_H < G$. In fact, $H \lhd N_H$ by definition. Let H, K be subgroups of G and $H \subset N_K$. Then $H \cap K \lhd H$. For $s \in H \cap K$ and $h \in H$,

$$hxh^{-1} \in H$$

it is also in K since $h \in N_K$, $x \in K$.

$H \subset N_K$ gives $HK = KH$, which is a group (check).

Exercise 1

Define $\varphi : H \to \frac{HK}{K}$ via $x \mapsto xK$. Check that this is a group homormophism. Also check this is surjective and $\ker \varphi = H \cap K$. We also have by the first isomorphism theorem

$$\frac{H}{H \cap K} \cong \frac{HK}{K}.$$

We stopped last time at the action of a group G on itself via conjugation. $G \to \mathrm{Aut}(G)$ maps via $x \mapsto \left(g \mapsto xgx^{-1}\right)$. (Note the distinction between automorphism and permutation: permutations are not necessarily homomorphisms). The kernel of the action is the center of the group. The image of $G \to \mathrm{Aut}(G)$ is the group of inner automorphisms denoted $Inn(G)$.

Proposition 4. *$Inn(G) \lhd Aut(G)$.*

Proof. Let $\varphi \in Aut(G)$, $c_x \in Inn(G)$. We would like to check that

$$\varphi \circ c_x \circ \varphi^{-1} \in Inn(G)$$

$$\varphi \circ c_x \circ \varphi^{-1}(g) = \varphi(x\varphi^{-1}(g)x^{-1}) = \varphi(x)g\varphi(x^{-1}) = c_{\varphi(x)}(g)$$

□

We are obliged to construct

$$\frac{Aut(G)}{Inn(G)} = Out(G)$$

Suppose G acts on S. Let $s \in S$. Define

$$G_s = \{x \in G : xs = s\}.$$

This is called the **stabilizer of the isotropy subgroup**. This is not to be confused with $G{\cdot}s = \{xs \mid x \in G\}$, which is called the **orbit of** s. Suppose $t \in G \cdot s$. Then we compare G_s and G_t. In fact, we have G_t is conjugate to G_s. We have

$$G_t = \{x \in G \mid xt = t\} = \{x \in G \mid xys = ys\}$$

$$= \{x \in G \mid y^{-1}xys = s\} = \{x \in G \mid y^{-1}xy \in G_s\} = yG_sy^{-1}$$

Set $K = \ker(G \to Perm(S))$. We can write $K = \bigcap_{s \in S} G_s$. We say that the action of G on S is faithful if $K = \{e\}$. Fixed points in S are those such that $xs = s \forall x \in G$.

Let $s \in S$. We can define $G \to Gs$ by $x \mapsto xs$. This yields a map $\frac{G}{G_s} \to Gs$ by $xG_s \mapsto xs$. If $xG_s = yG_s$, then $y^{-1}x \in G_s$. So $yx^{-1}s = s$ so $xs = ys$. Hence the map is well defined, surjective, and injective. Hence $\frac{G}{G_s \to Gs}$ is a bijection. We have

$$|Gs| = (G : G_s)$$

Two orbits Gs and Gt are either equal or disjoint. If they shared an element $gs = ht$. But this implies $Gs \subset Gt$, since for any $g's \in Gs$, $g's = g'g^{-1}gs = g'g^{-1}ht \in Gt$. Similarly, $Gt \subset Gs$. We can then write

$$S = \bigcup Gs_i$$

so $|S| = \sum |Gs_i| = \sum (G : G_{s_i})$ (this is called the class formula).

Let G act on a set S. The action is transitive if for some $s \in S$ $Gs = S$. Equivalently, we say the same if there is only one orbit.

The action of G on S restricts to an action on each orbit. On each orbit, the group is transitive.

Theorem 1. Cauchy's theorem: Suppose G is a finite group and p is a prime dividing $|G|$. Then G has an element of order p.

Definition 1. Let p be a prime integer. A group G is a p-group if $|G| = p^n$ for some $n \in \mathbb{N}$.

Lemma 1. Suppose G is a $p-$ group acting on a set S. Let F = fixed points in$S = \{s \in S \mid xs = s \forall x \in G\}$. Then $|S| \equiv |F|$ modulo p.

Proof. Apply the class formula $|S| = \sum(G : G_{s_i})$. We have $|S| = |F| + \sum_{\text{other } i}(G : G_{s_i})$. For $s_i \notin F$, $G_{s_i} \subsetneq G$, so $p|(G : G_{s_i})$. □

Proof. (of Cauchy's theorem): Let $S = \{(x_1, \ldots, x_p) \mid x_i \in G, x_1 \cdots x_p = e\}$. We have

$$|S| = |G|^{p-1}.$$

Define $\sigma \in \text{Perm}(S)$ by $\sigma : (x_1, \ldots, x_p) \mapsto (x_p, x_1, \ldots, x_{p-1})$. We have

$$x_1 \ldots x_{p-1} = x_p^{-1}$$

$$x_p x_1 \ldots x_{p-1} = e$$

So σ maps elements of S to S. σ has order p. Hence $\langle\sigma\rangle$ is a p-group acting on S, so $|F| \equiv |S| \mod p$ by the lemma. But $|S| \equiv 0 \mod p$, since p divides $|G|$ which divides $|S|$. $e, \ldots, e) \in F$, so $|F| \geq p$. But elements of F are of form $(x, \ldots, x)$, which implies that any nonidentity in F corresponds to a desired element. □

Suppose p divides $|G|$ and p is a prime. Let p^n be the highest power of p dividing $|G|$.

Theorem 2. G has a subgroup of order p^n. Such a subgroup called a p-Sylow subgroup.

Lemma 2. Fix a prime p dividing $|G|$. Suppose G acts on S with the property that $\forall s \in S$,there exists a p-subgroup of G that fixes only s. Then the action of G is transitive.

Proof. Suppose P is a p-subgroup fixing only $s \in S$. We have that $|S| \equiv 1 \mod p$ by a preceding lemma. If S has multiple orbits, we can write

$$S = S_1 \cup S_2$$

a disjoint union. Each subset has the same property as S that satisfies the theorem hypotheses, so $|S_1| \equiv 1 \mod p$ and $|S_2| \equiv 1 \mod p$. Hence

$$|S| \equiv |S_1| + |S_2| \mod p$$

implies

$$|S| \equiv 2 \mod p$$

Hence the action is transitive. □

3 January 20

Let G be a finite group, p be a prime dividing $|G|$. A **p-Sylow subgroup of** G is a subgroup of order p^n where p^n is the highest power of p dividing $|G|$.

Theorem 3. If a prime p divides $|G|$, then a p-Sylow subgroup exists.

Proof. We will work on induction on $|G|$. If $|G| = p$, then we are done, since G is the desired group. If $H < G$ and $p \not| (G : H)$ (so that in this case the highest power of p dividing $|G|$ is also the highest power for $|H|$), then a $p-$ Sylow subgroup of H is also a p-Sylow subgroup of G. We may therefore assume that for all subgroups $H \subsetneq G$, we have $p|(G : H)$.

Let G act on itself via conjugation

$$G \to \mathrm{Aut}(G)$$

The kernel of the homomorphism is also the center of the group denoted Z. Use the class equation:

$$|G| = |Z| + \sum_i (G : G_{x_i})$$

Here G is the set, Z is the set of fixed points, and the last set is the size of larger orbits. Here G_{x_i} is an isotropy subgroup, so $(G : G_{x_i})$ is the cardinality of the orbit of x_i. By our hypothesis, $(G : G_{x_i})$ is divisible by p for all i.

So $|G| \equiv |Z| \mod p$. This implies that p divides the order of Z since $|G| \equiv 0 \mod p$. We have $e \in Z$, so that $\exists a \in Z$ of order p by Cauchy's theorem. Now $\langle a \rangle$ has order p, and $a \in Z$ implies

$$\langle a \rangle \lhd G.$$

$\frac{G}{\langle a \rangle}$ has smaller order than G, so it must have some p-Sylow subgroup P by induction hypothesis. Then $|P|$ is p^{n-1} where p^n is the highest order of p dividing $|G|$. Now note that P corresponds to a subgroup of G which must have order p^n. It is $\varphi^{-1}(P)$ where

$$\varphi : G \to \frac{G}{\langle a \rangle}$$

is the natural map. □

Lemma 3. Suppose A, B are finite subgroups of G. Then AB is a set of products of elements of A, B. Then $|AB| = \frac{|A| \cdot |B|}{|A \cap B|}$.

Proof. $A \cap B < A$, so A can be written as a disjoint union of cosets

$$\bigsqcup_{i \in I} a_i (A \cap B)$$

for some $a_i \in A$. So

$$\begin{aligned} AB &= \bigcup_{i \in I} a_i (A \cap B) B \\ &= \bigcup_{i \in I} a_i B \end{aligned}$$

Claim: $AB = \bigsqcup_{i \in I} a_i B$ (the unioin is disjoint)

If $a_i b = a_j b'$ for $i \neq j$, $b, b' \in B$, then

$$a_i = a_j b' b^{-1}$$

so that $a_j^{-1} a_i = b' b^{-1} \in A \cap B$ so that

$$a_i \in a_j (A \cap B)$$

and $i = j$.

Claim yields

$$|AB| = \sum_{i \in I} |a_i B| = |I| \cdot |B| = |B| \cdot \frac{|A|}{|A \cap B|}$$

□

Theorem 4. Let p be a prime dividing $|G|$. Then:

1. Each p-subgroup is contained in a p-Sylow subgroup
2. The p-Sylow subgroups are conjugate.
3. Let s_p be the number of p-Sylow subgroups. Then $s_p || G|$ and $s_p \equiv 1 \mod p$.

Proof. Let $\mathcal{S}$ be the set of all p-subgroups. Then G acts on $\mathcal{S}$ by conjugation, since $|H| = |xHx^{-1}|$. Let $\mathcal{M}$ be the set of maximal elements of $\mathcal{S}$ (under inclusion). Claim: The action restricts to an action on $\mathcal{M}$. Let $p \in \mathcal{M}$. Suppose $xPx^{-1} \subset Q$ for some $Q \in \mathcal{S}$. Then $P \subset x^{-1}Qx \in \mathcal{S}$. But P was maximal, so $P = x^{-1}Qx$. This implies $xPx^{-1} = Q$, so that xPx^{-1} is maximal.

Now note that any p-Sylow subgroup must be in $\mathcal{M}$. We would like to prove that any $P \in \mathcal{M}$ is a p-Sylow subgroup, giving property 1 above. We know G acts on $\mathcal{M}$ by the above argument. If P is a p-Sylow subgroup, then $P \in \mathcal{M}$. Since G acts on $\mathcal{M}$, any subgroup also does. In particular, P acts on $\mathcal{M}$ via conjugation, and P fixes P since $xPx^{-1} = P \forall x \in P$. Suppose P fixes some $Q \in \mathcal{M}$. Then $xQx^{-1} = Q$ for all $x \in P$, so $P < N_Q$, and PQ is a subgroup of G. So

$$|PQ| = \frac{|P| \cdot |Q|}{|P \cap Q|}$$

($|P|, |Q|$ are powers of p and the quotient is an integer, so it must be a power of p) so PQ is a p-group. Then P, Q are maximal, so $P \subset PQ$ implies $P = PQ$ and $Q \subset PQ$ implies $Q = PQ$. So $P = Q$.

We have that P acts on $\mathcal{M}$ and fixes **only** itself. This implies the action by P is transitive by a previous lemma from class, which we recall:

Remark. Fix prime p. If G acts on $\mathcal{S}$ with the property that $\forall s \in S$, $\exists$ a p-subgroup fixing only s, then G is transitive on S.

In our context, G acts on $\mathcal{M}$. Each $P \in \mathcal{M}$ is a p-group that fixes **only** $P \in \mathcal{M}$. Hence G is transitive on $\mathcal{M}$. But then $\mathcal{M}$ is precisely the set of p-Sylow subgroups, and they are all conjugate. This also gives us property 2. Lastly, we figure out the deal with s_p. We know $s_p = |\mathcal{M}|$. $P \in \mathcal{M}$ acts on $\mathcal{M}$ with 1 fixed point, so $|\mathcal{M}| \equiv$ (number of fixed points $= 1$) $\mod p$. So $s_p \equiv 1 \mod p$. Now also G is transitive on $\mathcal{M}$, so $|\mathcal{M}| = (G : G_P)$ for $P \in \mathcal{M}$. Hence $s_p = \frac{|G|}{|G_P|}$. We have 3. □

Example. Suppose $|G| = 15$. We look at s_3, s_5. By the above theorem, $s_3 \equiv 1 \mod 3$ and $s_3 | 15$, so $s_3 = 1$.

We also have $s_5 \equiv 1 \mod 5$, $s_5 | 15$, implies $s_5 = 1$.

In general $s_p = 1$ if and only if a (the) p-Sylow is normal.

If Q is a 5-Sylow, then $(G : Q) = 3$, which is the smallest prime dividing $|G| = 15$. This implies that Q is normal. This is an alternative way to see that $s_5 = 1$.

Say $|P| = 3, |Q| = 5$. Then $PQ = 15$, so $PQ = G$. We can say more: let $[P, Q] = \langle [p, q] : p \in P, q \in Q \rangle$ where $[p, q] = pqp^{-1}q^{-1}$ (the commutator). If $P \lhd G$, $Q \lhd G$, then $pqp^{-1}q^{-1} \in P \cap Q$ so that in particular elements of P commute with those of Q (see proposition ahead). So

$$P \times Q \xrightarrow{(p,q) \mapsto pq} G$$

is a group homomorphism. We have

$$(p_1, q_1) \mapsto p_1 q_1$$
$$(p_2, q_2) \mapsto p_2 q_2$$
$$(p_1, q_1)(p_2, q_2) = p_1 q_1 p_2 q_2 = p_1 p_2 q_1 q_2$$

We know that the only groups of order $3, 5$ respectively are $\frac{\mathbb{Z}}{3}$, $\frac{\mathbb{Z}}{5}$. Hence G must be $\frac{\mathbb{Z}}{15}$.

Proposition 5. Suppose

1. $P \lhd G$, $Q \lhd G$
2. $PQ = G$
3. $P \cap Q = \{e\}$

Then $G \cong P \times Q$.

Proof. Consider $pqp^{-1}q^{-1}$ for $p \in P, q \in Q$. Now because $P \lhd G$, $qp^{-1}q^{-1} \in P$ and so $pqp^{-1}q^{-1} \in P$. Likewise, $Q \lhd G$ implies $pqp^{-1} \in Q$ and $pqp^{-1}q^{-1} \in Q$. Hence

$$pqp^{-1}q^{-1} \in P \cap Q = \{e\}$$

so that $pqp^{-1}q^{-1} = e$. In other words, $pq = qp$. Now define $P \times Q \to G$ by

$$(p, q) \mapsto pq$$

The fact that elements of P commute with those of Q ensures that this is a group homomorphism. It is surjective because of property 2. It is also injective. Given (p, q) mapping to e, we have $pq = e$. But $p = q^{-1} \in P \cap Q = \{e\}$, so that $p = e = q$. Hence it is also injective. □

4 January 25

Last time: Let G be a finite group and p be a prime dividing $|G|$. Then each subgroup is contained in a p-Sylow subgroup. Only 2 p-Sylow subgroups P, Q are conjugate. If s_p is the number of p-Sylow subgroups, then

$$s_p \big| |G|$$

and $s_p \equiv 1 \mod p$.

Corollary 1. Suppose that $|G| = pq$ where $p \neq q$ are primes. Suppose $p < q$, and that $p \not| q - 1$. Then G is cyclic.

Proof. Let Q be a q-Sylow subgroup. Its index is p, which is the smallest prime dividing the order of G, which implies $Q \lhd G$. Alternatively, $s_q \equiv 1 \mod q$ and $s_q \big| |G|$ so $s_q = 1$. Therefore $xQx^{-1} = Q$ for all $x \in G$.

Q is normal, so conjugation by any element of G takes Q to itself. That is $\forall x \in G$

$$c_x : Q \to Q$$

An automorphism of Q is determined by one is sent in $Q \cong \frac{\mathbb{Z}}{q}$, so $AutQ \cong \frac{\mathbb{Z}}{q}^*$ (multiplicative group which is of order $q - 1$).

We have a map $G \to \frac{\mathbb{Z}}{q}^*$. Since p doesn't divide $q - 1$, the map must be trivial.

Restating, $G \to \mathrm{Aut}Q$ must be trivial, ie, $xyx^{-1} = y$ for all $y \in Q$. This means Q is a subgroup of $Z(G)$.

If we take an element x of order p, $y \in Q$ of order q, then xy has order pq. Hence xy generates G. Note that Q is cyclic because any element divides the order of Q, so there is a generator of Q. □

Suppose $|G| = pq$ where $p \neq q$ are primes. Say $p < q$. Then there exists q-Sylow Q, $Q \lhd G$, and we can't say that G is necessarily cyclic, but we have $G \rhd Q \rhd \{e\}$. We have $\frac{G}{Q}$ and $\frac{Q}{\{e\}}$ is cyclic. We will eventually define G to be in this case a **solvable group**. We say $G = G_0 \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_n = \{e\}$ is a **normal tower** of subgroups of G. A normal tower as above is a **cyclic tower** if $\frac{G_i}{G_{i+1}}$ is cyclic for all i. It is an **abelian tower** if $\frac{G_i}{G_{i+1}}$ is abelian for all i. For instance $\mathbb{Q} \rhd \{1\}$ is an Abelian tower but not a cyclic tower.

A group G is **solvable** if it has an abelian tower. Note:

- Abelian groups are solvable. Because $G \rhd \{e\}$ works.
- If $|G| = pq$ for primes $p \neq q$ then G is solvable.
- Let's examine $G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in GL_2(\mathbb{R}) \right\}$, which is solvable.

Definition 2. $G \to \mathbb{R}^\times \times \mathbb{R}^\times$ where G is as above, and define

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mapsto \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$$

which is a group homomorphism. The group of the latter matrices is isomorphic to $\mathbb{R}^\times \times \mathbb{R}^\times$. The kernel is

$$K = \left\{ \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \mid c \in \mathbb{R} \right\}$$

Since the map is surjective,

$$\frac{G}{K} \cong \left(\mathbb{R}^\times\right)^2$$

So $G \rhd K \rhd \{1\}$, which gives the abelian tower.

- (Feil-Thompson Theorem 1963, 255 pages :O) Any group of odd order is solvable.

We will see soon that for $n \geq 5$, the group S_n is **not** solvable.

Corollary 2. Overkill consequence of the Feil-Thompson theorem) $|S_5| = 120$ is even.

Given a group G, what is the smallest normal subgroup you could mod out by to make it abelian? We define

$$G' = \left\langle [a,b] = aba^{-1}b^{-1} : a, b \in G \right\rangle$$

where $[a,b]$ denotes a commutator. In other words G' is generated by the commutators of G. Then $G' \lhd G$. We prove normality: given $x \in G$, and $aba^{-1}b^{-1} \in G'$,

$$xaba^{-1}b^{-1}x^{-1} = [xax^{-1}, xbx^{-1}]$$

In $\frac{G}{G'}$, we have that $aG'bG'a^{-1}G'b^{-1}G' = eG'$, so $\frac{G}{G'}$ is commutative. Conversely, if $N \lhd G$ and $\frac{G}{N}$ is abelian, then

$$G' \subset N$$

The reason is that $aNbNa^{-1}Nb^{-1}N = eN$ implies

$$aba^{-1}b^{-1}N = eN$$

or $[a,b] \in N$, so $G' \subset N$.

Remark. Any homomorphism $G \to H$ with H abelian factors as $G \to \frac{G}{G'} \to H$ where the composition is the original map.

Proposition 6. Suppose $H \lhd G$. Then G is solvable if and only if H and $\frac{G}{H}$ are solvable.

Proof. Lets prove the if direction. If we have abelian tower

$$H = H_0 \rhd H_1 \rhd \ldots \rhd H_m = \{e\}$$

and abelian tower of $\frac{G}{H}$, we can get

$$\frac{G}{H} \rhd \frac{G_1}{H} \rhd \frac{G_2}{H} \rhd \ldots \rhd \frac{G_n}{H} \frac{H}{H}$$

where G_1 is a normal subgroup of G, G_i is a normal subgroup of G_{i-1}, and

$$\frac{G_i/H}{G_{i+1}/H}$$

Then G is solvable since we have abelian tower

$$G \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_n = H \rhd H_1 \rhd H_2 \rhd \ldots \rhd H_m = \{e\}$$

Now we prove the only if direction. Suppose there exists Abelian tower

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_n = \{e\}$$

and define $H_i = G_i \cap H$. We have a natural inclusion

$$H_i \hookrightarrow G_i$$

and map

$$H_i \to \frac{G_i}{G_{i+1}} = H_i \cap G_{i+1} = (G_i \cap H \cap G_{i+1}) = H_{i+1}$$

Now we have an induced map

$$\frac{H_i}{H_{i+1}} \hookrightarrow \frac{G_i}{G_{i+1}}$$

To see $\frac{G}{H}$ is solvable, use

$$\frac{G}{H} = \frac{G_0}{H} \rhd \frac{G_1}{G_1 \cap H} \rhd \frac{G_2}{G_2 \cap H} \rhd \ldots \rhd \frac{G_n}{G_n \cap H} = \{e\}$$

and we have

$$\frac{G_i/G_i \cap H}{G_{i+1}/G_{i+1} \cap H} \cong G_i/G_{i+1}$$

which is abelian by assumption. The isomorphism comes from the first isomorphism theorem (exercise for later maybe). □

We now provide a more formal discussion on symmetric groups. We look at $S_n = \text{Perm}\{1, \ldots, n\}$. Let $e_1, \ldots, e_n$ be standard basis vectors for $\mathbb{R}^n$. We can view S_n as $\text{Perm}\{e_1, \ldots, e_n\}$, and it provides an action on $\mathbb{R}^n$. Each element of S_n acts on $\mathbb{R}^n$ as a permutation matrix. For $\sigma \in S_n$, define $\text{sgn}(\sigma) = \det(\text{permutation matrix of } \sigma) = \pm 1$. An element $\pi \in \text{Perm}\{1, \ldots, n\}$ can be written as

$$\begin{pmatrix} 1 & 2 & .. & n \\ \pi(1) & \pi(2) & \ldots & \pi(n) \end{pmatrix}$$

Fix π as above. Let $\langle \pi \rangle$ act on $\{1, \ldots, n\}$, and like any group acting on any set it partitions it into disjoint orbits. We can use this to write π in **cyclic notation**. The action of π on each orbit can be represented as a **cyclic** permutation.

Example. A **cyclic permutation** can for instance be written $(1, \pi(1), \pi^2(1), \pi^3(1), \ldots, \pi^m(1))$ where m is the smallest integer so that $\pi^{m+1}(1) = 1$.

5 January 27

Last time, we defined $\operatorname{sgn}\pi$, for π a permutation, as the determinant of the corresponding matrix. Notation:

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$$

Alternatively, we can write π with cyclic notation. Consider the orbits of $\langle\pi\rangle$ acting on $\{1, \dots, n\}$. We can write each cycle as

$$(1\ \pi(1)\ \pi^2(1)\ \dots\ \pi^{k-1}(1))$$

and likewise for other orbits. Since orbits partition the entire set into disjoint subsets, π can be expressed as a product of disjoint cycles.

Example. Consider

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}$$
$$= (1)(2\ 5)(3\ 4) = (2\ 5)(3\ 4)$$

Example. We can compose cycles: $(1\ 2\ 3)(3\ 4\ 5) = (1\ 2\ 3\ 4\ 5)$ Also note that the order of a cycle is discernible from its length. The above cycle has order 5. Also, for example, $(1\ 2\ 3)(4\ 5)$ has order 6.

We have

$$\pi(x_1\ x_2\ \dots\ x_k)\pi^{-1} = (\pi(x_1)\ \dots\ \pi(x_k))$$

Check that:

$$\left(\pi(x_1\ x_2\ \dots\ x_k)\pi^{-1}\right)(\pi(x_i)) = \pi(x_{i+1})$$

(maybe except when $i = k$, in which case the resulting element is $\pi(x_1)$. We have

$$\left(\pi(x_1\ x_2\ \dots\ x_k)\pi^{-1}\right)(\pi(y)) = \pi(y)$$

for $y \neq x_i$ for all i. By the cycle structure of $\sigma \in S_n$, we mean the number of 2 cycles, number of 3 cycles, etc when σ is written as disjoint cycles. Disjoint cycles commute, so the order doesn't matter. By what we have proved above, conjugation preserves the cyclic structure. For example,

$$\pi(1\ 2)(3\ 4\ 5)\pi^{-1} = (a\ b)(c\ d\ e)$$

We have

- Each element of S_n can be written as a product of disjoint cycles.
- It can be wirtten as a product of 2-cycles (ie we can write it as a product of transpositions).
- Every element can be written as a product of 2-cycles involving 1. For example,

$$(2\ 3) = (1\ 2)(1\ 3)(1\ 2)$$

- $S_n = \langle(1\ 2), (1\ 3), \dots, (1\ n)\rangle$. We can also write

$$S_n = \langle(1\ 2), (2\ 3), \dots, (n-1\ n)\rangle$$

- $S_n = \langle(1\ 2), (1\ 2\ \dots\ n)\rangle$. If we call the latter generator π, we have this because $\pi(1\ 2)\pi^{-1} = (2\ 3)$, and so on, giving the generators for the previous item.

We have a caveat:

$$S_4 \neq \langle (1\ 3), (1\ 2\ 3\ 4) \rangle$$

Call the former $\sigma = (1\ 3)$ and $\tau = (1\ 2\ 3\ 4)$. We have

$$\sigma\tau\sigma^{-1} = (3\ 2\ 1\ 4) = (4\ 3\ 2\ 1) = \tau^{-1}$$

so $\langle \tau \rangle \lhd \langle \sigma, \tau \rangle = \langle \sigma \rangle \langle \tau \rangle$. We will later come to the conclusion that this is a **dihedral group**. On the other hand, τ is not a normal subgroup of S_4, because

$$(1\ 2)\tau(1\ 2) = (2\ 1\ 3\ 4) \notin \langle \tau \rangle$$

Let p be prime. Then $S_p = \langle (1\ 2), \tau \rangle$ for any p-cycle τ. because some power of τ has the form $(1\ 2\ 3\ \ldots\ p)$. In other news, we have

$$\operatorname{sgn} : S_n \to \{\pm 1\}$$

is a group homomorphism, since determinants are multiplicative. We call $A_n = \ker \operatorname{sgn}$, called the **alternating group**. We automatically have $A_n \lhd S_n$ because it is a kernel. If $n \geq 2$, $(S_n : A_n) = 2$. Also $\operatorname{sgn}(i\ j) = -1$.

Elements of A_n are precisely those that are a product of an even number of 2-cycles. We can make a conclusion about the commutator subgroup S_n'. We have $S_n' \subset A_n$. Are they always equal? Let's look at examples:

$$S_1' = A_1$$

$$S_2' = A_2$$

After some work, $S_3' = A_3$.

Lemma 4. A_n is generated by 3-cycles.

Proof. If $n = 1, 2$ then this is vacuously true. For $n = 3$,

$$A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$$

so it is true for $n = 3$. Otherwise, any element can be written an even product of 2-cycles. Each pair is a product of 3-cycles:

$$(1\ 2)(2\ 3) = (1\ 2\ 3)$$

$$(1\ 2)(3\ 4) = [(1\ 2\ 4), (1\ 2\ 3)]$$

$$= (1\ 2\ 4)(1\ 2\ 3)(4\ 2\ 1)(3\ 2\ 1)$$

$$= (1\ 2\ 4)(4\ 3\ 2) = (1\ 2)(3\ 4)$$

□

Proposition 7. $S_n' = A_n$.

Proof. $\subset$ is true as remarked before the lemma. For $\supset$, it suffices to do it for $n \geq 3$ (we already noted $n = 1, 2$). Note

$$[(1\ 2\ 3), (1\ 2)] = (1\ 2\ 3)(1\ 2)(3\ 2\ 1)(1\ 2) = (1\ 2\ 3)(3\ 1\ 2) = (1\ 3\ 2)$$

So S_n' contains $(1\ 3\ 2)$, and hence every 3-cycle by a similar argument. □

Proposition 8.

$$A_1' = A_1$$
$$A_2' = A_2$$
$$A_3' = \{e\}$$
$$A_4' = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} = N$$
$$A_n' = A_n\ \forall\ n \geq 5$$

Proof. By explicit calculation, N is a subgroup. Conjugation preserves cycle structure, and N contains all of the possible pairs of disjoint 2-cycles. So conjugation by any element gives back an element in N.

$$\left|\frac{A_4}{N}\right| = 3$$

SO A_4/N is Abelian. Hence $A_4' \subset N$. But

$$(1\ 2)(3\ 4) \in A_4'$$

which is equal to

$$[(1\ 2\ 4), (1\ 2\ 3)]$$

The typical element of N can be written as a commutator. Hence $A_4' = N$. We now prove the conclusion for $n \geq 5$.

We saw $[(1\ 2\ 3), (1\ 2)] = (1\ 3\ 2)$. We do have, however

$$[(1\ 2\ 3), (1\ 2)(4\ 5)] = (1\ 3\ 2)$$

giving us all 3-cycles. □

Corollary 3. If $n \geq 5$, we have $A_n^{(k)} = A_n \forall k \geq 1$. Recall that $G' = [G, G] = \langle [\sigma, \tau] : \sigma, \tau \in G \rangle$. We now define

$$G^{(2)} = G'' = (G')'$$

and so on for $G^{(n)}$.

We also have A_4 is solvable because $A_4 \rhd N \rhd \{e\}$ is an Abelian tower. $|\frac{A_4}{N}| = 3$ so its abelian. Also, $|N| = 4$, so it is also abelian (in particular, it is $\frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2}$). Our corollary implies that A_n is not solvable. Anything that contains the commutator which we would mod out by to make an Abelian group must be the entirety of A_n, which is no abelian alone.

Proposition 9. G is solvable if and only if $G^{(n)} = \{e\}$ for some n.

Proof. The if direction comes from our previous discussion. Because then

$$G = G^{(0)} \rhd G^{(1)} \rhd \ldots \rhd G^{(n)} = \{e\}$$

is an Abelian tower. For the other direction, if G is solvable, we have

$$G = G_0 \rhd G_2 \rhd G_3 \rhd \ldots \rhd G_m = \{e\}$$

where G_i/G_{i+1} is abelian for all i. This fact says $G_0' \subset G_1$, and $G_i' \subset G_{i+1}$ in general. We have that $G_0^{(n)} \subset G_n$, so $G^{(m)} = \{e\}$. □

We saw $S_n' = A_n$ for all n. The shape of the tower for symmetric groups?

$$S_2' = \{e\}$$

$$S_3 \rhd S_3' = A_3 \rhd \{e\}$$

$$S_4 \rhd S_4' = A_4 \rhd A_4' = N \rhd \{e\}$$

$$S_5 \rhd S_5' = A_5 \rhd A_5' = A_5 \rhd \dots$$

so S_5 not solvable. We would like to prove that A_5 and higher are simple in some future class. For now, we talk about dihedral groups.

$$A_n < S_n$$

Definition 3. $D_n < S_n$ is the group of rigid symmetries of a regular n-gon. Meaning:

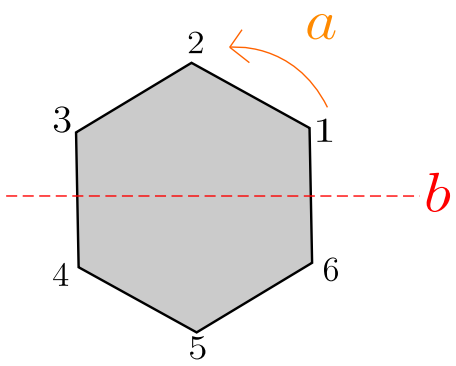


Figure 1: Symmetries include rotations and reflections

We have two kinds of elements in D_n :

- Rotations $a = (1\ 2\ \dots\ n)$ and
- Reflections

$$b = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & n & n-1 & \dots & 3 & 2 \end{pmatrix}$$

We have $b^2 = e$, $a^n = e$. We also have

$$bab^{-1} = (1\ n\ n-1\ \dots\ 2) = a^{-1}$$

Said otherwise,

$$\langle a \rangle \lhd \langle a, b \rangle$$

and

$$\langle a, b \rangle = \langle b \rangle \langle a \rangle$$

is a group of order $2n$. One might ask if a and b together give us other reflections. Is D_n solvable? Yes!

$$D_n \rhd \langle a \rangle \rhd \{e\}$$

shows that D_n is solvable, since

$$\left| \frac{D_n}{\langle a \rangle} \right| = 2$$

What is D_n'?

$$[a, b] = aba^{-1}b^{-1}$$
$$= (1\ 2\ \ldots\ n)(2\ 3\ \ldots\ n\ 1) = a^2$$

So $a^2 \in D_n'$. And $\left| \frac{D_n}{\langle a^2 \rangle} \right| = 4$.

6 February 1

Last time, we defined the Dihedral group $D_n = \langle a, b \rangle \subset S_n$ where $a = (1\ 2\ 3\ \ldots\ n)$ (rotation) and

$$b = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 1 & n & n-1 & \ldots & 3 & 2 \end{pmatrix}$$

Note that

$$bab^{-1} = (1\ n\ n-1\ \ldots\ 3\ 2) = a^{-1}$$

and $|D_n| = 2n$. We also defined $[b, a] = bab^{-1}a^{-1} = a^{-2}$, so $a^{-2} \in D_n'$.

What is D_n'? So far, we know that $a^2 \in D_n'$. What happens if we conjugate a^2 by some other element? For instance,

$$ba^2b^{-1} = a^{-2}$$

This shows $\langle a^2 \rangle \lhd D_n$. We discuss

$$\left| \frac{D_n}{\langle a^2 \rangle} \right| = \begin{cases} 2 & \text{if } n \text{ is odd} \\ 4 & \text{if } n \text{ is even.} \end{cases}$$

So $D_n / \langle a^2 \rangle$ is abelian. Hence $D_n' = \langle a^2 \rangle$. Hence $D_n' = \langle a^2 \rangle$. $|a| = n$, $|b| = 2$. We have

$$bab^{-1} = a^{-1}$$

We have an action

$$\langle b \rangle \to \operatorname{Aut} \langle a \rangle$$

conjugation by b or not. **Semi-direct Products:**

Definition 4. Suppose that N and H are groups, and we have a homomorphism $\alpha : H \to \operatorname{Aut}(N)$. We define a group structure on $\{(n, h) : n \in N, h \in H\}$ by

$$(n, h) \cdot (n', h') = (n\alpha(h)(n'), hh')$$

It is left to check the following properties:

1. Associativity (see exercise)
2. $(n, h) \cdot (e, e) = (n\alpha(h)(e), h) = (n, h)$ and

$$(e, e) \cdot (n, h) = (e\alpha(e)(n), h) = (n, h)$$

3. Inverses. $(n, h)^{-1} = (\alpha(h^{-1})(n^{-1}), h^{-1})$ (see exercise).

We write the defined group $N \rtimes H$, or $N \rtimes_\alpha H$.

Exercise 2

Check the associative property of this group. Also check that the inverse in property 3 is actually an inverse.

Note that $N \times \{e\} \lhd N \rtimes H$. In other words, we can reverse the operation of multiplying by N on the left by semi-direct product. We check that $N \times \{e\}$ is a normal subgroup indeed. We check

$$\begin{aligned}(n,h)\cdot(n',e)\cdot(n,h)^{-1} &= (n\alpha(h)(n'),h)\cdot(\alpha(h^{-1})(n^{-1}),h^{-1})\\ &= \left(n\alpha(h)(n')\alpha(h)\left(\alpha(h^{-1})(n^{-1})\right),hh^{-1}\right)\\ &\left(n\alpha(h)(n')n^{-1},e\right)\end{aligned}$$

We also have

$$\{e\}\times H < N \rtimes H$$

but not necessarily normality.

Proposition 10. Suppose G is a group, $N \lhd G$, $H < G$ such that

1. $NH = G$.
2. $N \cap H = \{e\}$.

Then $G \cong N \rtimes_\alpha H$ where $\alpha : H \to \mathrm{Aut}(N)$ is conjugation $\alpha(h)(n) = hnh^{-1}$.

Proof. Define $N \rtimes_\alpha H \to G$ by

$$(n,h)\mapsto nh$$

so it is at least a map. We check it's a homomorphism:

$$\begin{aligned}((n,h)\cdot_\alpha(n',h')) &= \left(nhn'h^{-1},hh'\right)\\ &\mapsto nhn'h^{-1}hh' = nhn'h'\end{aligned}$$

It's surjective by property 1, and injective by 2. □

$$D_n \cong \langle a\rangle \rtimes \langle b\rangle$$

where $\langle a\rangle \cong \frac{\mathbb{Z}}{n}, \langle b\rangle \cong \frac{\mathbb{Z}}{2}$. So we can define

$$D_\infty = \langle a\rangle \rtimes_\alpha \langle b\rangle$$

where $\langle a\rangle \cong \mathbb{Z}$ and $\langle b\rangle \cong \frac{\mathbb{Z}}{2}$. It has generators a, b by $|a| = \infty$ and $|b| = 2$. What is Aut$\mathbb{Z}$? It's $\frac{\mathbb{Z}}{2}$. Let's look at the α we define for the product:

$$\begin{aligned}(\alpha(b))(a) &= a^{-1}\\ bab^{-1} &= a^{-1}\end{aligned}$$

We know look to the following question: What are **all** groups of order 6? There must be a 3-Sylow $P \cong \frac{\mathbb{Z}}{3}$ which is a normal subgroup. Cauchy's theorem says there is a subgroup of order 2. A group of order 6 must hence be

$$\frac{\mathbb{Z}}{3}\rtimes_\alpha \frac{\mathbb{Z}}{2}$$

for some choice of α. We have

$$\alpha : \frac{\mathbb{Z}}{2} \to \mathrm{Aut}\frac{\mathbb{Z}}{3} \cong \frac{\mathbb{Z}}{2}$$

So if α is trivial, the semi-direct product is the direct product.

$$\frac{\mathbb{Z}}{3}\times\frac{\mathbb{Z}}{2}\cong\frac{\mathbb{Z}}{6}$$

If α is nontrivial, there's only one choice for it: $\alpha(1) = 2$

$$bab^{-1} = a^{-1}$$

$a = (1\ 2\ 3), b = (1\ 2)$.

$$bab^{-1} = a^{-1}$$

When can we say different (nontrivial) α's give us isomorphic groups?

Proposition 11. Suppose H is cyclic, and $\alpha, \beta : H \to \mathrm{Aut}(N)$ with the property that $\alpha(h)$ and $\beta(h)$ are conjugate subgroups of $\mathrm{Aut}(N)$. Then $N \rtimes_\alpha H \cong \mathbb{N} \rtimes_\beta H$

Proof. Let $H = \langle h \rangle = \langle h^k \rangle$ and $\beta(h) = \varphi \circ \alpha(h^k) \circ \varphi^{-1}$ (ie $\beta(h)$ is the conjugate of some generator of $\alpha(H)$).

Define

$$N \rtimes_\beta H \to N \rtimes_\alpha H$$

by

$$(n, h) \mapsto (\varphi(n), h^k)$$

$$(n, h) \cdot_\beta (n', h') = (n\beta(h)(n'), hh')$$

the product of the two elements' images on the left is

$$(\varphi(n), h^k) \cdot_\alpha (\varphi(n'), (h')^k)$$

$$= (\varphi(n)\alpha(h^k)(\varphi(n')), h^k(h')^k)$$

and the latter maps to

$$(\varphi(n)\varphi\varphi^{-1}\alpha(h^k)\varphi(n'), (hh')^k)$$

$$= (\varphi(n)\alpha(h^k)\varphi(n'), h^k(h')^k)$$

□

Example. On different $\rtimes$ structures.

$$\frac{\mathbb{Z}}{8} \rtimes \frac{\mathbb{Z}}{2}$$

We have $\mathrm{Aut}\left(\frac{\mathbb{Z}}{8}\right) = \left(\frac{\mathbb{Z}}{8}\right)^\times = \{1, 3, 5, 7\}$. Write $\frac{\mathbb{Z}}{8}$ as $\langle x \rangle$, $x^8 = 1$ and $\frac{\mathbb{Z}}{2}$ as $\langle y \rangle$ where $y^2 = 1$.

$$yxy^{-1} = \begin{cases} x \\ x^3 \\ x^5 \\ x^7 \end{cases}$$

Let's examine:

$$yxy^{-1} = x^3$$

In any of the above cases,

$$G = \{x^i, yx^i : 0 \le i \le 7\}$$

x^4 is an element of order 2, but we also have

$$\left(yx^i\right)^2 = yx^iyx^i = yx^iy^{-1}x^i = x^{3i}x^i = x^{4i}$$

This has order 2 if $i = 2, 4, 6, 8$. In this group, all the elements of order 2 are $\{x^4, yx^2, yx^4, yx^6, y\}$, so there are 5 elements. Similarly, when

$$yxy^{-1} = x^5,$$

we have

$$(yx^i)^2 = x^{6i}$$

which is 1 when $i = 0, 4$. So elements of order 2 are

$$\{x^4, y, yx^4\}.$$

We also have for

$$yxy^{-1} = x^7$$

(which is the actual dihedral group)

$$(yx^i)^2 = x^{8i} = 1$$

for all i. That is, the set of order 2 elements are

$$\{x^4, y, yx, yx^2, yx^3, yx^4, yx^5, yx^6, yx^7\}$$

However, when

$$yxy^{-1} = x$$

we have

$$(yx^i)^2 = x^{2i} = 1$$

when $i = 0, 4$ (but in this case we are working with $\frac{\mathbb{Z}}{8} \times \frac{\mathbb{Z}}{2}$). Hence the order 2 elements are

$$\{x^4, y, yx^4\}.$$

We have that $\frac{\mathbb{Z}}{8} \rtimes \frac{\mathbb{Z}}{2}$ has three nonisomorphic nonabelian $\rtimes$ structures.

Let $\mathbb{F}$ be a field, and consider $\mathrm{GL}_n(\mathbb{F})$. We can consider

$$\mathrm{SL}_n(\mathbb{F}) \lhd \mathrm{GL}_n(\mathbb{F})$$

Denote G to be the bigger group and $N = \mathrm{SL}_n(\mathbb{F})$. Take

$$H = \left\{ \begin{pmatrix} a & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \right\}$$

We prove we can write $G = N \rtimes H$. We have

$$\mathrm{GL}_n(\mathbb{F}) \xrightarrow{\det} \mathbb{F}^\times \xrightarrow{\sim} H$$

the former map has kernel $\mathrm{SL}_n(\mathbb{F})$. By a form of the first isomorphism theorem we may do later, the desired semi-direct product follows.

7 February 3

Suppose R is a commutative ring, and $0 \to L \to M \to N \to 0$ is an exact sequence of R-modules. This sequence splits if we can split the surjection and injection. In other words, there exists a map $N \to M$ such that

$$L \to M \to N$$

is the identity. This is the same thing as saying there exists $M \to L$ such that

$$L \to M \to L$$

is the identity. The same thing holds for groups, except we usually write 1 for multiplicative notation for groups. For an exact sequence of groups,

$$1 \to N \to G \to Q \to 1$$

we say this sequence splits if there exists a map $Q \to G$ such that

$$Q \to G \to Q$$

is the identity.

Example.

$$1 \to A_3 \to S_3 \to \frac{S_3}{A_3} \to 1$$

Suppose we take a nontrivial element in $\frac{S_3}{A_3}$ to a 2-cycle. Now $\frac{S_3}{A_3} \cong \frac{\mathbb{Z}}{2}$, so this forms a group homomorphism. But note that we cannot have a map $S_3 \to A_3$, because there is no normal subgroup of order 2. The takeaway here is a difference between the commutative and noncommutative case. The latter map is required to split, but the former map does not necessarily split if the latter one does.

Example. Consider

$$0 \to \frac{\mathbb{Z}}{p} \xrightarrow{\cdot p} \frac{\mathbb{Z}}{p^2} \to \frac{\mathbb{Z}}{p} \to 0$$

which does not split. (after reading the ahead discussion, note that there is no possible way to write $\frac{\mathbb{Z}}{p} \rtimes \frac{\mathbb{Z}}{p}$ other than $\frac{\mathbb{Z}}{p} \times \frac{\mathbb{Z}}{p}$.)

Proof. We would like to ultimately show that G is a semidirect product of Q and N if it is in a split exact sequence. We saw

$$N \cong \{(n, 1) : n \in N\} \lhd N \rtimes H$$

$$H \cong \{(1, h) : h \in H\} < N \rtimes H$$

We get

$$1 \to N \to N \rtimes H \to H \to 1$$

is split exact. The split map is $h \mapsto (1, h)$. Suppose $1 \to N \to G \to Q \to 1$ is split exact. Then there exists $Q' < G$ with $Q' \cong Q$ and $\varphi : Q \to G$. Suppose the sequence is split. We claim $G = NQ'$. We have a proposition $G \cong N \rtimes Q' \cong N \rtimes Q$.

Suppose $x \in N \cap Q'$.

$$1 \to N \to G \to Q \to 1$$

$$x \mapsto x \mapsto 1$$

by exactness. Since $x \in Q'$, there exists $y \in Q$ such that $\varphi(y) = x$. But $y \mapsto \varphi(y) \mapsto 1 = y$. So $x = 1$.

$$\frac{G}{N} \cong Q \cong Q'$$

$NQ' < G$, and

$$\frac{NQ'}{N} \cong \frac{Q'}{Q' \cap N}$$

$$NQ' < G$$

and $\frac{NQ'}{N} \cong \frac{G}{N}$. Using that subgroups of $\frac{G}{N}$ correspond to subgroups of G containing N, we get $NQ' = G$. □

Suppose $1 \to N \to G \to Q \to 1$ is exact. We say G is an extension of Q by N. For example, $\frac{\mathbb{Z}}{p^2}$ is an extension of $\frac{\mathbb{Z}}{p}$ by $\frac{\mathbb{Z}}{p}$. $Q = \{\pm_1, \pm i, \pm j, \pm k\}$. We have the rules

$$i \cdot j = k = -j \cdot i$$

$$j \cdot k = i = -k \cdot j$$

$$k \cdot i = j = -i \cdot k$$

$$1, -1 \in Z(Q)$$

Those elements have order 2, and i, j, k have order 4, their squares being -1. We have

$$\langle i \rangle \lhd Q$$

via

$$1 \to \langle i \rangle \to Q \to \frac{Q}{\langle i \rangle} \to 1$$

so Q is an extension of $\frac{\mathbb{Z}}{2}$ by $\frac{\mathbb{Z}}{4}$. This sequence does not split. The only element of order 2 is -1, which cannot be mapped to, since $-1 \in \langle i \rangle$.

$$Q \neq \frac{\mathbb{Z}}{4} \rtimes \frac{\mathbb{Z}}{2}$$

for any choice of $\alpha : \frac{\mathbb{Z}}{2} \to \mathrm{Aut}(\frac{\mathbb{Z}}{4}) = \frac{\mathbb{Z}}{2}$ which is either trivial or nontrivial. In the nontrivial case, we are looking at D_4. In this group, there are 5 elements of order 2. But Q has 1 element of order 2.

Groups of order 12 (see homework). We know there is a 2-sylow and a 3-sylow. The 3-sylow is isomorphic to $\frac{\mathbb{Z}}{3}$ and the 2-sylow (because it's of order 4) is isomorphic to either $\frac{\mathbb{Z}}{4}$ or $\frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2}$. Suppose $P \lhd G$ and $|G| = 12$. Then $G = PQ$.

$$P \cap Q = 1$$

So $G \cong P \rtimes Q$. There are some cases:

1. $\frac{\mathbb{Z}}{3} \rtimes_\alpha \frac{\mathbb{Z}}{4}$. This means we should have a map $\frac{\mathbb{Z}}{4} \to \mathrm{Aut}(\frac{\mathbb{Z}}{3}) = \left(\frac{\mathbb{Z}}{3}\right)^\times = \frac{\mathbb{Z}}{2}$. Two options exist. α is trival, giving
$$\frac{\mathbb{Z}}{3} \times \frac{\mathbb{Z}}{4} \cong \frac{\mathbb{Z}}{12}$$
or it is nontrivial. This yields a nonabelian
$$\frac{\mathbb{Z}}{3} \rtimes \frac{\mathbb{Z}}{4}.$$

2. $\frac{\mathbb{Z}}{3} \rtimes_\alpha \left(\frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2}\right)$, where $\alpha : \frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2} \to \frac{\mathbb{Z}}{2}$. You could kill $(1,0)$, $(0,1)$, or $(1,1)$. Some options: If α is trivial, we have
$$\frac{\mathbb{Z}}{3} \times \frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2}$$
If not, $\frac{\mathbb{Z}}{2} \times \left(\frac{\mathbb{Z}}{3} \rtimes \frac{\mathbb{Z}}{2}\right) \cong \frac{\mathbb{Z}}{2} \times S_3$ since there is only one nonabelian group of order 6.

Suppose P is not normal. There are several 3-Sylow subgroups. $s_3 = 4$ of them, to be exact. This gives exactly eight elements of order 3, and the remaining ones constitute Q. Hence $Q \lhd G$. So Q is normal. Suppose $\frac{\mathbb{Z}}{4} \rtimes \frac{\mathbb{Z}}{3}$. $\alpha : \frac{\mathbb{Z}}{3} \to \mathrm{Aut}(\frac{\mathbb{Z}}{4}) = \frac{\mathbb{Z}}{2}$ must be trivial. And the other group of order 4 is $\frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2}$, and so we have

$$\left(\frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2}\right) \rtimes \frac{\mathbb{Z}}{3}$$

Now $\alpha : \frac{\mathbb{Z}}{3} \to \mathrm{Aut}\left(\frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2}\right)$. Any automorphisms permute the three possible generators. In particular, we work with $\mathrm{GL}_2(\mathbb{F}_2)$. What have we of

$$|\mathrm{GL}_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1}).$$

Hence $\mathrm{GL}_2(\mathbb{F}_2) = S_3$ since its of order 6 and nonabelian. α is either trivial (a case we already covered) or nontrivial, in which case it hits some order 3 element. The new group is

$$\left(\frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2}\right) \rtimes \frac{\mathbb{Z}}{3}$$

Now we would like to distinguish groups that we have already found. Note that

$$\frac{\mathbb{Z}}{2} \times \left(\frac{\mathbb{Z}}{3} \rtimes \frac{\mathbb{Z}}{2}\right) \cong \frac{\mathbb{Z}}{6} \rtimes \frac{\mathbb{Z}}{2} = D_6$$

The distinguishing factor between $\left(\frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2}\right) \rtimes \frac{\mathbb{Z}}{3}$ and D_6 is that one has a normal 2 sylow and the other has a normal 3 sylow, but neither has both or else they would be abelian. In A_4, notice that we had a normal 2-sylow. It should accordingly be

$$A_4 = \left(\frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2}\right) \rtimes \frac{\mathbb{Z}}{3}$$

We now classify groups of order 8. If there exists elements of order 8, $G \cong \frac{\mathbb{Z}}{8}$.

1. If there is an element of order 8, $G \cong \frac{\mathbb{Z}}{8}$.
2. If $x^2 = 1$ for all $x \in G$, then we have commutativity, so $G \cong \frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2}$.
3. If there exists $x \in G$ of order 4, it generates a normal subgroup (since it's of index 2). So $\langle x \rangle \lhd G$. Suppose there exists $y \in G \setminus \langle x \rangle$ of order 2. Then $\langle x \rangle \langle y \rangle$. Hence

   $$G \cong \frac{\mathbb{Z}}{4} \rtimes_\alpha \frac{\mathbb{Z}}{2}$$

   So α is trivial or not. In the trivial case we have $\frac{\mathbb{Z}}{4} \times \frac{\mathbb{Z}}{2}$. In the nontrivial case, we have

   $$\frac{\mathbb{Z}}{4} \rtimes \frac{\mathbb{Z}}{2}$$

   which is nonabelian so it is D_4.
4. Last case: every element of $G \setminus \langle x \rangle$ has order 4. Pick $y \in G \setminus \langle x \rangle$. Then $y^2 \in \langle x \rangle$, so in particular $y^2 = x^2$. Our full list of group elements: $1, x, x^2, x^3, y, yx, yx^2, yx^3$. We call $x^2 = -1$, and $x = i$, $x^3 = -i$. Call $y = j$, $yx = -k, yx^2 = -j, yx^3 = k$. This group is the quaternion group Q.

8 February 8

We classify groups of order p^3 where p is an odd prime. When we did the groups of order 8, they were built up from cyclic groups by using direct products and semidirect products, with the exception of the quaternion group. It had elements of order 4, call it i, $\langle i \rangle$ complement also only had elements of order 4.

- Suppose there exists x of order p^3, then G is cyclic.
- Suppose $x^p = 1$ for all $x \in G$. Noting a result, $|G| = p^k$ $k \geq 1$ implies $Z \neq \{1\}$. Pick x of order p in Z, and $y \in G \setminus \langle x \rangle$. Then $\langle x, y \rangle$ is abelian, and

  $$\langle x, y \rangle \cong \frac{\mathbb{Z}}{p} \times \frac{\mathbb{Z}}{p}$$

  Also pick $w \in G \setminus \langle x, y \rangle$ be an element. Then

  $$G \cong \left(\frac{\mathbb{Z}}{p} \times \frac{\mathbb{Z}}{p}\right) \rtimes \frac{\mathbb{Z}}{p}$$

where the last copy is $\langle w \rangle$. Also pick

$$\alpha : \frac{\mathbb{Z}}{p} \to \text{Aut}\left(\frac{\mathbb{Z}}{p} \times \frac{\mathbb{Z}}{p}\right) = \text{GL}_2\left(\mathbb{F}_p\right)$$

Last time we calculated

$$|\text{GL}_2(\mathbb{F}_p)| = (p^2-1)(p^2-p)$$

The highest power of p dividing it is p. If α is nontrivial, then its image is a p-Sylow of $\text{GL}_2(\mathbb{F}_p)$, and all such are conjugate. We have two options.

- $\frac{\mathbb{Z}}{p} \times \frac{\mathbb{Z}}{p} \times \frac{\mathbb{Z}}{p}$ which is aelian if α is trivial.
- α is nontrivial $\left(\frac{\mathbb{Z}}{p} \times \frac{\mathbb{Z}}{p}\right) \rtimes \frac{\mathbb{Z}}{p}$.

- $\exists x \in G$ of order p^2. Suppose $\exists y \in G \setminus \langle x \rangle$ of order p. Then $G \cong \frac{\mathbb{Z}}{p^2} \rtimes \frac{\mathbb{Z}}{p}$.

$$\alpha : \frac{\mathbb{Z}}{p} \to \text{Aut}(\frac{\mathbb{Z}}{p^2}) \cong \left(\frac{\mathbb{Z}}{p^2}\right)^\times \cong \frac{\mathbb{Z}}{p(p-1)}$$

(we will look next Thursday $\left(\frac{\mathbb{Z}}{p^n}\right)^\times$ as a group and verify that it is cyclic). Now $\frac{\mathbb{Z}}{p(p-1)}$ has a unique subgroup of order p. Two possibilities:

- α is trivial, so we have
$$\frac{\mathbb{Z}}{p^2} \times \frac{\mathbb{Z}}{p}$$
which is abelian, or
- α is nontrivial, so we have
$$\frac{\mathbb{Z}}{p^2} \rtimes \frac{\mathbb{Z}}{p}$$
which is nonabelian.

- Now suppose that we again have $x \in G$ with order p^2 and for all $y \in G \setminus \langle x \rangle$ y has order p^2. We will get a contradiction. So pick $y \in G \setminus \langle x \rangle$. Then y of course has order p^2. So y^p has order p. Hence $y^p \in \langle x \rangle$. Hence $y^p = x^{pr}$ for some $r \in \mathbb{Z}$. We have
$$\langle x^r \rangle = \langle x \rangle$$
because r is relatively prime to p. We can replace x^r with x, so we may by abuse of notation assume $r = 1$. Hence $x^p = y^p$. Suppose G is abelian, then yx^{p^2-1} has order p. Separately note $yx^{p^2-1} \in G \setminus \langle x \rangle$. We get a contradiction however because of our claim about $G \setminus \langle x \rangle$. Hence G is not abelian. Then by a result from the homework, $|Z| = p$ so $|Z| = \langle x^p \rangle = \langle y^p \rangle$. We have $\frac{G}{Z}$ has order p^2 and is abelian because of that. Hence $G' \subset Z$. In particular, $[x, y] \in Z$. We utilize exercise 10. We have
$$x^n y^n = (xy)^n [x, y]^{\binom{n}{2}}$$
So $[x, y^{-1}] \in Z$ so
$$x^p y^{-p} = (xy^{-1})^p [x, y^{-1}]^{\binom{p}{2}}$$
now $x^p = y^p$ implies the left is the identity. Now $[x, y^{-1}] \in Z$, and $|Z| = p$, so $[x, y^{-1}]^p = 1$. But $\binom{p|(p}{2}$ for odd primes. So we have xy^{-1} has order p. But then xy^{-1} is an element of order p in $G \setminus \langle x \rangle$, a contradiction.

The same argument above doesn't work when $p = 2$. Note the Quaternion group, as $Q \setminus \langle i \rangle$ has only elements of order $4 = 2^2$. Recall that if
$$1 \to N \to G \to Q \to 1$$
is an exact sequence of groups, then we say G is an extension of Q by N. This gets us to the following notion.

Definition 5. G is called **simple** if its only normal subgroups are $\{1\}$ and G.

Every finite group is "built" from simple groups and extensions. What are finite simple groups?

- $\frac{\mathbb{Z}}{p}$
- A_n for $n \geq 5$.
- Some Lie groups and matrix groups $\mathrm{PSL}_n(\mathbb{F}_q)$ or $U_n(\mathbb{F}_q)$. Symplectic and orthogonal groups yadda yadda
- 26 sporadic simple groups

We prove next that for $n \geq 5$, A_n is simple.

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

As a first remark, note A_n is generated by 3-cycles.

Lemma 5. If $n \geq 5$, then all 3-cycles are conjugate in A_n.

Proof. Let (1 2 3) and $(a\ b\ c)$ be 3-cycles. Consider

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ a & b & c & ? & \dots & ? \end{pmatrix}$$

In the way we constructed π,

$$\pi(1\ 2\ 3)\pi^{-1} = (a\ b\ c)$$

If $\pi \in A_n$ we are done. If $\pi \notin A_n$, we can compose it with a 2-cycle, say (4 5). Then the resulting permutation does the same. □

Proof. (of the big theorem) Let $N \neq \{e\}$ be a normal subgroup of A_n.

1. If N contains a three cycle, we are done. Since in that case N contains all 3-cycles, so $N = A_n$.
2. For the remaining cases, let $\sigma \neq e$ be an element of N. Write σ as a product of disjoint cycles. Suppose σ includes a cycle of length ≥ 4. So $\sigma = (1\ 2\ \dots\ \tau)\zeta$ where $\tau \geq 4, \zeta$ disjoint. Note

$$\begin{aligned}[(1\ 2\ 3), \sigma] &= (1\ 2\ 3)(1\ 2\ \dots\ \tau)(1\ 2\ 3)^{-1}(\tau\ \tau-1\ \dots\ 2\ 1) \\ &= (2\ 3\ 1\ 4\ \dots\ \tau)(\tau\ \tau-1\ \dots\ 3\ 2\ 1) \\ &= (1\ 2\ 4) \in N\end{aligned}$$

   So N contains a 3-cycle, and we are done.
3. Now suppose σ consists of a three cycle and some disjoint 2 cycles. Then σ^2 is a 3-cycle and we're done.
4. Now suppose σ consists of multiple three cycles and disjoint 2 cycles. By squaring it, we may assume there are no 2-cycles. So

$$\sigma = (1\ 2\ 3)(4\ 5\ 6)\zeta$$

   where ζ is disjoint.

$$\begin{aligned}[(1\ 2\ 4), \sigma] &= (1\ 2\ 4)(1\ 2\ 3)(4\ 5\ 6)(4\ 2\ 1)(3\ 2\ 1)(6\ 5\ 4) \\ &= (2\ 4\ 3)(1\ 5\ 6)(3\ 2\ 1)(6\ 5\ 4) = (1\ 2\ 5\ 3\ 4)\end{aligned}$$

   so we are done by 2.

5. Finally, suppose σ consists of just 2 cycles. Each element of N is a product of (an even number) disjoint 2-cycles. Let $\sigma = (1\ 2)(3\ 4)\zeta \in N$, ζ is disjoint. Playing the same game,

$$[(1\ 2\ 3), \sigma] = (1\ 2\ 3)(1\ 2)(3\ 4)(1\ 2\ 3)^{-1}(2\ 1)(4\ 3)$$

$$(2\ 3)(1\ 4)(2\ 1)(4\ 3) = (1\ 3)(2\ 4) \in N$$

Now we have

$$\begin{aligned}[(1\ 3\ 5), (1\ 3)(2\ 4)] &= (1\ 3\ 5)(1\ 3)(2\ 4)(1\ 3\ 5)^{-1}(3\ 1)(4\ 2) \\ &= (3\ 5)(2\ 4)(3\ 1)(4\ 2) \\ &= (1\ 5\ 3) \in N\end{aligned}$$

Which completes the proof!

□

In a future point, we may discuss $\mathrm{PSL}_n(\mathbb{F}_q)$. Also, we may discuss $\mathrm{Aut}S_n$. As mentioned before, we will also discuss $\mathrm{Aut}\frac{\mathbb{Z}}{p^n}$.

Automorphism groups of cyclic groups in general. An infinite cyclic group $\mathbb{Z}$, we have

$$\mathrm{Aut}\mathbb{Z} = \frac{\mathbb{Z}}{2}$$

The elements are multiplication by ± 1. So $\mathrm{Aut}\mathbb{Z} \cong \frac{\mathbb{Z}}{2}$.

$$\mathrm{Aut}\left(\frac{\mathbb{Z}}{n}\right) = \left(\frac{\mathbb{Z}}{n}\right)^{\times}$$

What is $\left(\frac{\mathbb{Z}}{n}\right)^{\times}$? Suppose $n = p_1^{e_1} \cdots p_k^{e_k}$ where p_i are distinct primes. The Chinese remainder theorem yields

$$\frac{\mathbb{Z}}{n} \cong \frac{\mathbb{Z}}{p_1^{e_1}} \times \cdots \times \frac{\mathbb{Z}}{p_k^{e_k}}.$$

A k-tuple is a unit precisely if each coordinate is a unit. So

$$\left(\frac{\mathbb{Z}}{n}\right)^{\times} \cong \left(\frac{\mathbb{Z}}{p_1^{e_1}}\right)^{\times} \times \cdots \times \left(\frac{\mathbb{Z}}{p_k^{e_k}}\right)^{\times}$$

This finally gets us to the question of $\mathrm{Aut}\left(\frac{\mathbb{Z}}{p^e}\right)$ when p is prime. This is the subject of the next lecture.

9 February 10

Recall a homework problem: Suppose G is a finite group in which $x^d = 1$ has at most d solutions for each d dividing its order. Then G is cyclic.

Corollary 4. The multiplicative group $\mathbb{F}^{\times}$ for a finite field $\mathbb{F}$ is cyclic.

In particular, we have

Corollary 5. If p is a prime, then $\left(\frac{\mathbb{Z}}{p}\right)^{\times}$ is cyclic. A generator is called a primitive root mod p.

Last time, what we mentioned was that if n is a positive integer, and $n = \prod p_i^{e_i}$ where p_i are distinct, the Chinese remainder theorem yields

$$\frac{\mathbb{Z}}{n} \cong \prod_i \left(\frac{\mathbb{Z}}{p_i^{e_i}}\right)$$

Likewise, we get

$$\left(\frac{\mathbb{Z}}{n}\right)^\times \cong \prod_i \left(\frac{\mathbb{Z}}{p_i^{e_i}}\right)^\times$$

Now what is $\left(\frac{\mathbb{Z}}{p^e}\right)^\times$? We do know

$$\left|\left(\frac{\mathbb{Z}}{p^e}\right)^\times\right| = \varphi(p^e) = p^e - p^{e-1}$$

the Euler phi function.

Theorem 6. Suppose p is an odd prime. Then $\left(\frac{\mathbb{Z}}{p^e}\right)^\times$ is cyclic of order $p^e - p^{e-1}$.

Proof. $e = 1$ is covered by an above corollary. Now about the general case. We have a canonical surjection

$$\frac{\mathbb{Z}}{p^e} \twoheadrightarrow \frac{\mathbb{Z}}{p}$$

If we have a ring element on the left that is a unit, it maps to a unit on the right. So we have

$$\frac{\mathbb{Z}}{p^e}^\times \twoheadrightarrow \frac{\mathbb{Z}}{p}^\times$$

So $\left(\frac{\mathbb{Z}}{p}\right)^\times$ has an element of order $p-1$, namely a primitive root. The inverse image of such an element has order $(p-1)\cdot p^k$, $k \leq e-1$. Some power of the inverse image has order $p-1$. In $\left(\frac{\mathbb{Z}}{p^e}\right)^\times$, we have proved the existence of an element α of order $p-1$. Next we want $\beta \in \left(\frac{\mathbb{Z}}{p^e}\right)^\times$ of order p^{e-1}. If we do have such an element, $\alpha\beta$ has order $(p-1)p^{e-1}$ since the group is commutative. Now a big claim. $\beta = 1+p$ has order p^{e-1}. So far, we haven't used the fact that p is odd. We have

$$\begin{aligned}\beta^{p^{e-1}} &\equiv 1 + \binom{p^{e-1}}{1}p + \binom{p^{e-1}}{2}p^2 + \ldots + p^{p^{e-1}} \mod p^e \\ &\equiv 1\end{aligned}$$

So β has order p^{e-1} or some lower power of p. We have

$$\begin{aligned}\beta^{p^{e-2}} &\equiv 1 + \binom{p^{e-2}}{1}p + \binom{p^{e-2}}{2}p^2 + \ldots + p^{p^{e-2}} \\ &\equiv 1 + p^{e-1} \not\equiv 1\end{aligned}$$

□

Theorem 7. Suppose $e \geq 3$, then $\left(\frac{\mathbb{Z}}{2^e}\right)^\times \cong \frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2^{e-2}}$.

Proof. $\pm 1, \pm\left(2^{e-1}-1\right)$, are roots of $x^2 = 1$ since

$$\left(2^{e-1}-1\right)^2 = 2^{2(e-1)} - 2\cdot 2^{e-1} + 1$$
$$= 2^{2e-2} - 2^e + 1$$

So $\left(\frac{\mathbb{Z}}{2^e}\right)^\times$ cannot be cyclic. Enough to find an element β of order 2^{e-2}. Use the Abelian group structure theorem to prove the claim from there. We claim $\beta = 5 = 1+2^2$ is up for the job.

$$(1+2^2)^{2^{e-2}} = 1 + \binom{2^{e-2}}{1}2^2 + \binom{2^{e-2}}{2}2^4 + \ldots + 2^{2(e-2)} \mod 2^e$$
$$\equiv 1 \mod 2^e$$

Likewise, as in the previous proof, $(1+2^2)^{2^{e-3}} \not\equiv 1$.

$$(1+2^2)^{2^{e-3}} = 1 + \binom{2^{e-3}}{1}2^2 + \binom{2^{e-3}}{2}(2^2)^2 + \ldots + (2^2)^{2^{e-3}}$$
$$\equiv 1 + 2^{e-1}$$

□

Consider $Q = \{\pm_1, \pm i, \pm j, \pm k\}$. What is $\mathrm{Aut}(Q)$? As we will see on the homework, it will be S_4. What we will at least comment on is $|\mathrm{Aut}(Q)| = 4!$. An automorphism does preserve order, so $\varphi \in \mathrm{Aut}(Q)$ implies that $\varphi(-1) = -1$. $\varphi(i) = \{\pm i, \pm j, \pm k\}$. Now note that $\varphi(i)$ narrows down choices for $\varphi(j)$. From there, $\varphi(i), \varphi(j)$ determine the whole automorphism.

$$\varphi(j) = \{\pm i, \pm j, \pm k\} \setminus \{\pm\varphi(i)\}$$

This gives us an upper bound on $|\mathrm{Aut}(Q)|$ by $4!$.

Exercise 3

Tedious exercise: prove that having chosen $\varphi(i), \varphi(j)$ appropriately defines an automorphism.

The topic we want to understand is $\mathrm{Aut}(S_n)$. Some remarks:

- If $n \geq 3$, then $Z(S_n) = \{e\}$.

  Proof. Suppose $\sigma \neq e$ in S_n. Let $a \neq b$ be elements with $\sigma(a) = b$. There is a third letter c by $n \geq 3$. Note $(b\ c)\sigma \neq \sigma(b\ c)$. □

- If $n \geq 5$, then the only normal subgroups of S_n are $\{e\}, A_n, S_n$.

  Proof. Suppose $N \lhd S_n$. Then $A_n \cap N \lhd A_n$. From last time though, we proved that A_n is simple for $n \geq 5$. So $A_n \cap N = A_n$ or $A_n \cap N = \{e\}$. In the former, A_n has index 2 implies $A_n = N$ or $S_n = N$. In the latter, if $N \neq \{e\}$, then it has an element that is not in A_n.

  $$NA_n = S_n$$

  N and A_n are both normal implies then that we can write S_n as a direct product. This implies $|N| = 2$. In other words there is a nontrivial 2-cycle that is in the center, a contradiction to $Z(S_n) = \{e\}$. □

We note more things about $\mathrm{Aut}(S_n)$.

1. Let $\varphi \in \mathrm{Aut}(S_n)$. Then φ takes conjugate elements to conjugate elements. Given x, yxy^{-1},

   $$\varphi(x)$$

   is conjugate to

   $$\varphi(y)\varphi(x)\varphi(y)^{-1}$$

2. More interesting is if $\varphi \in \mathrm{Aut}(S_n)$, if φ takes 2-cycles to 2-cycles, then $\varphi \in \mathrm{Inn}(S_n)$.
3. Say $\varphi(1\ 2) = (a\ b)$. If $\varphi(1\ 3) = (c\ d)$ for $c, d \notin \{a, b\}$. Now $(a\ b)$ and $(c\ d)$ commute but $\varphi(1\ 2)$ and $\varphi(1\ 3)$ don't. We may write

$$\varphi(1\ 2) = (a\ b)$$
$$\varphi(1\ 3) = (a\ c)$$

We have

$$\varphi(1\ 4) = (a\ d) \text{ or } (b\ c)$$

In the latter case, then

$$(a\ b)(a\ c)(b\ c) = (a\ c)$$

Apply φ^{-1}.

$$(1\ 2)(1\ 3)(1\ 4) = (1\ 3)$$

a contradiction. Hence $\varphi(1\ 4) = (a\ d)$. We can keep labeling so that $\varphi(1\ x) = (a\ y)$. Define $\pi \in S_n$ by

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \dots \\ a & b & c & d & \dots \end{pmatrix}$$

We would like to show that φ is conjugation by π. Conjugation by π the cycles $(1\ x)$ yields φ.

We can write

$$S_n/Z(S_n) \cong \mathrm{Inn}(S_n) \lhd \mathrm{Aut}(S_n)$$

Conjugacy classes of elements of order 2 in S_n. On the one hand we have the class of $(1\ 2)$, $(1\ 2)(3\ 4)$, $(1\ 2)(3\ 4)(5\ 6)$, etc etc. In the first form, we have $\binom{n}{2}$ such elements. In the second we have $\frac{1}{2!}\binom{n}{2}\binom{n-2}{2}$. In the third form $\frac{1}{3!}\binom{n}{2}\binom{n-2}{2}\binom{n-4}{2}$. The conjugacy class of $(1\ 2)(3\ 4)\dots(2k-1\ 2k)$ has size

$$\frac{1}{k!}\binom{n}{2}\binom{n-2}{2}\cdots\binom{n-2k+2}{2}$$

$$= \frac{1}{k!}\frac{n(n-1)\cdots(n-2k+2)(n-2k+1}{2^k}$$

So if φ takes the conjugacy classes of $(1\ 2)$ to the conjugacy class of $(1\ 2)(3\ 4)\dots(2k-1\ 2k)$, we have

$$\binom{n}{2} = \frac{1}{k!}\frac{n(n-1)\dots(n-2k+2)(n-2k+1)}{2^k}$$

$$= \frac{n(n-1)}{2}$$

So

$$\frac{(n-2)(n-3)\cdots(n-2k+1)}{k!2^k} = \frac{1}{2}$$

$$= \binom{n-2}{n-2k} = \frac{k!\cdot 2^k}{(2k-2)!}$$

$$= \frac{k}{(2k-3)(2k-5)\dots\cdot 3\cdot 1} \le \frac{k}{2k-3}$$

$$< 1 \text{ if } k > 3$$

so φ cannot change the conjugacy class of an element $(1\ 2)$ to $(1\ 2)(3\ 4)\dots(2k-1\ 2k)$ if $k > 3$. $k = 1 : \varphi$ takes 2-cycles to 2-cycles, so we have that the above formula that was contradicted is true. If $k = 2$, we have

$$\binom{n-2}{n-2k} = \frac{k!\cdot 2^k}{2(2k-2)!}$$

implies

$$\binom{n-2}{n-4} = \frac{2 \cdot 2^2}{2 \cdot 2!}$$
$$= \binom{n-2}{2} = 2$$

but $\binom{*}{2}$ is never 2. In the case $k = 3$,

$$\binom{n-2}{n-6} = \frac{3! \cdot 2^3}{2(4!)}$$
$$\binom{n-2}{4} = 1$$

so $n = 6$. So for $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$ if $n \neq 6$. We could say

$$\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n) \cong S_n \text{ if } n \neq 2, 6$$

We have $\mathrm{Aut}(S_2) = \{e\}$. The only thing left to examine is $\mathrm{Aut}(S_6)$. Next time, we will show

$$\left| \frac{\mathrm{Aut}(S_6)}{\mathrm{Inn}(S_6)} \right| = 2$$

so there is a

$$1 \to S_6 \to \mathrm{Aut}(S_6) \to \frac{\mathbb{Z}}{2} \to 0$$

is exact.

10 February 15

From homework 2, the grader would like to make known a few common mistakes:

- $H < G \not\Rightarrow Z(H) < Z(G)$. Example: $\langle i \rangle < Q$
- $H \lhd N \lhd G \not\Rightarrow H \lhd G$ Example: $\langle (1\ 2)(3\ 4) \rangle \lhd \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \lhd S_4$. The middle group is normal because conjugation preserves cycle structure.
- $H \lhd N_H$ always but $N_H \not\lhd G$. $H = \langle (1\ 2) \rangle$ in S_3. We have N_H is the set of elements fixing the set $\{1, 2\}$, but this is not normal.

Last time If $n \neq 1, 2, 6$, then $\mathrm{Inn}S_n = \mathrm{Aut}S_n$. If $n = 1, 2$ then $\mathrm{Aut}(S_n) = \{e\}$, so $\mathrm{Inn}(S_n) = \mathrm{Aut}(S_n)$. Now what for $n = 6$? This is the case we will look at today.

Definition 6. We say that H is a **transitive** subgroup of S_n if it acts transitively on $\{1, \ldots, n\}$. In other words, $i, j \in \{1, \ldots, n\}$ there exists $h \in H$ with

$$h(i) = j$$

Example. Transitive subgroups of S_3: $\langle (1\ 2\ 3) \rangle$, S_3.

Transitive subgroups of S_4:

- $\langle (1\ 2\ 3\ 4) \rangle$, etc (cyclics generated by 4-cycles).
- D_4
- $\langle (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), e \rangle$
- A_4
- S_4

Transitive subgroups of S_5 :

- $\langle(1\ 2\ 3\ 4\ 5)\rangle$, etc.
- D_5
- $\frac{\mathbb{Z}}{5} \rtimes \frac{\mathbb{Z}}{4}$.
- A_5
- S_5

Lemma 6. If H is transitive in S_n and $\varphi \in \text{Inn}(S_n)$, then $\varphi(H)$ is transitive as well.

Proof. Say φ is conjugation by σ. Given $i, j \in \{1, \ldots, n\}$, choose element $h \in H$ such that $h(\sigma^{-1}(i)) = \sigma^{-1}(j)$. We have

$$\sigma \circ h \circ \sigma^{-1}(i) = j$$

This implies that $\varphi(H)$ is transitive. □

Lemma 7. There exists a transitive copy of S_5 in S_6. That is, there exists injection

$$S_5 \hookrightarrow S_6$$

such that the image is transitive.

Proof. S_5 has 4! elements of order 5 (elements of order 5 have to be 5 cycles, and there are 4! choices of said cycles). It also has $6 = 4!/4$ 5-Sylow subgroups. Let X be the set of 5-Sylow subgroups of S_5. We have a homomorphism

$$S_5 \to \text{Perm}(X) = S_6$$

via conjugation. The image of this homomorphism is transitive by the second Sylow theorem. In other words, the image has at least 6 elements. The kernel is a normal subgroup of S_5, but the only normal subgroup of S_5 is A_5, S_5, or $\{e\}$. Only $\{e\}$ fits the description. Hence $S_5 \hookrightarrow S_6$. □

Theorem 8. $\text{Inn}S_6$ is not $\text{Aut}S_6$.

Proof. Let H be a transitive subgroup of S_6 with $H \cong S_5$ as allowed in the lemma above. Then S_6 acts on $\frac{S_6}{H}$ by left translation $g \mapsto (hH \mapsto ghH)$. We have

$$S_6 \to \text{Perm}(\frac{S_6}{H}) \cong S_6$$

There are 6 left cosets. This action is transitive as well. The image of S_6 is thus a transitive subgroup of S_6, and so by the same reasoning in the lemma, the map is actually injective. The domain and codomain have the same order, so the map is actually bijective. Call the isomorphism $\varphi : S_6 \to S_6$. Suppose for contradiction that φ is inner automorphism. Now note that by the lemma even further above, $\varphi(H) = \{e\}$ is a transitive subgroup, a contradiction. □

The counting argument shows that any element of $\text{Aut}(S_n) \setminus \text{Inn}S_n$ is exchanging the conjugacy class of (1 2) with the class of (1 2)(3 4)(5 6). That is, given an outer automorphism, it maps the class of (1 2) to (1 2)(3 4)(5 6), and applying any outer automorphism again puts the class back. Hence the composition of any two non-inner automorphisms is an inner automorphism. That is, $\varphi_1, \varphi_2 \in \text{Aut}S_6 \setminus \text{Inn}S_6$ implies $\varphi_1 \circ \varphi_2 \in \text{Inn}(S_6)$. Hence

$$|\text{Aut}S_6/\text{Inn}S_6| = 2$$

So we have that

$$\{e\} \to \mathrm{Inn}S_6 \to \mathrm{Aut}S_6 \to \frac{\mathbb{Z}}{2} \to \{0\}$$

is exact. Also note $\mathrm{Inn}S_6 \cong S_6$. Does the sequence split? Yes, because there exists $\varphi \in \mathrm{Aut}S_6 \setminus \mathrm{Inn}S_6$ (verify this)! But the proof is done by calculation! Suppose $n \geq 5$, and S_n is acting transitively on $\{1, \ldots, n\}$. This gives

$$S_n \to S_n = \mathrm{Perm}\left(\{1, \ldots, n\}\right)$$

What does it mean for an automorphism to be inner? Suppose φ is conjugation by σ. Relabel i has $\sigma^{-1}(i)$. Then say $\pi = (i\ j)$.

$$\varphi(\pi)\left(\sigma(i)\right) = \sigma(j)$$

(ask about this0

Let G be a group. Let $Z(G)$ be its center. Then $Z(G) \lhd G$. We can thus discuss $\frac{G}{Z(G)}$ and its center $Z\left(\frac{G}{Z(G)}\right)$, and so on.

Definition 7. Set $Z_0 = \{e\}$. $Z_1 = Z(G)$. Set Z_i to be the inverse image of $Z\left(\frac{G}{Z_i}\right)$ under

$$G \to \frac{G}{Z_i}$$

In other words, $Z_{i+1}/Z_i = Z\left(\frac{G}{Z_i}\right)$. In particular,

$$\frac{Z_{i+1}}{Z_i} = Z\left(\frac{G}{Z_i}\right)$$

We have $Z_{i+1} \lhd G$ for all i. This is even stronger than nested normality by the initial comments. We have

$$Z_0 = \{e\} \lhd Z_1 \lhd Z_2 \lhd \ldots$$

which are all normal in G. The definition is G is **nilpotent** if $Z_k = G$ for some k. In ways, this measures how close the group is to being abelian. In this case,

$$\{e\} = Z_0 \lhd Z_1 \lhd Z_2 \lhd \ldots \lhd Z_k = G$$

but note by the previous remark $\frac{Z_{i+1}}{Z_i} = Z\left(\frac{G}{Z_i}\right)$ which is abelian. Hence G is solvable.

- Abelian groups are nilpotent.
- A p-group has nontrivial center. If the center is not the whole group, the center is also a p-group. We can mod out, and repeat the process. Hence, we have
- Every p-group is nilpotent.
- H, K are nilpotent implies that $H \times K$ is nilpotent.

  Proof. $Z(H \times K) = Z(H) \times Z(K)$. □

Theorem 9. A finite group is nilpotent if and only if it is a product of its p-Sylow subgroups.

Lemma 8. Suppose G is nilpotent, and $H < G$. If $H \neq G$, then $N_H \gneq H$.

Proof. Let n be the largest integer with $Z_n \subset H$. Then $Z_{n+1} \not\subset H$, so $\exists a \in Z_{n+1} \backslash H$. We have $aZ_n \in Z\left(\frac{G}{Z_n}\right)$. For each $h \in H$, one has $aZ_nhZ_n = hZ_naZ_n$. So $aha^{-1}h^{-1} \in Z_n \subset H$. Hence $aha^{-1} \in H$. Hence $a \in N_H \setminus H$. □

Lemma 9. Let G be a finite group and P be a Sylow subgroup of G. Then $N_{N_P} = N_P$.

11 February 17

Define $Z_i \lhd G$ using $Z_0 = \{e\}$. That gave us $Z_{i+1}/Z_i = Z\left(\frac{G}{Z_i}\right)$. This also gave us

$$\{e\} = Z_0 \lhd Z_1 \lhd Z_2 \lhd \dots$$

G is **nilpotent** if $Z_k = G$ for some k. Abelian groups are surely nilpotent, and so are p-groups. The product of nilpotent groups if nilpotent. What did we prove last time? If G is nilpotent and $H < G$, then $H \neq G$ implies $H \subsetneq N_H$. We attempted to prove a lemma last time but didn't complete:

Lemma 10. If P is a p-Sylow of G, then $N_{N_P} = N_P$.

Proof. We automatically have $N_P \subset N_{N_P}$. We have left to show that if $x \in N_{N_P}$, then $x \in N_P$. We have

$$xN_Px^{-1} = N_P$$

$P \lhd N_P$, so $xPx^{-1} \lhd xN_Px^{-1} = N_P$. But then xPx^{-1} is a p-Sylow of N_P, hence $xPx^{-1} = P$ (normalness $P \lhd N_P$ implies that P is the unique p-Sylow). Hence $x \in N_P$. □

Theorem 10. Let G be a finite group. The following are equivalent:

1. G is a direct product of Sylow subgroups.
2. G is nilpotent.
3. Each Sylow subgroup of G is normal in G

Proof. 1 implies 2 is automatic from the fact that p-groups are nilpotent.

To show 2 implies 3, let P be a Sylow subgroup. If $N_P \neq G$, then $N_P \subsetneq N_{N_P}$. But this is not the case by the lemma we have just proven, so $N_P = G$. Hence P is normal.

To show 3 implies 1, let $P_1, P_2, \dots, P_k$ be the normal Sylows. Since each Sylow is normal, each Sylow is the only Sylow corresponding to its prime. They correspond to distinct primes dividing $|G|$. If $i \neq j$, $[P_i, P_j]$ is what? If $x \in P_i, y \in P_j$,

$$xyx^{-1}y^{-1} \in P_i \cap P_j$$

by the normality of P_i, P_j (for instance $xyx^{-1} \in P_j$ and so the product is in P_j. Same for P_i). Hence $[P_i, P_j] = \{e\}$ since there are no nontrivial subgroups of a prime order group. Define $P_1 \times P_2 \times \dots \times P_k \to G$ by the multiplication map. It is a homomorphism by the property we just proved. It is injective (work out this argument, it is done via orders), and the equality of cardinalities implies it is surjective. We have an isomorphism. □

We have shown nilpotent groups are solvable. A solvable that is not nilpotent is S_3, since its 2-Sylows are not normal.

We talked about

$$\{e\} \lhd Z_1 \lhd Z_2 \lhd \dots \lhd G$$

an ascending series to be contrasted with

$$G = G^{(0)} \rhd G^{(1)} \rhd G^{(2)} \rhd \dots$$

(the commutators) which is a descending series. There is one more:

$$C_{i+1} = [C_i, G]$$

where $C_0 = G$. It is also a descending series. We get

$$C_0 \rhd C_1 \rhd C_2 \rhd \dots$$

Theorem 11. G is a nilpotent (namely $Z_k = G$ for some k) if and only if $C_n = \{e\}$ for some n. Even better, if $Z_k = G$ then $C_i \subset Z_{k-i}$ for all i. If $C_k = \{e\}$, then $C_{k-i} \subset Z_i$ for all i. The least k is called the **nilpotency class of** G, which measures how far G is from being abelian.

Proof. It suffices to show the latter stronger statements. We do these by induction on i. This statement is true for $i = 0$ because $C_0 = G \subset Z_k = G$. Suppose the statement is true for $i - 1$, so $C_{i-1} \subset Z_{k-i+1}$. We h ave

$$C_i = [C_{i-1}, G] \subset [Z_{k-i+1}, G].$$

We hope that the latter is $\subset Z_{k-i}$. We have

$$\frac{Z_{k-i+1}}{Z_{k-i}} = Z\left(\frac{G}{Z_{k-i}}\right)$$

For the second stronger statement, note $C_k = \{e\} \subset Z_0 = \{e\}$. Inductively assume $C_{k-i+1} \subset Z_{i-1}$. Then $C_{k-i+1} = [C_{k-i}, G] \subset Z_{i-1}$. Hence the image of C_{k-i} in G/Z_{i-1} lies in $Z\left(\frac{G}{Z_{i-1}}\right) = \frac{Z_i}{Z_{i-1}}$. Hence $C_{k-i} \subset Z_i$. □

We saw that A_n is simple for $n \geq 5$. In the context of the classification of simple finite groups. We will talk about when $\mathrm{PSL}_n(\mathbb{F}_q) = \mathrm{SL}_n(\mathbb{F}_q)/\mathbb{Z}$ is simple.

Theorem 12. (Schreier)Two normal towers of a group G ending with $\{e\}$ have equivalent refinements. In other words, we can refine each to

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \dots \rhd G_k = \{e\}$$

such that the same G_i/G_{i+1} show up up to permutation and isomorphism.

Proof. (Sketch)

$$G = G_0 \rhd G_1 \rhd \dots \rhd G_r = \{e\}$$

and another

$$H_0 \rhd H_1 \rhd \dots \rhd H_s = \{e\}$$

Define $G_{ij} = G_{i+1}\,(H_j \cap G_i)$ and

$$G = G_0 = G_{00} \rhd G_{01} \rhd G_{02} \rhd \dots \rhd G_{0s} = G_1 = G_{10} \rhd G_{11} \rhd \dots \rhd G_{1s} = G_2 \rhd \dots$$

and so on until you reach G_r. Likewise, we can define $H_{ji} = (G_i \cap H_j)\,H_{j+1}$ and we have

$$\frac{G_{ij}}{G_{i,j+1}} = \frac{G_{i+1}(H_j \cap G_i)}{G_{i+1}(H_{j+1} \cap G_i)} \cong \frac{(G_i \cap H_j)H_{j+1}}{(G_{i+1} \cap H_j)H_{j+1}} = \frac{H_{ji}}{H_{j,i+1}}$$

by what is called Zassenhaus's lemma. Again, this is a proof sketch! □

Example. $S_4 \rhd A_4 \rhd \{e\}$ a normal tower. We could also get a normal tower

$$S_4 \rhd \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} = P \rhd \{e\}$$

We could get

$$S_4 \rhd A_4 \rhd P \rhd \{e, (1\ 2)(3\ 4)\} \rhd \{e\}$$

which is a refinement of the first tower where every quotient is simple. The building blocks are

$$\frac{\mathbb{Z}}{2}, \frac{\mathbb{Z}}{3}, \frac{\mathbb{Z}}{2}, \frac{\mathbb{Z}}{2}$$

It refines both towers!

Theorem 13. (Jordan-Holder Theorem) Suppose we have a normal tower

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_k = \{e\}$$

with $\frac{G_i}{G_{i+1}}$ simple for all i. Then we have that any other tower with the same property has the same simple groups showing up in it up to permutation and isomorphism.

Proof. (sketch) This is an immediate consequence of Schreier's theorem. If we tried to refine such a tower we could not actually do so, because each consecutive pair has simple quotient. □

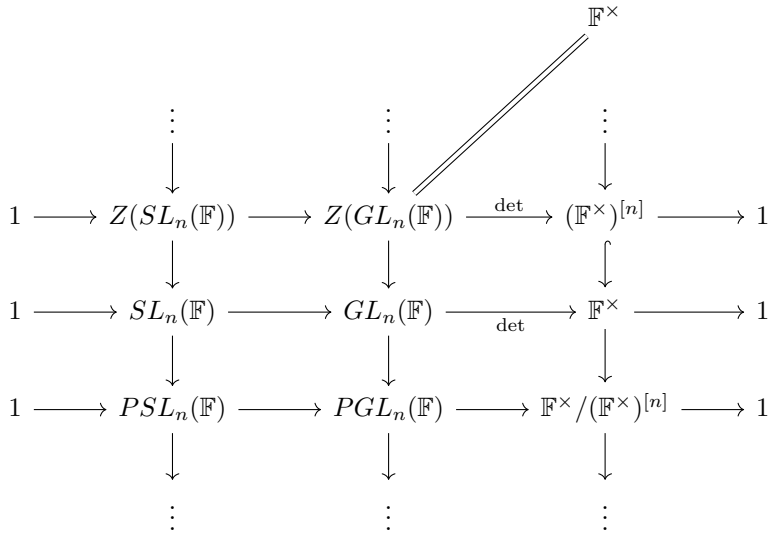
Example.

$$\frac{\mathbb{Z}}{6} \rhd \frac{\mathbb{Z}}{3} \rhd 0$$
$$\frac{\mathbb{Z}}{6} \rhd \frac{\mathbb{Z}}{2} \rhd 0$$

Moving on, let $\mathbb{F}$ be a field. We have sequence

$$1 \to \mathrm{SL}_n(\mathbb{F}) \to \mathrm{GL}_n(\mathbb{F}) \xrightarrow{\det} \mathbb{F}^\times \to 1$$

which is exact. We know $Z\left(\mathrm{SL}_n(\mathbb{F})\right)$ is the scalar multiples of id. We temporarily define $(\mathbb{F}^\times)^{[n]}$ to be n-th powers in $\mathbb{F}^\times$.



Say $\mathbb{F}_q$ is a field with q elements. We have

$$|SL_n(\mathbb{F}_q)| = \frac{(q^n - 1)(q^n - q)\cdots(q^n - q^{n-1})}{q - 1}$$

We have

$$|PSL_n(\mathbb{F}_q)| = \frac{(q^n-q)(q^n-q)\cdots(q^n-q^{n-1})}{(q-1)gcd(n,q-1)}$$

Number of roots of x^n-1 in $\mathbb{F}_q^\times$ is $gcd(n,q-1)$.

Theorem 14. $PSL_n(\mathbb{F}_q$ is simple if $\begin{cases} n \geq 3 \\ n = 2 \text{ and } q \geq 4 \end{cases}$.

Proof. We prove $n=2$ case in the next lecture. Note

$$|PSL_2(\mathbb{F}_q)| = \frac{(q^2-1)(q^2-q)}{(q-1)gcd(2,q-1)}.$$

If $q=2$,

$$|PSL_2(\mathbb{F}_2)| = 6$$

so $q=2$ must be an exception; no group of order 6 is simple. At $q=3$,

$$|PSL_2(\mathbb{F}_3)| = 12$$

Some more info:

$$PSL_2(\mathbb{F}_4) \approx A_5 \approx PSL_2(\mathbb{F}_5)$$

$$PSL_4, PSL_3(\mathbb{F}_4) \text{ are simple non isomorphic order 20160}$$

20160 is the smallest number that you have nonisomorphic simple groups by coincidence. We complete this theorem's proof next class. □

12 February 22

Let $\mathbb{F}$ be a field. Let

$$Z\left(SL_n(\mathbb{F})\right) = \left\{ \begin{pmatrix} d & 0 & \dots & 0 \\ 0 & d & \ddots & 0 \\ 0 & 0 & \dots & d \end{pmatrix} | d^n = 1 \right\}$$

$PSL_n(\mathbb{F}) = SL_n(\mathbb{F})/Z\left(SL_n(\mathbb{F})\right)$ A **transvection** is a matrix of the form

$$\begin{pmatrix} 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & \dots & b_{ij} & \dots & 0 \\ 0 & 0 & 1 & \ddots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

$$= I + be_{ij} = T_{ij}(b)$$

$b \in \mathbb{F} \setminus \{0\}$, $i \neq j$.

Theorem 15. $SL_2(\mathbb{F})$ and more generally $S_n(\mathbb{F})$ is generated by transvections.

Proof. $T_{ij}(b)M$ adds a multiple of one row to another in M given $M \in M_n(\mathbb{F})$. Multiplying an element of $SL_2(\mathbb{F})$ by transvections gets us to (via such row operations)

$$\begin{pmatrix} d & 0 \\ 0 & d^{-1} \end{pmatrix} \text{ or } \begin{pmatrix} 0 & -d^{-1} \\ d & 0 \end{pmatrix}$$

$$\begin{pmatrix} d & 0 \\ 0 & d^{-1} \end{pmatrix} \xrightarrow{\text{left mult. by } T_*()} \begin{pmatrix} d & 0 \\ d & d^{-1} \end{pmatrix}$$
$$\mapsto \begin{pmatrix} 0 & -d^{-1} \\ d & d^{-1} \end{pmatrix} \mapsto \begin{pmatrix} 0 & -d^{-1} \\ d & 0 \end{pmatrix}$$
$$\mapsto \begin{pmatrix} 0 & -d^{-1} \\ d & -d^{-1} \end{pmatrix} \mapsto \begin{pmatrix} 1 & -d^{-1} \\ d & 0 \end{pmatrix}$$
$$\mapsto \begin{pmatrix} 1 & -d^{-1} \\ 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

□

The following lemma is useful in the context of trying to show $PSL_2(\mathbb{F}_q)$ is simple.

Lemma 11. If $H \lhd SL_2(\mathbb{F}_q)$ and H contains a transvection, then $H = SL_2(\mathbb{F}_q)$.

Proof. Say $T_{12}(\mu) = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} \in H$, $\mu \neq 0$ (similar case for T_{21}). Let's conjugate:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$
$$= \begin{pmatrix} 1 - \mu ac & \mu a^2 \\ -\mu c^2 & 1 + \mu ac \end{pmatrix}$$

for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{F}_q)$. Taking $c = 0$ gives us

$$\begin{pmatrix} 1 & \mu a^2 \\ 0 & 1 \end{pmatrix} \in H$$

for $a \in \mathbb{F}_q^\times$ by the normality of H. So

$$K = \left\{ \alpha \in \mathbb{F}_q | \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \in H \right\}$$

The above is a subgroup of $(\mathbb{F}_q, +)$. We have

$$\left|\mathbb{F}_q^\times\right| = q - 1$$

We have

$$\left|\{a^2 | a \in \mathbb{F}_q^\times\}\right| \geq \frac{q-1}{2}$$

So $|K| \geq \frac{q-1}{2} + 1$ where 1 is the identity in $SL_2(\mathbb{F})$. Hence $K = \mathbb{F}_q$, since its order is greater than the order of the largest strict subgroup.

$$a = 0 \Rightarrow \begin{pmatrix} 1 & 0 \\ -\mu c^2 & 1 \end{pmatrix} \in H$$

By a similar argument each $\begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}$ is in H. So H has all transvections, so $H = SL_2(\mathbb{F}_q)$. □

Theorem 16. $PSL_2(\mathbb{F}_q)$ is simple if $q \geq 4$. If $n \geq 3$, $PSL_n(\mathbb{F}_q)$ is simple.

Proof. Suppose there is a normal subgroup greater than the center of $SL_2(\mathbb{F}_q)$, $Z \subsetneq H \triangleleft SL_2(\mathbb{F}_q)$. We want to show $H = SL_2(\mathbb{F}_q)$. By the correspondence theorem this suffices to prove the theorem for $n = 2$. Equivalently we want to show that H contains a transvection by the preceding lemma. Suppose $\begin{pmatrix} \frac{1}{t} & 0 \\ s & t \end{pmatrix} \in H$, then

$$\left[\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} \frac{1}{t} & 0 \\ s & t \end{pmatrix}\right] = \begin{pmatrix} 1 & 0 \\ 1-t^2 & 1 \end{pmatrix} \in H$$

Suppose $\begin{pmatrix} 0 & -\frac{1}{\mu} \\ \mu & x \end{pmatrix} \in H$, then

$$\left[\begin{pmatrix} \frac{1}{\alpha} & 0 \\ 0 & \alpha \end{pmatrix}, \begin{pmatrix} 0 & -\frac{1}{mu} \\ \mu & x \end{pmatrix}\right] = \begin{pmatrix} \frac{1}{\alpha^2} & 0 \\ \mu x(\alpha^2) - 1) & \alpha^2 \end{pmatrix} \in H$$

Let $M \in H \setminus Z$ without loss of generality in rational form. There are two possible forms for M then:

$$M = \begin{pmatrix} \frac{1}{t} & 0 \\ 0 & t \end{pmatrix}$$

in which case $t \neq \pm 1$. As above using the commutator,

$$\begin{pmatrix} 1 & 0 \\ 1-t^2 & 1 \end{pmatrix} \in H$$

Since $t^2 \neq 1$, this is a transvection. In the other possible rational form,

$$M = \begin{pmatrix} 0 & -1 \\ 1 & x \end{pmatrix}$$

in which case we have

$$\begin{pmatrix} \frac{1}{\alpha^2} & 0 \\ x(\alpha^2 - 1) & \alpha^2 \end{pmatrix} \in H$$

and using the other commutator result we have

$$\begin{pmatrix} 1 & 0 \\ 1-\alpha^4 & 1 \end{pmatrix} \in H$$

so H contains a transvection if there exists $\alpha \in \mathbb{F}_q^\times$ which is not a 1st, 2nd, or 4th root of unity. We are done if $q > 5$. If $q = 4$, $\alpha^4 = \alpha$. for all $\alpha \in \mathbb{F}_q$. Choose $\alpha \notin \{0, 1\}$. If $q = 5$, suppose $x \neq 0$. Pick α with $\alpha^2 \neq 1$. Then

$$\begin{pmatrix} \frac{1}{\alpha^2} & 0 \\ x(\alpha^2 - 1) & \alpha^2 \end{pmatrix}$$

$\alpha^2 \neq 1$ and $\alpha^4 = 1$ implies $\alpha^2 = -1$ implies

$$\begin{pmatrix} -1 & 0 \\ -2x & -1 \end{pmatrix}$$

Its square is a transvection since $x \neq 0$. Now suppose $x = 0$. Then $M^2 = -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. So the Jordan form of M is $\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \in H$. Apply one of the commutators to get

$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \in H$$

We are done since this is a transvection. □

We discuss free groups.

Definition 8. Let $\{A_i\}_{i\in I}$ be a possibly infinite family of abelian groups. There are two possible constructions we can apply to the family. The **direct product**

$$\prod_{i\in I}(A_i) = \{(a_i)_{i\in I} : a_i \in A_i\}$$

with operation $(a_i) + (b_i) = (a_i + b_i)$. We can also define the **direct sum**

$$\bigoplus_{i\in I} A_i = \{(a_i)_{i\in I} : a_i \in A_i \text{ and } a_i = 0 \text{ for all but finitely many } i.\}$$

We have that $\bigoplus_{i\in I} A_i$ satisfies the following universal property. Suppose $\exists$ an abelian group B and homomorphisms from each A_i to B. Then there exists a unique homomorphism from $\bigoplus_{i\in I} A_i$ to B. It satisfies the diagram

$$A_i \hookrightarrow \bigoplus_{i\in I} A_i \xrightarrow{\varphi} B$$

Where the composition is f_i. Indeed, define

$$\varphi\left((a_i)_{i\in I}\right) = \sum_{i\in I} f_i(a_i)$$

Definition 9. A **free abelian group** is a free $\mathbb{Z}$-module. It's a direct sum of copies of $\mathbb{Z}$, which can be written

$$\bigoplus_{i\in I} \mathbb{Z}_i$$

We now define free groups:

Definition 10. Let X be a set. To each $x \in X$ associate a new symbol x^{-1}. Let $X' = X \cup \{x^{-1} : x \in X\}$. By a **word** we mean a finite string of elements of X'. Define two words $w_1 \sim w_2$ to be **equivalent** if they have the same reduced form. Such a form is obtained by cancelling adjacent x and x^{-1}. As an example,

$$abb^{-1}a^{-1}ab \sim abb^{-1}a^{-1}ab$$

so that

$$abb^{-1}b \sim aa^{-1}ab$$

Define the operation $*$ on the set of equivalence classes to get a group. $*$ is defined by concatenation. We have

$$free * group = freegroup$$

$$(free)^{-1} = e^{-1}e^{-1}r^{-1}f^{-1}$$

This is the free group on X, which we shall denote by FX.

It has a universal property. If $f : X \to G$ is a map where G is a group, then f extends uniquely to a homomorphism $\varphi : FX \to G$ such that

$$X \hookrightarrow FX \xrightarrow{\varphi} G$$

where the composition is f. $\varphi(group) = f(g)f(r)f(o)f(u)f(p)$. Generators and relations: We saw $S_3 = \langle(1\ 2\ 3), (1\ 2)\rangle$. $X = \{a, b\}$, $f(a) = (1\ 2\ 3)$, $f(b) = (1\ 2)$. This gives $FX \twoheadrightarrow S_3$. And so

$$S_3 = \frac{FX}{K}$$

where $K = \ker \varphi$. The generators for K are called the **relations.**

More generally, if R is a subset of FX, then $\langle X|R\rangle = FX/$smaller normal subgroup containing R. We can write

$$\frac{\mathbb{Z}}{n} \cong \langle x|x^n\rangle$$

We can also write

$$D_n \cong \langle x, y|x^n, y^2, yxy^{-1}x\rangle$$

13 February 24

Last time, we discussed definitions of groups using generators as relations. Such as:

1. $\frac{\mathbb{Z}}{p} = \langle x|x^p\rangle$.
2. $\mathbb{Z} \times \mathbb{Z} = \langle x, y|[x, y]\rangle$.
3. Suppose we write $G = \langle x, y|x^4, y^3, xy = y^2x^2\rangle$. The last relation allows us to pass x through y, and so every element can be written $x^n y^m$. There are thus at most 12 elements of G. For instance,

$$y^2x^3y = y^2x^2 \cdot xy = xyxy = xyy^2x^2 = x^3$$

$$x^3y = yx^3$$

   and so x^3 is central. But $x^4 = 1 \in Z$, so $x \in Z$, and so G is abelian. Once we know this, we can write $xy = x^2y^2$, $xy = 1$, and so $|G| = 1$.

4. $D_n = \langle a, b|a^n, b^2, baba\rangle$? (The dihedral group sits in S_n)

   Proof. One can define $\pi : \langle a, b\rangle \to D_n < S_n$ where

$$a \mapsto (1\ 2\ 3\ \ldots\ n)$$

$$b \mapsto \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & n & n-1 & \ldots & n \end{pmatrix}$$

   We know that $a^n, b^2, baba \in \ker \pi$. This means that the map factors through to get

$$\langle a, b|a^n, b^2, baba\rangle \twoheadrightarrow D_n$$

   The relations tell us that the group has order $\leq 2n$. $|D_n| = 2n$, so this means we have a bijection. □

5. Murder weapon: $G = \langle a, b, c|a^2 = b^3 = c^5 = (abc)^{-2}\rangle$. Maple tells us the group has order 7320. c has order 610.

Exercise 4

Call $G = \langle a, b, c, \ldots, z|\text{anagrams}\rangle$. In G, $act = cat$, so $ac = ca$. $art = rat$, $care = race$. An anagram is a word that can be obtained from another by rearranging the letters. Hence G is commutative since any two letters commute.

The exercise: Prove all but $j, q, x, z \in Z(G)$. Beware: this problem can take a while and possibly depends on the dictionary you use.

A free group on a set X has free **rank** $|X|$. If G is a free group, define $\text{rank}(G) = \text{rank}\left(\frac{G}{[G,G]}\right)$ as a $\mathbb{Z}$-module. For people who are familiar with algebraic topology (if not then feel free to tune out): look at this bouquet of loops. It has fundamental group $\langle a, b, c, d\rangle$. Similarly, has fundamental group $\langle a, b\rangle$. As we can see, free

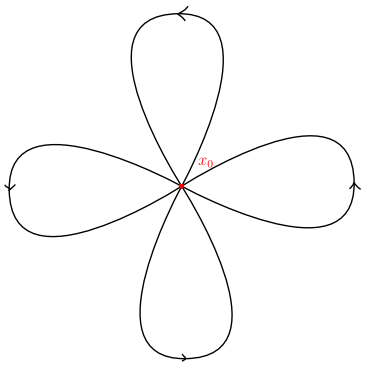


Figure 2: Wedge sum of four circles. Its fundamental group is the free product of four copies of $\mathbb{Z}$.

groups appear in lots of places.

Returning back to the content of the lecture (tune back in), if we look at $\langle a, b\rangle \to \frac{\mathbb{Z}}{2}$, $a \mapsto 1$, $b \mapsto 1$. Words of even length are the kernel. Such words are precisely the group $\langle a^2, ab, b^2\rangle$. Even $ba = b^2(ab)^{-1}, a^2$. We can't identify any relations for this group. This motivates the following theorem:

Theorem 17. (Nielson-Schreier) Every subgroup of a free group is free. Moreover: If F is free of rank n, and $H < F$ has $(F : H) = k$, then H is free of rank $nk - k + 1$.

In our previous example, for $H = \langle a^2, ab, b^2\rangle$, $F = \langle a, b\rangle$. Then $(F : H) = 2$. Indeed, $3 = 2 \cdot 2 - 2 + 1$. For that matter, take $F = \langle x_1, \ldots, x_n\rangle \twoheadrightarrow \frac{\mathbb{Z}}{k}$. Each x_i maps to $1 \mod k$. So we have the kernel is the group $H = \langle$words of length multiple of $k\rangle$ is free of rank $nk - k + 1$.

We provide some quick introduction to covering spaces. A **covering space of** a topological space X is a topological space C with $p : C \to X$ such that for every $x \in X$, x has a neighborhood U with

$$\pi^{-1}(U)$$

is a union of disjoint open sets such that p restricts to each as a homeomorphism to U. Fix $x_0 \in X$ and consider $\pi_1(X, x_0)$. The result is each subgroup of $\pi_1(X, x_0)$ corresponds to a covering space of X, say C. Fix $\tilde{x_0}$ with $\tilde{x_0} \mapsto x_0$. Then $\pi_1(C, \tilde{x_0}) \to \pi_1(X, x_0)$ is injective and the image is loops at x_0 whose lifts are loops at $\tilde{x_0}$.

View 5 of the included sheet. Its subgroup is $\langle a^3, b^3, ab, ba\rangle$. Suppose F is a free group of rank n, F is the fundamental group of the bouquet of n circles. Suppose $H < F$ has index k. H corresponds to a covering space with k vertices, nk loops.

A spanning tree has $k-1$ edges. We can collapse a spanning tree to a point to get 1 vertex and $nk-(k-1) = nk - k + 1$ loops. Collapsing the spanning tree in the fundamental group gives that many loops: We now move to a completely separate topic: **Fields:** A commutative ring in which each nonzero element is a unit is called a **field**. The only ideals in a field are (0) and the field itself. This means that a homomorphism of a fields, as a homomorphism of rings $\varphi : K \to L$, is an injection. Let R be a commutative ring, so it has

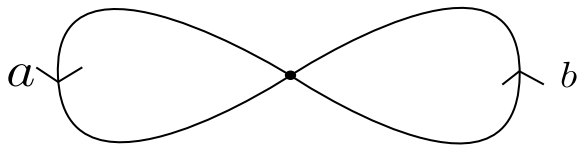


Figure 3: Wedge sum of two circles.

$1 \in R$ multiplicative identity. Then we can construct $\mathbb{Z} \to R$. Its kernel is some (n) for some $n \geq 0$. We say R has characteristic n. The characteristic of a field is either 0 or a prime p. By the former case we mean $\mathbb{Z} \hookrightarrow K$ for field K, which forces there to be a copy $\mathbb{Q}$ in K. In the characteristic p case, We have $\frac{\mathbb{Z}}{p} \hookrightarrow K$ Hence any field is either a $\mathbb{Q}$-vector space or a $\frac{\mathbb{Z}}{p}$ vector space. Let $K \subset L$ be fields. Then L is a K-vector space, and we can discuss its rank as such. Call $[L : K]$ as the rank of L as a K vector space. An element $\alpha \in L$ is algebraic over K there exists polynomial $p \in K[x]$ with $p(\alpha) = 0$. Otherwise α is transcendental. We call $\alpha \in \mathbb{C}$ is transcendental if it is over $\mathbb{Q}$. The set of algebraic elements are countable, so most numbers are transcendental. Looking at the history, in 1844, Liouville constructed transcendental numbers (we will look at this in a future class). In 1873, e Hermite In 1882, π Lindemann. In 1891, Almost all numbers are transcendental cantor. In 1934, Gelfond-Schneider theorem: if a, b, are algebraic, $a \neq 0, 1$, and $b \notin \mathbb{Q}$, then a^b is transcendental. For instance, $2^{\sqrt{2}}$ is transcendental.

14 March 3

Notes on exam: The overall grade will be calculated for the course, and the final grade will be released. Whichever is higher will be one's actual grade in the course.

1. The normal subgroups of S_6 are $\{e\}, A_6, S_6$. We have

$$\ker\left(S_6 \to S_5 \times S_5 \xrightarrow{\pi_i} S_5\right) \supset A_6$$

2. All elements have order 1 or p (fixed p). A group has nontrivial center. Automorphisms preserve the center, and the automorphism group acts transitively. A theorem gives us that the group is

$$\frac{\mathbb{Z}}{p} \times \ldots \times \frac{\mathbb{Z}}{p}$$

the automorphism group is $GL_n(\frac{\mathbb{Z}}{p})$.

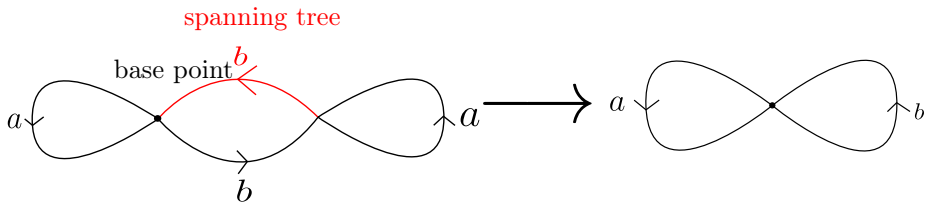


Figure 4: Collapse a spanning tree in a covering space

3. One remembers $\mathrm{Aut}(\frac{\mathbb{Z}}{11}) \cong \frac{\mathbb{Z}}{10}$.

$$\frac{\mathbb{Z}}{11} \rtimes_\alpha \frac{\mathbb{Z}}{4}$$

   $\alpha : \frac{\mathbb{Z}}{4} \to \frac{\mathbb{Z}}{10}$. We can send 1 to 5.

4. One might have missed $p = 2$.

Last time we introduced some field theory. We continue: Let K, L be fields. If $\varphi : K \to L$ be a homomorphism, then $\varphi(1) = 1$ by definition, so φ is injective because K only has two ideals. If $K \subset L$ are fields, then L is a K vector space. We defined an extension degree by

$$[L : K] = \mathrm{rank}_K L$$

rank of L as a K-vector space. Suppose $k \subset K \subset L$ are fields. We have

$$[L : k] = [L : K][K : k]$$

if $\{x_i\}$ is a basis for L over K and $\{y_j\}$ is one for K over k, then $\{x_i y_j\}$ is a basis for L over k. We have

$$L = \sum Kx_i = \sum \left(\sum ky_j \right) x_i$$

$$K = \sum ky_j$$

As in last time, $K \subset L$ fields and $\alpha \in L$ is **algebraic** over K if $f(\alpha) = 0$ for some nonzero $f(x) \in K[x]$. Otherwise, α is called **transcendental.**

Theorem 18. (Liouville, 1844) If α is defined $\sum_{n=0}^{\infty} 2^{-n!}$, α is transcendental over $\mathbb{Q}$.

Proof. Suppose α is algebraic. Let $f(x) \in \mathbb{Q}[x]$ be a polynomial with

$$f(\alpha) = 0$$

and $f \neq 0$. Without loss of generality, f is monic and irreducible over $\mathbb{Q}[x]$.

Say $f(x) = x^d + a_1 x^{d-1} + \ldots + a_d$, $a_i \in \mathbb{Q}$. We can also clear denominators, so that there exists $D > 0$ with $D \cdot f(x) \in \mathbb{Z}[x]$. Let

$$S_N = \sum_{n=0}^{N} \frac{1}{2^{n!}}.$$

Claim: $f(S_N) \neq 0$. Suppose $d = 1$. Then $f(x) = x - \alpha$, so $f(S_N) \neq 0$. If $d > 1$, then the irreducibility of f implies that f has no rational roots.

So we can plug in S_N into $D \cdot f(x)$. We find further $D' = 2^{(N!)d} \cdot d$ such that

$$2^{(N!)d} \cdot D \cdot f(S_N) \in \mathbb{Z} \setminus \{0\}$$

We note $|2^{(N!)d} D f(S_N)| \geq 1$. We apply the fundamental theorem of algebra so that f has complex roots $\alpha_1, \ldots, \alpha_d$. So

$$f(x) = \prod_{i=1}^{d} (x - \alpha_i)$$

say $\alpha = \alpha_1$. So

$$|f(S_N)| = |S_N - \alpha| \cdot |\prod_{i=2}^{d} (S_N - \alpha_i)|$$

The former term $\to 0$ as $N \to \infty$, while the latter term is bounded. In particular, $|f(S_N)| \leq \frac{C}{2^{(N+1)!}}$. Hence eventually we get a contradiction for large N. □

Exercise 5

Open: Is e is transcendental over $\mathbb{Q}(\pi)$?

There's a notion of transcendence degree. Given L a field extension over K, $\sup\{n : \exists \alpha_1, \ldots, \alpha_n \in L\}$ where $\alpha_1, \ldots, \alpha_n$ are algebraically independent over K. In other words,

$$K \subsetneq K(\alpha_1) \subsetneq \ldots \subsetneq K(\alpha_1, \ldots, \alpha_n)$$

To rephrase our open question above, is $trdeg_{\mathbb{Q}}(\mathbb{Q}(e, \pi)) = 2$?? Schanuel's conjecture: If $z_1, \ldots, z_n \in \mathbb{C}$ are linearly independent over $\mathbb{Q}$, then $trdeg_{\mathbb{Q}}\mathbb{Q}(z_1, \ldots, z_n, e^{z_1}, \ldots, e^{z_n})$ is $\geq n$. If this conjecture is to be believed, then $z_1 = 1$, $z_2 = \pi i$ gives

$$trdeg_{\mathbb{Q}}\mathbb{Q}(\pi i, e) \geq 2$$

Suppose $K \subset L$ are fields and $\alpha \in L$ is transcendental over K.

$$K[x] \to L$$

by evaluation at α. The map is injective if and only if α is transcendental. We have

$$K(x) = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], g \neq 0 \right\}$$

We get an induced map by injectivity:

$$K(x) \to L$$

which is still an injection. In fact, if $L = K(\alpha)$, we get an isomorphism. We say $K(\alpha)$ is the smallest field containing K and α. If K countable, then $K(x)$ is countable. Hence you can't adjoin finitely many elements to $\mathbb{Q}$ to get $\mathbb{R}$. If $A \subset B$ are rings and $\{b_\lambda\}_{\lambda \in \Lambda} \subset B$ we use $A[b_\lambda : \lambda \in \Lambda]$ to denote the smallest ring A and b_λ. If $A \subset B$ are fields, $\{b_\lambda\}_{\lambda \in \Lambda} \subset B$, then $A\,(b_\lambda | \lambda \in \Lambda)$ denotes the smallest field containing A and b_λ. So we could have

$$\mathbb{Q}[\sqrt{2}]$$

and

$$\mathbb{Q}(\sqrt{2})$$

they are the same because $\mathbb{Q}[\sqrt{2}]$ is already a field. The point is that

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{(a+b\sqrt{2})(c-d\sqrt{2})}{c^2-2d^2}$$

Noting that $\mathbb{Q}[\sqrt{2}] = \mathbb{Q} + \mathbb{Q}\cdot\sqrt{2}$. More generally

Proposition 12. Suppose $K \subset L$ are fields and $\alpha \in L$ is algebraic over K. Then $K[\alpha] = K(\alpha)$.

Define $K[x] \to L$ by evaluation at α. It has a kernel $(f(x))$ since $K[x]$ is a principal ideal domain. Because α is algebraic, $f \neq 0$. We have an induced injection

$$\frac{K[x]}{(f(x))} \hookrightarrow L$$

So the former is a domain, and $f(x)$ is irreducible. Since $K[x]$ is a PID, $(f(x))$ which is prime is also maximal. Hence $\frac{K[x]}{(f(x))}$ is a field inside L. Its image is essentially polynomials with α plugged in, so $K[\alpha]$. Since it is also a field, it contains $K(\alpha)$, hence is equal.

Proposition 13. Let $K \subset L$ be fields. Define

$$E = \{\alpha \in L | \alpha \text{ is algebraic over } K\}$$

Then E is a field.

We do this after the break.

15 March 15

Let K be a field. Let

$$f(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_0$$

be in $K[x]$ where $a_d \neq 0$. Then define $\mathbf{deg}(f(x)) = d$ Then

$$\frac{K[x]}{(f(x))}$$

is a ring, it is a K-vector space of rank d since $1, x, x^2, \ldots, x^{d-1}$ is a basis. In particular, In particular, if $f(x)$ is irreducible, then $L = \frac{K[x]}{(f(x))}$ is a field and

$$[L : K] = d$$

Suppose $K \subset L$ are fields. Then fix $a \in L$. Then $[K(a) : K] < \infty$ if and only if a is algebraic. In this case,

$$K[x] \to L$$

by $f(x) = f(a)$ has kernel $(p(x))$ for some monic irreducible $p(a) = 0$ which is called the **minimal polynomial** for a. For example,

$$[\mathbb{Q}[i] : \mathbb{Q}] = 2$$

since i has minimal polynomial $x^2 + 1$. We also have

$$[\mathbb{Q}(\sqrt[3]{2} : \mathbb{Q}] = 3$$

since $.\sqrt[3]{2}$ has minimal polynomial $x^3 - 2$. Eisenstein's criterion shows $x^3 - 2$ is irreducible. The theorem?

Theorem 19. Let $f(x) \in \mathbb{Z}[x]$ be of the form

$$f(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_1 x + a_0$$

for $a_i \in \mathbb{Z}$. If there exists a prime p with p divides a_i $\forall i$, but p^2 doesn't divide a_0, then f is irreducible.

Example.

$$f(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1 \in \mathbb{Z}[x]$$

p prime. The trick is to consider $f(x+1) = \frac{(x+1)^p - 1}{x} = \frac{x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \ldots + 1 - 1}{x}$

$$= x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}xp^{p-3} + \ldots + p$$

is irreducible by Eisenstein.

Hence

$$[\mathbb{Q}(e^{2\pi i/p} : \mathbb{Q}] = p - 1$$

since it has minimal polynomial. What we ended on last time was algebraicness of some elements. If we add algebraic elements, is the result algebraic?

Theorem 20. Let $K \subset L$ be fields. Set $E = \{a \in L : a \text{ is algebraic over } K\}$. We claim E is a field, and if $a \in L$ is algebraic over E, then it is in E. We say E is algebraically closed in L.

Proof. Let $a, b \in E$. Want $a \pm b, ab, \frac{a}{b} \in E$ $(b \neq 0)$. We say

$$[K(a) : K] < \infty$$

$[K(b) : K] < \infty$. We can look at tower of fields $K(a, b)$ over $K(a)$ over K. We know

$$[K(a, b) : K] = [K(a, b) : K(a)][K(a) : K]$$

We know

$$[K(a, b) : K(a)] \leq [K(b) : K]$$

by working with the minimal polynomial for a in K. We have

$$[K(a, b) : K] \leq [K(b) : K][K(a) : K]$$

Since then $a \pm b, ab, \frac{a}{b} \in K(a, b)$, which is algebraic over K. For the second assertion, suppose $a \in E$ is algebraic over E. Then it has minimal polynomial

$$x^d + c_{d-1}x^{d-1} + \ldots + c_1 x + c_0$$

over E. We write

$$[K(a, \overline{c}) : K] = [K(a, \overline{c}) : K(\overline{c})][K(\overline{c}) : K]$$
$$< \infty$$

So $[K(a) : K] < \infty$, hence $a \in E$. □

Suppose $f(x) \neq 0$ in $K[x]$ where K is a field. To find a root for $f(x)$, we may assume it is irreducible. Without loss of generality, $f(x)$ is irreducible. We slap name to roots, but they all seem to be algebraically indistinguishable. We look at the field extension

$$K[x]/(f(x))$$

over K. The image of x in the extension is precisely the root of $f(x)$. View $\frac{K[x]}{(f(x))}$ as an extension field of K. An example:

$$\mathbb{Q} \hookrightarrow \mathbb{Q}[x] \twoheadrightarrow \frac{\mathbb{Q}[x]}{(x^2-2)}$$

Set $\overline{x} = x + (x^2-2)\mathbb{Q}[x]$. We have

$$\begin{aligned}\overline{x}^2 - 2 &= (x^2-2) + (x^2-2)\mathbb{Q}[x] \\ &= (x^2-2)\mathbb{Q}[x]\end{aligned}$$

So far, each each nonzero degree $f(x) \in K[x]$ has a root in some finite extension field L of K. In other words, $[L:K] < \infty$. If $a \in L$ is a root, then $f(x) = (x-a)g(x)$ for some $g(x) \in L[x]$. This way, repeating the process, if $f(x)$ is a monic polynomial of degree d in $K[x]$, then there exists an extension field L with $[L:K] < \infty$ such that $f(x) = \prod_{i=1}^{d}(x-a_i)$ for $a_i \in L$.

The splitting field of $f(x)$ over K is the field $K(a_1, \ldots, a_d) \subset L$ for some choice L over which f factors completely, in which case we can choose its roots $a_1, \ldots, a_d$. We later need to prove this is independent of choice of L.

Example.

$$x^2 - 2 \in \mathbb{Q}[x]$$

has splitting field $\mathbb{Q}(\sqrt{2})$, in which it has roots $\sqrt{2}, -\sqrt{2}$. Likewise with the cube root of 2, except we also need to adjoin the root of unity:

$$\mathbb{Q}(\sqrt[3]{2}, \omega^3\sqrt{2}, \omega^{23}\sqrt{2})$$

where $\omega = e^{2\pi i/3}$

If p is prime, $x^p - 1 \in \mathbb{Q}[x]$ has splitting field $\mathbb{Q}(e^{2\pi i/p})$. Suppose the characteristic of K is positive and $x^p - x - c \in K[x]$.Suppose a is a root of the polynomial. $a^p - a - c = 0$. We have

$$(a+1)^p - (a+1) - c = a^p + 1 - a - 1 - c = 0$$

Hence $a, a+1, \ldots, a+p-1$ are roots. The splitting field is $K(a)$.

16 March 17

We say $f(x) \in k[x]$ has **multiple roots** if in its splitting field

$$f(x) = (x-a)^2 g(x)$$

Suppose K is a field, $f(x) \in k[x]$ and $a \in K$ is a root of $f(x)$.

$$f(x) = q(x)(x-a) + r(x)$$

for some q, r using the division algorithm where the degree of $r(x)$ is less than 1, meaning r is constant. Plugging in a, we can evaluate at a to get

$$f(a) = q(a)(a-a) + r = 0 = r$$

implying $r = 0$. This shows that $f(x)$ has at most $\deg(f(x))$ roots in a field. What about division rings? (Multiplication need not be commutative)

Example. $\mathbb{H} = \mathbb{Q}$-vector space with basis $1, i, j, k$ in the Quaternion group. We multiply vectors using the multiplication table $i^2 = j^2 = k^2 = -1$, $ij = k = -ji$, $jk = i = -kj$, $ki = j = -ik$.

$$\begin{aligned}&(\alpha \cdot i + \beta \cdot j + \gamma \cdot k)(\alpha \cdot i + \beta \cdot j + \gamma \cdot k) \\ &= -\alpha^2 - \beta^2 - \gamma^2\end{aligned}$$

So all elements (α, β, γ) on the unit sphere (over $\mathbb{Q}$ or $\mathbb{R}$) give solutions of $x^2 + 1$.

Let K be a field and $f(x) \in K[x]$. Write $f(x) = \sum a_i x^i$, and define

$$f'(x) = \sum i a_i x^{i-1}$$

Theorem 21. $f(x)$ has multiple roots if and only if $\gcd(f(x), f'(x)) \neq 1$.

Recall the gcd of two polynomials $h(x)$ and $k(x)$ is the **monic** polynomial generating the ideal $(h(x), k(x))$.

Remark. $h(x)$ and $k(x) \in K[x]$ are **relatively prime** if and only if they are relative prime in $L[x]$ for any field $L \supset K$.

Proof. (of the remark): If h and k share a common factor over $K[x]$, the fact that they aren't relatively prime in $L[x]$ follows. If they are relatively prime in $K[x]$, we can write

$$1 = p(x)h(x) + q(x)k(x)$$

for polynomials $p, q \in K[x]$. This is also true in $L[x]$. □

Proof. (of the theorem): By the remark above, we may work in the splitting field of $f(x)$, L. Then

$$f(x) = \prod_1^n (x - \alpha_i)$$

for $\alpha_i \in L$. Then

$$f'(x) = \sum_{i=1}^n (x - \alpha_1) \cdots (x - \hat{\alpha_i}) \cdots (x - \alpha_n)$$

If $\alpha_i = \alpha_j$ for some $i \neq j$, then $f'(\alpha_i) = 0$. Hence α_i is a common root of f, f'. Conversely, if α_i are all distinct, then $f'(\alpha_i) \neq 0$. In this case, the gcd is 1. □

Definition 11. An irreducible polynomial is **separable** if it has distinct roots(it does not have a multiple root).

Proposition 14. If $\mathrm{char}(K) = 0$, then each irreducible polynomial is separable.

Proof. Suppose $f(x)$ is irreducible, so it has degree $d = \deg(f) \geq 1$ (the polynomial must generate a prime ideal, not the whole ring, so f cannot be constant). Then

$$\deg(f'(x)) = d - 1$$

by the condition that the characteristic is zero. Hence $\gcd(f(x), f'(x)) = 1$. Hence f has distinct roots. □

Example. Note $K = \mathbb{F}_p(t)$. Then $f(x) = x^p - t$ is irreducible but not separable.

$$f'(x) = px^{p-1}$$

This means

$$\gcd(f(x), f'(x)) = f(x)$$

Suppose $f(x) = \sum a_i x^i \in K[x]$ is an irreducible polynomial that is **not** separable. Characteristic K greater than 0, and $f'(x) = 0 = \sum i a_i x^{i-1}$. $a_i \neq 0$ implies $i a_i = 0$, which in turn implies $i = 0 \bmod p$. In other words, f is really a polynomial in x^p.

Definition 12. A field K of characteristic p is **perfect** if $K \xrightarrow{F} K$ defined by $a \mapsto a^p$ is bijective.

Example. $\frac{\mathbb{Z}}{p}$ is perfect by little Fermat. Given a finite field, we know $a \mapsto a^p$ is a homomorphism, which hence must be injective. An injective map of finite sets must be bijective.

- Finite fields are perfect
- Algebraically closed fields are perfect.

$\mathbb{F}_p(t)$ is not perfect, as we saw before.

Proposition 15. Over a perfect field, each irreducible polynomial is separable

Proof. Suppose $f(x)$ is irreducible, but **not** separable. Then $f'(x) = 0$. f is really a polynomial in x^p. So

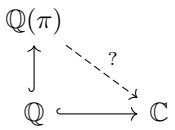
$$f(x) = \sum b_i x^{ip}$$

Since K is perfect, $b_i = a_i^p$ for some $a_i \in K$. We can write

$$f(x) = \sum (a_i x^i)^p = \left(\sum a_i x^i\right)^p$$

since $a \mapsto a^p$ is a homomorphism. We get a contradiction to the irreducibility of f. □

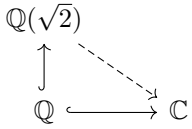
Example. Consider $\mathbb{Q} \hookrightarrow \mathbb{C}$. $\mathbb{Q} \subset \mathbb{Q}(\pi)$. How many homomorphisms do we get $\mathbb{Q}(\pi) \to \mathbb{C}$?



The homomorphisms must be of the form where π gets sent to any transcendental. The same is true if we replace $\mathbb{Q}(\pi)$ with $\mathbb{Q}(x)$. $\mathbb{Q}[x] \to \mathbb{C}$ is defined $f(x) \mapsto f(\pi)$ has zero kernel since π is transcendental. Since $\mathbb{C}$ is a field, we get an induced injection

$$\mathbb{Q}(x) \hookrightarrow \mathbb{C}$$

Suppose instead we worked with an algebraic element:



Suppose $\sqrt{2}$ maps to $\alpha \in \mathbb{C}$, then $\left(\left(\sqrt{2}\right)^2 \mapsto \alpha^2 = 2\right)$. Suppose we have fields $K \hookrightarrow L$, and α is algebraic over K. The number of possible $\varphi : K(\alpha) \to L$ depends on the minimal polynomial in K (it is the number of distinct roots precisely). α must end up getting sent to another root of the minimal polynomial.

Conversely, suppose $\beta \in L$ is a root of $f(x)$.

$$K[x] \xrightarrow{\text{eval } \beta} L$$

The kernel of this map is $(f(x))$. It maps onto $K(\beta)$. We also have

$$K[x]/(f(x)) \to K(\alpha)$$

is an isomomorphism, and so is

$$K[x]/(f(x)) \to K(\beta)$$

Theorem 22. Let $K \hookrightarrow \Omega$ be fields. Suppose $f(x) \in K[x]$ splits in Ω. Let $\alpha_1, \ldots, \alpha_m$ be some of the roots of $f(x)$.

$$\begin{array}{ccc} K(\alpha_1, \ldots, \alpha_m) & & \\ \uparrow & \overset{\varphi}{\searrow} & \\ K & \hookrightarrow & \Omega \end{array}$$

Then the number of homomorphisms φ such that the diagram commutes is $\leq [K(\alpha_1, \ldots, \alpha_m) : K]$. Moreover, equality holds if $f(x)$ has distinct roots.

Proof. Consider $\varphi_1 : K(\alpha_1) \to \Omega$. Let $f_1(x)$ be the minimal polynomial of α_1 over K. It is something that divides f. The number of φ_1 is the number of roots of $f_1(x)$ in Ω which is $\leq \deg(f_1(x)) = [K(\alpha) : K]$. Equality holds if f has distinct roots. Then we can count $\varphi_2 : K(\alpha_1, \alpha_2) \to \Omega$. Repeat. □

Definition 13. Let $K \subset L$ be fields.

$$\mathrm{Aut}_K L = \{\varphi : L \to L \text{ automorphisms} \ni \varphi|_K = \mathrm{id}_K\}$$

Example. $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{id, \text{complex conjugation}\}$.

In another example, let $[L : K] < \infty$. Then $\mathrm{Aut}_K L$ is a finite group. THen

$$L = K(\alpha_1, \ldots, \alpha_m)$$

Let Ω be the splitting field of $f(x)$.

$$\begin{array}{ccccc} K(\alpha_1, \ldots, \alpha_m) & & & & \\ \uparrow & & & & \\ K & \hookrightarrow & L & \hookrightarrow & \Omega \end{array}$$

But recall that we bounded the number of automorphisms $K(\alpha_1, \ldots, \alpha_m) \to \Omega$.

17 March 24

Theorem 23. Let $K \subset L$ be a finite extension of fields with $[L : K] < \infty$. The following are equivalent:

1. L is the splitting field of some polynomial in $K[x]$ with distinct roots.
2. $K = L^G$ for $G = \mathrm{Aut}_K(L)$
3. $K = L^G$ for some $G < \mathrm{Aut}(L)$.
4. $K \subset L$ is normal and seperable.
5. $|\mathrm{Aut}_K L| = [L : K]$.

If these equivalent conditions hold we say L/K $K \subset L$ is Galois with Galois group

$$\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$$

Proof. We have seen 1 implies 5. Suppose 5 holds. Let $G = \mathrm{Aut}_K(L)$.

$$\begin{array}{c} L \\ | \\ L^G \\ | \\ K \end{array}$$

where the extension degree of L over L^G is $|G|$. But then that implies the degree of L^G over K is 1, so $L^G = K$. Hence 5 implies 2. □

Suppose L/K is Galois.

- If $K \subset F \subset L$ are fields, then K is the splitting field of a polynomial over K, hence over F. Hence L/F is Galois.
- Does transitivity hold? If L/F and F/K, then is L/K Galois? Not necessarily: note $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Each subextension is normal but not the entire thing, because $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal. $\sqrt[4]{2}$ has minimal polynomial $x^4 - 2$ which does not split in $\mathbb{Q}(\sqrt[4]{2})$.
- Suppose L/K is a finite seperable extension. Then there exists M/L, L/K such that M/K is Galois.

  Proof. Say $L = K(\alpha_1, \ldots, \alpha_m)$. Let M be the smallest field in which the minimal polynomials of $\alpha_1, \ldots, \alpha_m$ split. □

Theorem 24. Let L/K be a Galois extension. Set $G = \mathrm{Gal}(L/K)$

1. There exists a bijection between subgroups of G and intermediate fields. $H < G$, then $H \mapsto L^H$. Conversely, given $K \subset F \subset L$, then $F \mapsto \mathrm{Gal}(L/F)$.
2. $H_2 \subset H_1$ if and only if $L^{H_1} \subset L^{H_2}$. In this case, $[H_1 : H_2] = [L^{H_2} : L^{H_1}]$.
3. For $\sigma \in G$, $H < G$, then $L^{\sigma H \sigma^{-1}} = \sigma(L^H)$. And
$$\mathrm{Gal}(L/\sigma(L^H)) = \sigma H \sigma^{-1}$$
4. $H \lhd G$ if and only if L^H/K is normal if and only if L^H/K is Galois. In this case, $\mathrm{Gal}(L^H/K) = G/H$.

Proof. 1. $H \mapsto L^H \mapsto \mathrm{Gal}(L/L^H)$. We have

$$\left|\mathrm{Gal}\left(L/L^H\right)\right| = [L : L^H] = |H|.$$

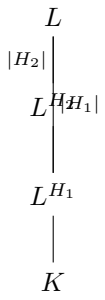
First, note $H < \mathrm{Aut}_{L^H}(L)$ so one inequality is obtained like so:

$$\mathrm{Gal}(L/L^H) = H$$

Similarly for $F \mapsto \mathrm{Gal}(L/F) \mapsto L^{\mathrm{Gal}(L/F)}$.

2. Now that the bijection is established, this can be obtained by calculation: $L/L^{H_2}/L^{H_1}$. Stuff that is fixed by H_1 is fixed by anything in H_1. To prove the equality, note this link to see the figure, which is

broken in this pdf.



So L^{H_2} over L^{H_1} has degree $[H_1 : H_2]$.

3. $\alpha \in L^{\sigma H \sigma^{-1}}$ iff $\sigma h \sigma^{-1}(\alpha) = \alpha$ for all $h \in H$ if and only if $h\sigma^{-1}(\alpha) = \sigma^{-1}(\alpha)$ iff $\sigma^{-1}(\alpha) \in L^H$ iff $\alpha \in \sigma(L^H)$. This yields the desired equation $L^{\sigma H \sigma^{-1}} = \sigma(L^H)$. Also
$$\mathrm{Gal}\left(L/\sigma(L^H)\right) = \mathrm{Gal}\left(L/L^{\sigma H \sigma^{-1}}\right) = \sigma H \sigma^{-1}$$
by a previous part (1).

4. Suppose $H \lhd G$. Then $\sigma H \sigma^{-1} = H$ for all $\sigma \in G$, so 3 tells us $\sigma(L^H) = L^H \forall \sigma \in G$. We can define a map $G \to \mathrm{Aut}_K(L^H)$ via $\sigma \mapsto \sigma|_{L^H}$ (restriction). Its kernel is σ such that $\sigma|_{L^H} = id_{L^H}$. More precisely, $\mathrm{Gal}\left(L/L^H\right) = H$. So $G/H \hookrightarrow \mathrm{Aut}_K(L^H)$. So
$$|G : H| \leq |\mathrm{Aut}_K(L^H)| \leq [L^H : K] = \frac{[L : K]}{[L : L^H]} = [G : H]$$
So $G : H \cong \mathrm{Aut}_K(L^H)$. Hence L^H/K is Galois, with Galois group G/H. Conversely, suppose $H < G$ and L^H/K is Galois. Let $L^H = K(\alpha_1, \ldots, \alpha_m)$. Let $\sigma \in G$. $\sigma(\alpha_i) \in L^H$ for all i. So $\sigma(L^H) = L^H$. Recall $L^{\sigma H \sigma^{-1}} = \sigma(L^H)$. So $L^{\sigma H \sigma^{-1}} = L^H$. In particular, $\sigma H \sigma^{-1} = H$.

□

Theorem 25. Let L/K be a finite extension of fields of characteristic 0. Then there exists $\gamma \in L$ with $L = K(\gamma)$ (γ is called a **primitive element** for L/K).

Example. Note $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. This is because
$$\frac{1}{\sqrt{2} + \sqrt{3}} = \frac{\sqrt{3} - \sqrt{2}}{3 - 2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$
$$\sqrt{3} - \sqrt{2} + \sqrt{2} + \sqrt{3} = 2\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$
So $\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Similarly $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Proof. It is enough to consider $L = K(\alpha, \beta)$. Let α, β have minimal polynomial $f(x)$ and $g(x)$ over K. Let the roots of $f(x)$ be $\alpha = \alpha_1, \ldots, \alpha_m$. And let the roots of $g(x)$ be $\beta = \beta_1, \ldots, \beta_n$. Consider $\alpha_i + x\beta_j = \alpha + x\beta$ $j \neq 1$. It is only a genuine nonconstant polynomial in x if $j \neq 1$. It has solution
$$x = \frac{\alpha_i - \alpha}{\beta - \beta_j}$$
As long as $j \neq 1$, this solution exists. Pick $c \in K$ that is not any of these finitely many elements. Pick $c \in K$ such that $\alpha_i + c\beta_j = \alpha + c\beta$ if and only if $(i, j) = (1, 1)$. Set $\gamma = \alpha + c\beta \in K(\alpha, \beta)$. The claim: $K(\gamma) = L$.Consider $g(x)$ and $f(\gamma - cx)$ in $K(\gamma)[x]$. β is a common root, since $g(\beta) = 0$ and $f(\gamma - c\beta) = f(\alpha) = 0$. They have no other root in common since the other roots of g are β_j, but $f(\gamma - c\beta_j)$ will never vanish if $j \neq 1$ by choice of c. What is the gcd of g, f? It is $x - \beta \in K(\gamma)[x]$. This implies $\beta \in K(\gamma)$. Also note $\alpha \in K(\gamma)$. □

Let's use this result to prove an important theorem:

Theorem 26. (Fundamental theorem of Algebra) Each polynomial in $\mathbb{C}[x]$ of positive degree has a root in $\mathbb{C}$.

Proof. We would like to show that any irreducible polynomial has degree 1. Suppose K is a field, $\mathbb{C} \subset K$, and $[K : \mathbb{C}] < \infty$. We want: $K = \mathbb{C}$. We may assume that K is Galois over $\mathbb{C}$ by enlarging K if necessary. We can also assume that K is Galois over the reals. Let $G = \mathrm{Gal}(K/\mathbb{R})$. Let H be a 2-Sylow in G.

$$\begin{array}{c} K \\ | \\ \mathbb{C} \\ |2 \\ \mathbb{R} \end{array}$$

This means K^H over $\mathbb{R}$ has odd degree. By the primitive element theorem, K^H is $\mathbb{R}(\gamma)$ for some $\gamma \in K$. The minimal polynomial for γ necessarily has odd degree. By theorems from analysis, an odd degree polynomial in $\mathbb{R}[x]$ has a real root (use the intermediate value theorem). Hence the degree of K^H over $\mathbb{R}$ is 1. So far, G is a 2-group. Let us check out K over $\mathbb{C}$. Let $\overline{G} = \mathrm{Gal}\,(K/\mathbb{C})$. This is a 2-group, hence it is solvable (p-groups are solvable). Hence we get a tower

$$\overline{G} \rhd G_1 \rhd G_2 \rhd \ldots \rhd \{e\}$$

where $G_i/G_{i+1} = \frac{\mathbb{Z}}{2}$. So far: if there exists $K/\mathbb{C}$ with $[K : \mathbb{C}] > 1$, then there exists $K^{G_1}/\mathbb{C}$ with $[K^{G_1} : \mathbb{C}] = 2$. But every degree 2 pollynomial in $\mathbb{C}[x]$ splits in $\mathbb{C}$: $x^2 + bx + c$ has root

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

(quadratic formula). □

18 March 29

Suppose L/K is Galois. Let $G = \mathrm{Gal}\,(L/K)$. There is a bijection between subgroups $H < G$ and intermediate fields $L/L^H/K$. L^H/K is Galois if and only if L^H/K is normal if and only if $H \lhd G$. Note L over L^H is always Galois with group H. In this case, $\mathrm{Gal}(L^H/K) \cong G/H$.

Suppose $f(x) \in K[x]$ has distinct roots. Then by the Galois group of $f(x)$ we mean $\mathrm{Gal}(f) = \mathrm{Gal}(L/K)$ where L is the splitting field of $f(x)$. Some examples:

Example. $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. The splitting field is $L = \mathbb{Q}(\alpha, \omega)$, $\alpha = 2^{\frac{1}{3}}$, $\omega = e^{2\pi i/3}$. The extension degree is

$$[L : \mathbb{Q}] = 6$$

Suppose we were in a hurry. Can we say what the Galois group is from the extensions $\mathbb{Q}(2^{\frac{1}{3}}, \omega)/\mathbb{Q}(2^{\frac{1}{3}})/\mathbb{Q}$. The Galois group must be S_3 since it is nonabelian. This is because $\mathbb{Q}(\alpha)/\mathbb{Q}$ is not normal. Its corresponding subgroup could not be abelian. Think of our field extension of $L/\mathbb{Q}$ as broken up: $L/\mathbb{Q}(\omega)/\mathbb{Q}$. We have

$$[L : \mathbb{Q}(\omega)] = 3$$

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$$

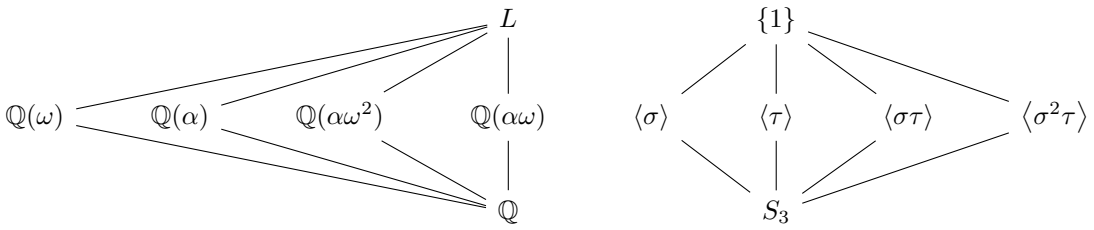
so that $x^3 - 2 \in \mathbb{Q}(\omega)[x]$ is irreducible. So there exists $\sigma : \alpha \mapsto \alpha\omega$. It fixes ω. There exists automorphism $\tau : \alpha \mapsto \alpha$, $\omega \mapsto \omega^2$. So $\sigma, \tau \in \mathrm{Gal}(L/\mathbb{Q})$. $\sigma^2 : \alpha \mapsto \alpha\omega^2$, $\omega \mapsto \omega$. $\sigma^3 = id$. Also

$$\tau^2 = id$$

$\sigma^3 = 1 = \tau^2$. So

$$\langle\sigma\rangle \lhd \mathrm{Gal}\,(L/K)$$

$\tau\sigma\tau^{-1} : \alpha \mapsto \alpha\omega^2$, $\omega \mapsto \omega$. So $\tau\sigma\tau^{-1} = \sigma^2$. We would like to draw intermediate fields

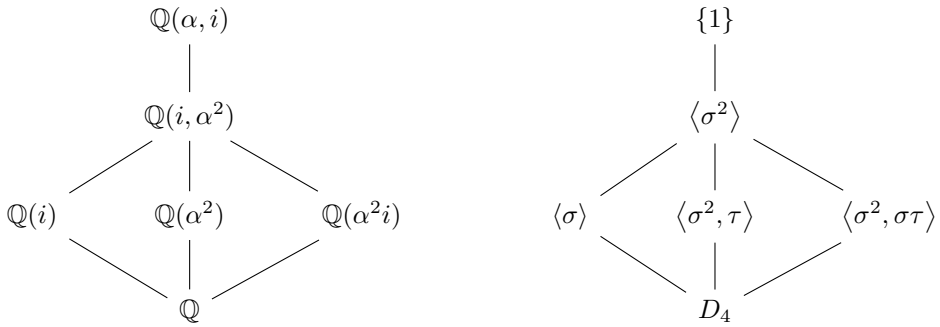


The diagram of the left are some intermediate fields, and the diagram on the right are their correponding subgroups.

Example. $f(x) = x^4 - 2 \in \mathbb{Q}[x]$. The splitting field is $L = \mathbb{Q}\,(\alpha, i)$, $\alpha = 2^{\frac{1}{4}}$. Note $\mathbb{Q}(i)$ over $\mathbb{Q}$ has degre 2, degree of L over $\mathbb{Q}(i)$ has degree 4. There exists $\alpha \mapsto \alpha i$, $i \mapsto i$. $\tau : \alpha \mapsto \alpha, i \mapsto -i$.

$$\tau\sigma\tau^{-1} = \sigma^3$$

$D_4 = \mathrm{Gal}(x^4 - 2) = \{1, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$.



On the left, you have intermediate fields and on the right you have subgroups. The reflections are $\tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau$. The corresponding fixed fields are $\mathbb{Q}(\alpha), \mathbb{Q}(\alpha(1+i)), \mathbb{Q}(\alpha i), \mathbb{Q}(\alpha(1-i))$.

Example. Now let's look at

$$\mathrm{Gal}(x^n - 1).$$

When does $x^n - 1 \in K[x]$ have distinct roots? Its gcd with nx^{n-1} is 1 if and only if $n \neq 0$ in K. Let K be a field of characteristic **not** dividing n ($\mathbb{Q}$). Let L be a splitting field for $x^n - 1$. THe set of roots is a group, which is hence a cyclic group. Any generator is called a **primitive n-th root of unity.** Let $G = \mathrm{Gal}(L/K)$. Let $G = \mathrm{Gal}(L/K)$ and $\zeta \in L$ be a primitive root. Then for all $\sigma \in G$, $\sigma(\zeta)$ is also a primitive root, so $\sigma(\zeta) = \zeta^i$ for some i with $gcd(i, n) = 1$. $G \to (\mathbb{Z}/n)^\times$ with $\sigma \mapsto i$. So G is a subgroup of $(\frac{\mathbb{Z}}{n})^\times$. Let

$$\Phi_n(x) = \prod_{\zeta \text{ primitive } n\text{-th root}} (x - \zeta)$$

Note that δ permutes the roots, so it fixes the polynomial. Hence the coefficients of Φ_n are in K as opposed to L. Any root of $x^n - 1$ is a primitive d-th root of unity for some $d|n$.

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

$\Phi_n(x)$ is called the n-th **cyclotomic polynomial**. Let's make

$$\Phi_1(x) = x - 1, \Phi_2(x) = x + 1, \Phi_3(x) = x^2 + x + 1, \Phi_4(x) = x^2 + 1$$

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$

$$\Phi_6(x) = \frac{x^6 - 1}{\Phi_1\Phi_2\Phi_3}$$

$$= \frac{x^6 - 1}{\Phi_2(x^3 - 1)} = \frac{x^3 + 1}{x + 1} = x^2 - x + 1$$

There was a conjecture saying that coefficients must always be zeros and ones, but that only holds for Φ_n for n up to 104.

Theorem 27. (**Bang**, 1895) $\Phi_{105}(x) = \cdots - 2x^{41} + \cdots - 2x^7 + \cdots$.

$\Phi_n(x) \in \mathbb{Z}[x]$ for all $n \geq 1$. If p is prime, $\Phi_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \ldots + x + 1$. The degree of $\Phi_n(x) = \varphi(n)$.

Theorem 28. (Dedekind, 1857) $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof. We have a monic polynomial with integer coeffcients. If it factors in $\mathbb{Q}$, then it factors in $\mathbb{Z}$ by Gauss's lemma. It suffices to show that $\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$. If $\Phi_n(x) = f(x)g(x)$ for f, g monic in $\mathbb{Z}[x]$, let ζ be a root of $\Phi_n(x)$, which must also be a root of f or g, say f. Suppose p is a prime not dividing n. ζ^p is also a primitive n-th root, so $\Phi_n(\zeta^p) = 0$. ζ^p is also a root of either f or g. If it's not a root of f, then it is a root of g. So ζ is a root of $g(x^p) \in \mathbb{Z}[x]$. But this means $f(x)$ and $g(x^p)$ share a common root. So $gcd(f(x), g(x^p)) \neq 1$. Consider $\frac{\mathbb{Z}[x]}{p\mathbb{Z}[x]}$, in which $\overline{\Phi_n(x)} = \overline{f(x)g(x)}$ (bar just means mod p). $\overline{x^n - 1}$ has distinct roots, so Φ_n also has distinct roots. Now

$$\overline{g(x^p)} = \left(\overline{g(x)}\right)^p$$

in $\frac{Z[x]}{p\mathbb{Z}[x]}$. So $gcd(\overline{f}, \overline{g}) \neq 1$, a contradiction to the fact that Φ_n has distinct roots. Hence, $f(\zeta) = 0$ and $p \nmid n$ implies $f(\zeta^p) = 0$. Any primitive root has the form ζ^r for some r coprime to n. Using our result, $f(\zeta) = 0$ implies $f(\zeta^r) = 0$, so f has all of the roots of Φ_n! Hence

$$\Phi_n(x) = f(x).$$

□

19 March 31

Last time, we were working with **cyclotomic polynomials** $\Phi_n(x)$, which is

$$\prod(x - \zeta)$$

where ζ runs through primitive n-th roots of 1. These may be computed inductively using $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

Theorem 29. $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$.

We have

Corollary 6.
1. $\Phi_n(x)$ is the minimal polynomial for $e^{2\pi i/n}$.
2. $\mathrm{Gal}_{\mathbb{Q}}(x^n - 1) = (\mathbb{Z}/n)^\times$.

Something we haven't proved yet is:

Theorem 30. (Kronecker-Weber) Every Abelian extension of $\mathbb{Q}$ (in particular every extension with Abelian Galois group) is contained in a cyclotomic extension of the form $\mathbb{Q}(e^{2\pi i/n})$.

Example. $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) = ?$

$$\begin{array}{c}\mathbb{Q}(\sqrt{2},\sqrt{3})\\ \Big|2\\ \mathbb{Q}(\sqrt{2})\\ \Big|2\\ \mathbb{Q}\end{array}$$

with $\sigma:\sqrt{2}\to\sqrt{2}$, $\sqrt{3}\to-\sqrt{3}$. The Galois group is generated by $\langle\sigma,\tau\rangle$ ($\tau:\sqrt{2}\to-\sqrt{2},\sqrt{3}\to\sqrt{3}$) and of order 4, so it must be the Klein 4-group. Note

$$\mathbb{Q}(\sqrt{2},\sqrt{3})\subset\mathbb{Q}\left(e^{2\pi i/24}\right)$$

as per the Kronecker Weber theorem (we haven't proved it, we just by coincidence found an example). Note

$$\mathrm{Gal}\left(\mathbb{Q}(e^{2\pi i/24})/\mathbb{Q}\right)=(\mathbb{Z}/24)^\times=\left(\frac{\mathbb{Z}}{8}\right)^\times\times\left(\frac{\mathbb{Z}}{3}\right)^\times$$

How many subgroups of order 2? 7. How many subgroups of order 4? 7! Every subgroup of $\left(\frac{\mathbb{Z}}{3}\right)^3$ is the kernel of

$$(\frac{\mathbb{Z}}{2})^3\twoheadrightarrow\frac{\mathbb{Z}}{2}$$

and $\mathrm{Hom}(\frac{\mathbb{Z}}{2}^3,\frac{\mathbb{Z}}{2})\cong(\frac{\mathbb{Z}}{2})^3$ has eight elements. We remove the 1 zero map.

There are 7 degree 2 extensions of $\mathbb{Q}$ inside $\mathbb{Q}(\sqrt{2},\sqrt{3},i)$. Namely: $\mathbb{Q}(\sqrt{2}),\mathbb{Q}(\sqrt{3}),\mathbb{Q}(i),\mathbb{Q}(\sqrt{2}\sqrt{3}),\mathbb{Q}(i\sqrt{2}),\mathbb{Q}(i\sqrt{3}),\mathbb{Q}(i\sqrt{6})$. There are 7 degree 4 extensions:

$$\mathbb{Q}(i,\sqrt{2}),\mathbb{Q}(i,\sqrt{3}),\mathbb{Q}(\sqrt{2},\sqrt{3}),\mathbb{Q}(\sqrt{2},i\sqrt{3}),\mathbb{Q}(\sqrt{6},i),\mathbb{Q}(i\sqrt{3},i\sqrt{2}),\mathbb{Q}(i\sqrt{2},\sqrt{3})$$

Example. Let $x_1,\ldots,x_n$ be indeterminates over $\mathbb{Q}$. Let

$$L=\mathbb{Q}(x_1,\ldots,x_n)$$

Let S_n act on L by permuting x_i.

$$\begin{array}{c}L\\ \Big||S_n|=n!\\ L^{S_n}\end{array}$$

Inside the fixed field is $\mathbb{Q}(e_1,\ldots,e_n)$ where $e_1=\sum x_i$, $e_2=\sum_{i<j}x_ix_j$,... Note

$$\prod_{i=1}^n(T-x_i)=T^n-e_1T^{n-1}+\ldots\pm e_n$$

splits in L. So $[L:\mathbb{Q}(e_1,\ldots,e_n)]\le n!$. Hence

$$L^{S_n}=\mathbb{Q}(e_1,\ldots,e_n)$$

$$\mathrm{Gal}\left(\mathbb{Q}(x_1,\ldots,x_n)/\mathbb{Q}(e_1,\ldots,e_n)\right)\cong S_n$$

(same if $\mathbb{Q}$ is replaced by any field). Any finite group is (up to isomorphism) a subgroup of S_n. Hence it is the Galois group of some field extension.

Remark. (Inverse Galois problem) Is every finite group G the extension of some $L/\mathbb{Q}$? We just showed any finite group is the Galois group of some extension of a field that is not necessarily $\mathbb{Q}$. The answer is yes for solvable groups.

Let $f(x) \in K[x]$ be a polynomial with distinct roots. Let L be its splitting field, $G = \mathrm{Gal}(L/K)$. Then G can be viewed as a subgroup of $\mathrm{Perm}\{\alpha_1, \ldots, \alpha_m\} \cong S_n$ where $f(x) = \prod_1^n (x - \alpha_i)$.

Proposition 16. G is a transitive subgroup of S_n if and only if f is irreducible.

Proof. Suppose f is irreducible. Then we have seen before that there is some element of the Galois group taking one root to another. Suppose G is transitive. G permutes roots of any irreducible factor. (the proof in class is kind of hand-wavy) □

Suppose $f(x) \in K[x]$ is irreducible, with distinct roots $\alpha_1, \ldots, \alpha_n$ in a splitting field L.

$$\sigma\left(\prod_{i<j}(\alpha_i - \alpha_j)\right)$$

$$= (\mathrm{sgn}(\sigma)) \prod_{i<j}(\alpha_i - \alpha_j)$$

Define $\Delta(f) = \prod_{i<j}(\alpha_i - \alpha_j)$. Then $\sigma(\Delta(f)^2) = \Delta(f)^2$, so $\Delta(f)^2 \in K$. The **discriminant of** f is $\Delta(f)^2$. Example:

$$D(x^2 + bx + c) = b^2 - 4c$$

$$D(x^3 + bx + c) = -4b^3 - 27c^2$$

Recall

$$G = \mathrm{Gal}(L/K) < S_n$$

Proposition 17. $G \cap A_n = \mathrm{Gal}(L/K(\Delta(f)))$

Proof. $\sigma \in \mathrm{Gal}(L/K(\Delta(f)))$ if and only if $\sigma \in G$ and σ fixes $\Delta(f)$ if and only if $\sigma \in G$ and $\sigma \in A_n$. □

Proposition 18. $G < A_n \Leftrightarrow \Delta(f) \in K$

$\Leftrightarrow D(f)$ is a square in K

Example. Suppose $f(x) \in K[x]$ is an irreducible degree 3 with distinct roots. Then $\mathrm{Gal}(f) = S_3$ or A_3. Writing $f(x) = x^3 + bx + c$,

$$\mathrm{Gal}(f) = \begin{cases} S_3 & \text{if } D(f) = -4b^3 - 27c^2 \text{ is not a square in } K \\ A_3 & \text{otherwise} \end{cases}$$

1. $f(x) = x^3 - 2$, $D(f) = -27 \cdot 4$ is not a square, so $\mathrm{Gal}(f) = S_3$.
2. $f(x) = x^3 - 3x + 1 \in \mathbb{Q}[x]$. $D(f) = 4 \cdot 27 - 27 = 81$ is a square, so $\mathrm{Gal}(f) = A_3$.
3. $f(x) = x^3 + 3x + 1$, $D(f) = -4 \cdot 27 - 27 = -5 \cdot 27 = -135$, which is not a square. Hence $\mathrm{Gal}(f) = S_3$. To check that the polynomial is irreducible, if it reduces then there is a rational root, which implies an integer root. THe integer root must divide 1, but neither case for the root actually works.

Radical solutions of cubics. Want to solve

$$x^3 + ax^2 + bx + c = 0$$

We can complete the cube with $x = y - \frac{a}{3}$. This gives

$$y^3 + py + q = 0$$

Set $y = z - \frac{p}{3z}$.

$$\left(z - \frac{p}{3z}\right)^3 + p(z - \frac{p}{3z}) + q = 0$$

$$z^3 - z^2\frac{p}{z} + 3z(\frac{p}{3z})^2 - \frac{p^3}{27z^3} + pz - \frac{p^2}{3z} + q$$

$$z^3 - \frac{p^3}{27z^3} + q = 0$$

where we can use the quadratic formula to solve for z^3. This gives formulae involving coefficients, square roots, cube roots, with which we can solve the cubic! The quadratic likely came around 1500 BC from Babylon. The Cubic can be traced to 1515 by Cardano. The quartic comes 1545 from Fe. We reduce the quartic to the cubic to solve it. The quintic and higher degree polynomials were proved in 1820 by Ruffini-Abel to be generally unsolvable by radicals. In 1832 Galois completely articulated what it means for something to be solvable.

20 April 5

Consider $f(x) \in K[x]$. We say that $f(x)$ is solvable by radicals if there exists fields

$$K \subset K(\omega_1) \subset K(\omega_1, \omega_2) \subset K(\omega_1, \omega_2, \ldots, \omega_n)$$

such that

1. $f(x)$ splits in $K[\omega_1, \ldots, \omega_n]$.
2. There exists $\gamma_i \in \mathbb{Z}_+$ such that
$$\omega_i^{\gamma_i} \in K(\omega_1, \ldots, \omega_{i-1})$$

Suppose $f(x)$ is a polynomial of degree 4 which is without loss of generality irreducible. Assume $f(x)$ has distinct roots $\alpha_1, \ldots, \alpha_4$.

$$x^4 + bx^3 + cx^2 + dx + e$$
$$= \prod_{i=1}^{4}(x - \alpha_i)$$

Then $\mathrm{Gal}(f) < S_4$. We have

$$S_4 \rhd \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} = N$$

Set

$$\alpha = \alpha_1\alpha_2 + \alpha_3\alpha_4$$
$$\beta = \alpha_1\alpha_3 + \alpha_2\alpha_4$$
$$\gamma = \alpha_1\alpha_4 + \alpha_2\alpha_3$$

Note that $N \cap \mathrm{Gal}(f)$ fixes these elements. Define $g(x) = (x - \alpha)(x - \beta)(x - \gamma)$. Let's see how any 2-cycle acts on g. It fixes α, and swaps β, γ. So it fixes g! Hence S_4 fixes g by similar calculations, so it is fixed by $\mathrm{Gal}(f)$ in $K[x]$. Indeed,

$$g(x) = x^4 + cx^2 + (bd - 4e)x - b^2e + 4ce - d^2$$

The discriminant for g is in fact the discriminant for f. One can also just compute manually the differences of roots: say

$$\alpha - \beta = (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)$$

$g(x)$ is solvable by radicals by last lecture (because it's a cubic), so radical extensions get us α, β, γ. Now

$$\alpha = \alpha_1\alpha_2 + \alpha_3\alpha_4$$

$$e = \alpha_1\alpha_2\alpha_3\alpha_4$$

$$(\alpha_1\alpha_2)^2 - \alpha_1\alpha_2(\alpha) + \alpha_1\alpha_2\alpha_3\alpha_4 = 0$$

so we can solve $\alpha_1\alpha_2$. Further radical extensions yield $\alpha_1\alpha_2$, $\alpha_1\alpha_3$, $\alpha_1\alpha_4$, $\alpha_2\alpha_3$, $\alpha_2\alpha_4$, $\alpha_3\alpha_4$. By calculations

$$\alpha_2/\alpha_3$$

is in the extension, and so is $\alpha_2\alpha_3$. Multiplying, α_2^2 is in the extension, and we can further extend to get α_2. By symmetry we can obtain $\alpha_1, \alpha_3, \alpha_4$.

Theorem 31. (Galois) Let $f(x)$ be an irreducible polynomial over a field of characteristic 0. Then

$$f(x)$$

is solvable by radicals if and only if $\mathrm{Gal}(f)$ is solvable.

Indeed, the group S_4 is solvable as we have shown. All the remainder of the class will be working towards a proof.

Lemma 12. Suppose a field K has a primitive n-th root of unity. Then

$$\mathrm{Gal}_K(x^n - a)$$

is abelian (in fact cyclic).

Proof. Let ζ be a primitive n-th root. Suppose α is one root of $x^n - a$. Then the roots are $\alpha\zeta^k$. $\mathrm{Gal}_K(x^n - a) \to \langle\zeta\rangle$ with $\sigma \mapsto \sigma(\alpha)/\alpha$ is an injective map into a cyclic group, and a subgroup of a cyclic group is cyclic. □

Proof. (One direction) Suppose $f(x)$ is solvable by radicals. There exists radical tower

$$K \subset K(\omega_1) \subset K(\omega_1, \omega_2) \subset \ldots \subset K(\omega_1, \ldots, \omega_n)$$

where $f(x)$ splits in $K(\omega_1, \ldots, \omega_n)$. There exists $\gamma_i \in \mathbb{N}$ where $\omega_i^{\gamma_i} \in K(\omega_1, \ldots, \omega_{i-1})$.Let ω_0 be a primitive $(\gamma_1\gamma_2\cdots\gamma_n)$-th root of 1.

$$K \subset K(\omega_0) \subset K(\omega_0, \omega_1) \subset \ldots \subset K(\omega_0, \ldots, \omega_n)$$

We want a radical tower that is Galois.

Interlude: Suppose $K \subset K(\alpha_1, \ldots, \alpha_n)$ is a separable extension. Let $f_i(x)$ be the minimal polynomial of α_i over K. Let $L \supset K(\alpha_1, \ldots, \alpha_n)$ be the splitting field of $\prod f_i(x)$. Then L/K is Galois. Let $G = \mathrm{Gal}(L/K) = \{\sigma_1 = e, \sigma_2, \ldots, \sigma_m\}$. Set $L' = K(\sigma_i(\alpha_j) : 1 \le i \le n, 1 \le j \le n)$. $|G| \le |\mathrm{Aut}_K(L')| \le [L' : K] \le [L : K] = |G|$ so equality holds. In particular, $L' = L$.

$$K \subset K(\sigma_1(\omega_0)) \subset K(\sigma_1(\omega_0), \sigma_2(\omega_0)) \subset \ldots \subset K(\sigma_1(\omega_0), \ldots, \sigma_m(\omega_0))$$
$$\subset K(\sigma_1(\omega_0), \ldots, \sigma_m(\omega_0), \sigma_1(\omega_1)) \subset \ldots \subset K(\sigma_i(\omega_j) \forall i, j)$$

where $\{\sigma_1, \ldots, \sigma_m\} = \mathrm{Gal}(\text{Galois closure of } K(\omega_0, \ldots, \omega_n) \text{ over } K/K)$. Every extension is radical. The latter most field is L' as in the above argument.

After a change of notation (make n bigger or something), there exists a radical tower

$$K \subset K(\omega_0) \subset K(\omega_0, \omega_1) \subset \ldots \subset K(\omega_0, \ldots, \omega_n) = L$$

where L/K is Galois (and f splits in L). Given tower $L_n/L_{n-1}/\ldots/L_0/K$. We have

$$\mathrm{Gal}\,(L/K) \rhd \mathrm{Gal}(L/L_0) \rhd \mathrm{Gal}(L/L_1) \rhd \ldots \rhd \mathrm{Gal}(L/L_{n-1}) \rhd \{e\}$$

where

$$\frac{\mathrm{Gal}\,(L/L_i)}{\mathrm{Gal}\,(L/L_{i+1})} \cong \mathrm{Gal}\,(L_{i+1}/L_i)$$

which is abelian (moreover cyclic) by the preceding lemma. So the Galois group is solvable. We have said that f splits inside some large extension that is Galois. Is $\mathrm{Gal}(f)$ solvable as a group? Let E be the splitting field of $f(x)$ inside L. We have tower $L/E/K$. We have $\mathrm{Gal}(E/K) = \mathrm{Gal}_K(f)$, which is what we want to show is solvable. It is isomorphic to

$$\mathrm{Gal}\,(L/K)\,/\mathrm{Gal}\,(L/E)$$

The image of a solvable group is solvable. This completes one direction for the theorem. □

Suppose L/K is Galois, so $G = \mathrm{Gal}(L/K)$. Define $N_{L/K} : L^\times \to K^\times$ by $\alpha \mapsto \prod_{\alpha \in G} \sigma(\alpha)$. Because the image is fixed by G, it lies in K. For example,

$$\mathbb{C}^\times \to \mathbb{R}^\times$$

is the usual norm but squared, $\overline{z}z$. The unit circle is the kernel. But this means $\overline{z}/z$ is in the kernel of the norm squared. In general, for $\beta \in L$,

$$N_{L/K}(\sigma(\beta)/\beta) = 1$$

Definition 14. A **character** is a group homomorphism $G \to K^\times$ where K is a field.

Theorem 32. (Dedekind) Distinct characters $\chi_1, \ldots, \chi_n : G \to K^\times$ are linearly independent. If

$$a_1\chi_1 + \ldots + a_n\chi_n = 0$$

then $a_i = 0$ for all i.

Proof. If not, take a minimal counterexample; a smallest n such that the equation holds. There exists $h \in G$ with $\chi_1(h) \neq \chi_2(h)$.

$$a_1\chi_1(hg) + \ldots + a_n\chi_n(hg) = 0$$
$$= a_1\chi_1(h)\chi_1(g) + \ldots + a_n\chi_n(h)\chi_n(g) = 0$$
$$a_1\chi_1(g) + \ldots + a_n\chi_n(g) = 0$$
$$a_1\chi_1(h)\chi_1(g) + \ldots + a_n\chi_1(h)\chi_n(g) = 0$$

and subtract it off:

$$a_2(\chi_2(h) - \chi_1(h))\chi_2(g) + \ldots + a_n(\chi_n(h) - \chi_1(h))\chi_n(g) = 0$$

this yields a contradiction since this holds for all g and n was supposed to be minimal. □

Theorem 33. (Hilbert's theorem 90) Suppose $\mathrm{Gal}(L/K) \cong \mathbb{Z}/n$ and $N_{L/K}(\alpha) = 1$ for some $\alpha \in L$. Then there exists $\beta \in L$ with

$$\alpha = \frac{\sigma(\beta)}{\beta}$$

21 April 12

Remark. Recall: A real number b is **constructible** if it can be obtained given

- 1 (a unit length)
- A straightedge
- A compass

Theorem 34. If b is constructible then $[\mathbb{Q}(b) : \mathbb{Q}] = 2^k$ for some k.

Theorem 35. If $b \in L$ where L is a Galois extension of $\mathbb{Q}$, with

$$[L : \mathbb{Q}] = 2^k$$

for some k, then b is constructible.

Proof. The Galois group is a 2-group, so it must be solvable. So

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_k = \{e\}$$

where

$$G_i/G_{i+1} = \mathbb{Z}/2$$

We have

$$L = L^{G_k} \supset L^{G_{k-1}} \supset \ldots \supset L^{G_0} = \mathbb{Q}$$

this is a tower of degree 2 extensions, which are each obtained from each other by adjoining roots of quadratics. □

Example.

$$f(x) = x^4 - 4x + 2$$

has derivatives

$$f'(x) = 4x^3 - 4 = 4(x^3 - 1)$$

which has a root at $x = 1$, at which $f(1) = -1$. This has 2 real roots. Say α is one of them. $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, but α is not constructible. The discriminant of $f(x)$ is -4864, which is not a square. This means

$$\mathrm{Gal}(f) \not\subset A_4$$

Based on the coefficients, there is a resolvent cubic $x^3 - 8x - 16$. This is irreducible because if it were reducible, it would factor over $\mathbb{Q}$, hence it would factor over $\mathbb{Z}$. That means that the constant coefficients of the two factored polynomials must divide -16. Hence $3||\mathrm{Gal}(f)|$. Hence there is an element of order 3 in $\mathrm{Gal}(f)$. The only transitive subgroups of S_4 with order a multiple of 3 are A_4 and S_4. Hence the Galois group is S_4, which doesn't have order a power of 2.

Suppose α is constructible. Let L be the splitting field of $f(x)$, L over $\mathbb{Q}(\alpha)$ and $\mathbb{Q}$. We assume α has degree 4, so there is an intermediate field $K \subset \mathbb{Q}(\alpha)$ which is a degree two extension of $\mathbb{Q}$. Likewise L has degree 6 over $\mathbb{Q}(\alpha)$. $G = \mathrm{Gal}(L/\mathbb{Q})$, and $N = \mathrm{Gal}(L/K)$. $N \lhd G$ since N has index 2. N contains a 3-cycle, hence all 3-cycles so $N = A_4$. But then $\mathrm{Gal}\,(L/\mathbb{Q}(\alpha))$ is a subgroup of order 6 in A_4.

Proposition 19. There are no subgroups of order 6 in A_4.

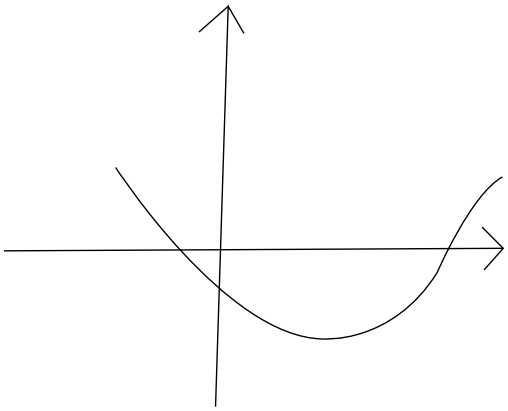


Figure 5: somegraphoff

Proof. The elements of A_4 : $e, (1\ 2)(3\ 4)$ (3 of these), $(1\ 2\ 3)$ (8 of these). Any order 6 group would have to contain $(1\ 2)(3\ 4), (1\ 2\ 3)$ (or other permutations of the same form). But the group generated by these two is more than 6 elements large.

□

Theorem 36. A regular n-gon is constructible by a straightedge and compass if and only if $n = 2^k p_1 \cdot \cdots \cdot p_m$ where $p_1, \ldots, p_m$ are distinct Fermat primes. Recall p is a Fermat prime $p = 2^{2^e} + 1$ for some integer e.

Given an n-gon, it is equivalent to constructing $\cos 2\pi/n$. Gauss proved $\cos 2\pi/17$ is constructible by square roots (google).

Proof. We have a tower $\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q}(\cos 2\pi/n)/\mathbb{Q}$. The degree of the first extension is at most 2. The whole extension has degree $\varphi(n)$, and it is Galois. A regular n-gon is constructible if and only if $\varphi(n)$ is a power of 2. Let $n = p_1^{f_1} \cdot \cdots \cdot p_m^{f_m}$ for primes $p_i \neq p_j$. Then

$$\varphi(n) = \prod \varphi(p_i^{f_i}) = \prod_i p_i^{f_i - 1}(p_i - 1)$$

So $\varphi(n)$ is a power of 2 precisely when $f_i = 1$ except perhaps when $p_i = 2$, and when $f_i = 1$ $p_i - 1$ is a power of 2. When is $2^t + 1$ prime? If $t = rs$ for s odd, $s > 1$, then $2^t + 1$ is not prime,

$$x^s + 1 = (x + 1)(x^{s-1} - x^{s-2} + \ldots + 1)$$

We would like to factor 2^{rs}, so we may set $x = 2^r$. If s is odd,

$$2^{rs} + 1 = (2^r + 1)(\cdots)$$

If $2^t + 1$ is prime, then t has no odd function, so $t = 2^e$. Hence primes of the form $2^t + 1$ are of the form $2^{2^e} + 1$. □

Now to another topic! **Transcendental extensions**: Recall a transcendental extension is not algebraic. That is, $K \subset L$ for fields K, L, elements $a_1, \ldots, a_n \in L$ are **algebraically independent** over K for any $f \in K[x_1, \ldots, x_n]$,

$$f(a_1, \ldots, a_n) \neq 0$$

That is,

$$K[x_1, \ldots, x_n] \xrightarrow{\text{eval}(a_1, \ldots, a_n)} L$$

is injective. A subset A of L is algebraically independent over K if each finite subset of A is algebraically independent.

Definition 15. The transcendence degree of L over K is defined to be

$$\text{transcdeg}_K L = \sup\{|A| : A \text{ is algebraically independent over } K\}$$

We would like to show that this is well defined.

Theorem 37. If $K \subset L$ are fields, suppose $\alpha_1, \ldots, \alpha_m$ are algebraically independent over K, and there exists $\beta_1, \ldots, \beta_n \in L$ such that each α_i is algebraic over $K(\beta_1, \ldots, \beta_n)$, then $m \leq n$.

Corollary 7. If $A = \{\alpha_1, \ldots, \alpha_m\}$ and $B = \{\beta_1, \ldots, \beta_n\}$ are maximal algebraically independent subsets of L over K, then $m = n$.

A set A or B as in the corollary is a **transcendence basis for L over K.** We get that such a set A makes $L/K(A)$ an algebraic extension.

Example. If $x_1, \ldots, x_n$ are indeterminates over K, then $L = K(x_1, \ldots, x_n)$ has transcendence basis $\{x_1, \ldots, x_n\}$. We also have $\{x_1^2, \ldots, x_n^2\}$ is a transcendence basis as well as $\{e_1, \ldots, e_n\}$. Now we have tower $K(x_1, \ldots, x_n)/K(e_1, \ldots, e_n)/K$. where e_i is the symmetric polynomial of degree i. Each x_i is a root of $\prod_{j=1}^n (T - x_j) = T^n - e_1 T^{n-1} + \ldots \pm e_n$.

Lemma 13. If β is algebraic over $K(\alpha_1, \ldots, \alpha_m)$, but **not** algebraic over $K(\alpha_1, \ldots, \alpha_{m-1})$. α_m is algebraic over $K(\alpha_1, \ldots, \alpha_{m-1}, \beta)$.

Proof. There exists $f(x_1, \ldots, x_m, y) \in K[x_1, \ldots, x_m, y]$ where

$$f(\alpha_1, \ldots, \alpha_m, \beta) = 0$$

and

$$f(\alpha_1, \ldots, \alpha_m, y) \neq 0$$

Let $f = \sum f_i x_m^i$ where $f_i \in K[x_1, \ldots, x_{m-1}, y]$. We have that the algebraic independence of $\alpha_1, \ldots, \alpha_{m-1}, \beta$ implies that $f_i(\alpha_1, \ldots, \alpha_{m-1}, \beta) \neq 0$ for some i. Hence this yields a nontrivial polynomial relation for x_m over $K[\alpha_1, \ldots, \alpha_{m-1}, \beta]$ □