10/1/15

HW 2 due today.
HW 3 TBA.

Today we are going to upgrade the First Isomorphism Theorem for groups.

Let $N \trianglelefteq G$ be a normal subgroup and consider the canonical quotient map

$$\pi : G \twoheadrightarrow G/N .$$

This induces a Galois connection

$$\pi : \mathcal{L}(G) \rightleftarrows \mathcal{L}(G/N) : \pi^{-1}$$

which restricts to an isomorphism of lattices

$$\pi : \mathcal{L}(G,N) \xleftrightarrow{\sim} \mathcal{L}(G/N) : \pi^{-1}$$

Let's examine this isomorphism. Suppose we have $H \in \mathcal{L}(G,N)$, i.e., H is a subgroup of G containing N.

Since $N \trianglelefteq G$ we also have $N \trianglelefteq H$ so we can define the quotient group H/N. The quotient map $H \twoheadrightarrow H/N$ is defined by

$$h \longmapsto hN .$$

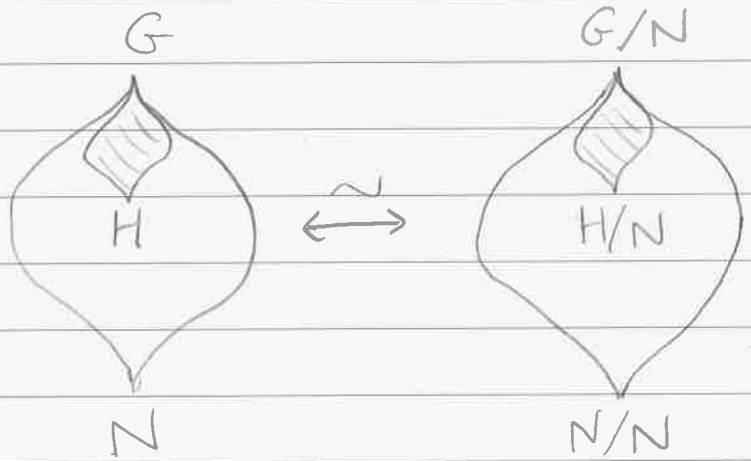
But note that this is the map $\pi : G \twoheadrightarrow G/N$ restricted to H. We conclude that

$$\pi(H) = H/N$$

and it follows that

$$\pi^{-1}(H/N) = H .$$

Picture:



Now suppose we also have $H \trianglelefteq G$, so we can define the quotient group G/H.

By the previous isomorphism we know that

$$\mathcal{L}(G, H) \approx \mathcal{L}(G/N, H/N).$$

Does this lattice isomorphism come from an isomorphism of groups

$$\frac{G}{H} \approx \frac{G/N}{H/N} \quad ?$$

What do we need to check?

Lemma: Consider a surjective group hom

$$\varphi : G \twoheadrightarrow G'$$

and two subgroups $H \leq G$, $H' \leq G'$.

- If $H \trianglelefteq G$ then $\varphi(H) \trianglelefteq G'$
- If $H' \trianglelefteq G$ then $\varphi^{-1}(H') \trianglelefteq G$.

Proof: For the first part suppose that $H \trianglelefteq G$ and consider $g' \in G'$, $h' \in \varphi(H)$. Since φ is surjective $\exists\ g \in G$, $h \in H$ such that $\varphi(g) = g'$, $\varphi(h) = h'$. Then since $H \trianglelefteq G$ we have $ghg^{-1} \in H$, hence

$$g'h'g'^{-1} = \varphi(g)\varphi(h)\varphi(g)^{-1}$$
$$= \varphi(ghg^{-1}) \in \varphi(H). \quad ///$$

For the second part suppose that $H' \trianglelefteq G$ and consider any $h \in \varphi^{-1}(H')$, $g \in G$. Since $\varphi(h) \in H'$ and $H' \trianglelefteq G$ we have

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} \in H'$$

and hence $ghg^{-1} \in \varphi^{-1}(H')$ ///

Returning to the situation

$N \trianglelefteq G$ and $H \in \mathcal{L}(G, N)$.

we have

$$H \trianglelefteq G \iff H/N \trianglelefteq G/N.$$

Proof: Consider the surjective hom.

$$\pi : G \twoheadrightarrow G/N$$

and note that $\pi(H) = H/N$, $\pi^{-1}(H/N) = H$. ///

★ Isomorphism Theorem (either the Second or Third, depending on who you ask):

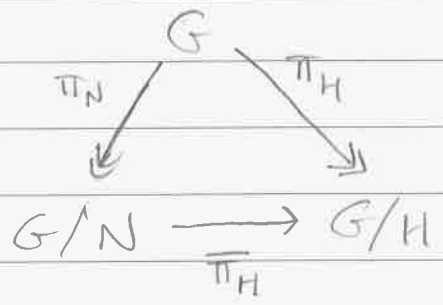
Let $N \trianglelefteq G$ and $H \in \mathcal{L}(G, N)$. Then we have $H \trianglelefteq G$ if and only if $H/N \trianglelefteq G/N$, in which case we get a group isomorphism

$$\frac{G}{H} \cong \frac{G/N}{H/N}$$

Proof: We will use the universal property of group quotients. Let $H \trianglelefteq G$ and consider the quotient homomorphisms

$$\pi_N : G \twoheadrightarrow G/N, \quad \pi_H : G \twoheadrightarrow G/H.$$

Since $\ker \pi_N = N \subseteq H = \ker \pi_H$, the universal property of π_N says that π_H factors through π_N as follows:



Since π_H is surjective we conclude that $\overline{\pi}_H : G/N \to G/H$ is surjective.

To finish the proof we will show that $\ker \overline{\pi}_H = H/N$, and hence

$$\frac{G/N}{H/N} = \frac{G/N}{\ker \overline{\pi}_H} \approx \operatorname{im} \overline{\pi}_H = G/H$$

by the First Isomorphism Theorem.

Recall that $\overline{\pi}_H$ is defined (uniquely) by

$$\overline{\pi}_H(gN) = \pi_H(g) = gH.$$

We conclude that

$$\overline{\pi}_H(gN) = 1_{G/H} \iff gH = 1_{G/H}$$
$$\iff g \in H,$$

and hence

$$\ker \bar{\pi}_H = \{ gN : g \in H \} = H/N. \quad ///$$

Remark: This theorem actually goes back to Galois. Let F be a field and consider a finite subgroup $G \subseteq \mathrm{Aut}(F)$. Recall the classical Galois connection.

$$\mathcal{L}(F) \rightleftarrows \mathcal{L}(\mathrm{Aut}(F))$$

$$E \longmapsto \mathrm{Aut}(F/E)$$
$$F^H \longleftarrow H$$

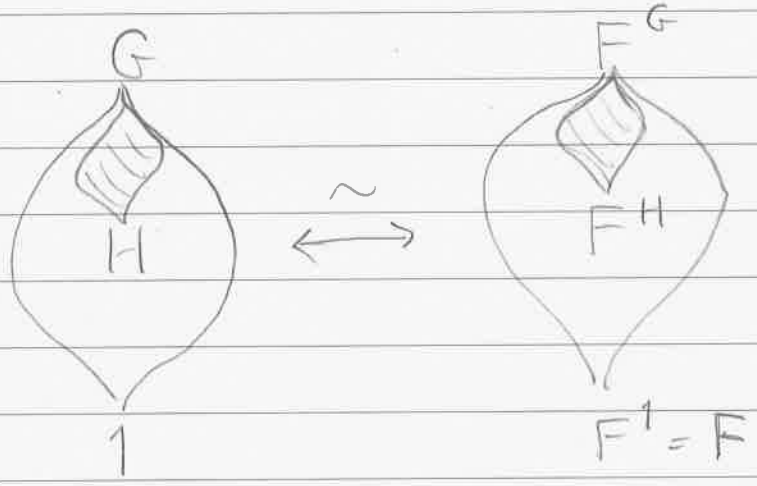
An important property I didn't mention the first time is that given a subgroup $H \subseteq G$ we have

$$H \trianglelefteq G \iff \text{the field extension } F^G \subseteq F^H \text{ is "Galois" (whatever that means)},$$

in which case we get an isomorphism of groups

$$\frac{G}{H} = \frac{Aut(F/F^G)}{Aut(F/F^H)} \approx Aut(F^H/F^G)$$

Picture.



In fact, this is the reason that Galois invented the concept of normal subgroups. Recall that the fundamental theorem says the following:

☆ F.T.G.T.: If $f(x) \in F^G[x]$ is a polynomial with splitting field F, then the polynomial is "solvable by radicals" if and only if there exists a chain of subgroups

{

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_m = 1$$

such that each quotient G_i/G_{i+1} is an abelian group. In this case we say by analogy that the group G is solvable.

My next goal is to examine some issues surrounding solvable groups.

Definition: We say that a group G is simple if it has no normal subgroups except 1 & G.

Example: Consider $n \in \mathbb{Z}$. Recall the fundamental theorem of cyclic groups

$$\mathcal{L}(\mathbb{Z}/n\mathbb{Z}) \approx \mathrm{Div}(n)^{op}.$$

Since every subgroup of $\mathbb{Z}/n\mathbb{Z}$ is normal, we conclude that $\mathbb{Z}/n\mathbb{Z}$ is a simple group if and only if n is prime.

Thus, in some sense, simple groups are a generalization of prime numbers.

///

Now suppose that G is not simple. In this case we would like to "factorize" G into simple groups.

Here's how we will proceed: Let $G_0 = G$. Since G is not simple we can find a nontrivial normal subgroup. Let G_1 be a maximal such group [Warning: This G_1 might not exist if G is badly infinite. Let's just assume that G_1 exists.].

Claim: Then the quotient G_0/G_1 is a simple group.

Proof: We have a lattice isomorphism

$$\mathcal{L}(G_0, G_1) \approx \mathcal{L}(G_0/G_1)$$

that preserves normality.

{

Since there are no normal subgroups between G_0 & G_1 (by definition) we conclude that there are no normal subgroups between G_0/G_1 and 1. ///

Now we continue the process. Let G_2 be a maximal proper normal subgroup of G_1 so that the quotient G_1/G_2 is simple.

If this process is able to continue, and if it terminates, then we obtain a chain of subgroups

$$(*) \quad G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_m = 1$$

such that G_i/G_{i+1} is simple for all i. We call such a chain $(*)$ a composition series for G and the simple quotients G_i/G_{i+1} are called "the" composition factors of G.

[Why did I say "the"?]

10/6/15

HW 2 due now.
HW 3 TBA

Recall: We say that a group G is simple if the trivial subgroup $1 \trianglelefteq G$ is maximal among proper normal subgroups. [In particular, we must have $1 \neq G$.]

Theorem: The simple abelian groups are just $\mathbb{Z}/p\mathbb{Z}$ for p prime.

Proof: Let G be a simple abelian group. Since $G \neq 1$, there exists an element $1 \neq a \in G$. Since $1 \subsetneq \langle a \rangle \trianglelefteq G$ and since 1 is maximal normal, we have $\langle a \rangle = G$, hence G is cyclic.

Note that $\mathbb{Z}$ is not simple, so G must be finite, say $|G| = |\langle a \rangle| = n$. If there exists $1 < k < n$ with $k \mid n$ then we obtain a proper normal subgroup

$$1 = \langle a^n \rangle \subsetneq \langle a^k \rangle \trianglelefteq \langle a^1 \rangle = G,$$

which contradicts the fact that G is simple. We conclude that n is prime. ///

Thus simple groups are a generalization of prime numbers, and the interesting simple groups are non-abelian.

Examples:

(1) The group of rotational symmetries of the regular dodecahedron / icosahedron is a simple group of order $60 = 2^2 \cdot 3 \cdot 5$. It is the smallest non-abelian simple group.

(2) If we view S_n as the group of $n \times n$ permutation matrices, then the determinant is a surjective group homomorphism onto the group of units $\mathbb{Z}^\times = \{\pm 1\}$,

$$\det : S_n \twoheadrightarrow \mathbb{Z}^\times .$$

The kernel is a normal subgroup,

{

called the alternating group:

$$A_n := \ker(\det) \trianglelefteq S_n$$

By the First Isomorphism Theorem and Lagrange's Theorem (i.e. the fact that there is a bijection between any two cosets) we have

$$|S_n| / |A_n| = |\mathbb{Z}^\times|.$$

$$|A_n| = |S_n| / |\mathbb{Z}^\times|$$

$$= n! / 2$$

$$= 3 \cdot 4 \cdot 5 \cdots n.$$

Theorem: The group A_n is simple for all $n \geq 5$. Moreover, A_5 is isomorphic to the unique simple group of order 60.

Corollary: There exist infinitely many non-abelian simple groups.

(3) Let K be a field and consider the general linear group $GL_n(K)$. The determinant is a surjective homomorphism onto the group of units $K^\times = K \setminus \{0\}$,

$$\det : GL_n(K) \twoheadrightarrow K^\times$$

The kernel is a normal subgroup, called the special linear group:

$$SL_n(K) := \ker(\det) \trianglelefteq GL_n(K).$$

The center of $GL_n(K)$ is given by scalar matrices

$$Z(GL_n(K)) = \{\alpha I : \alpha \in K, \alpha \neq 0\}.$$

and the center of $SL_n(K)$ is given by n^{th} roots of unity

$$Z(SL_n(K)) = \{\alpha I : \alpha \in K, \alpha^n = 1\}.$$

The center is always normal, we kill it by defining the projective special linear group:

$$PSL_n(K) := \frac{SL_n(K)}{Z(SL_n(K))}.$$

Theorem: The group $PSL_n(K)$ is simple for all $n \geq 2$ and for all fields K, except when $n=2$ and $K = \mathbb{F}_2$ or $\mathbb{F}_3$.

[Remark: I proved this theorem last time I taught the course and it ate up too much time, so I won't prove it this time. I might (or you might) prove that A_n is simple.]

When $K = \mathbb{F}_q$ is a finite field of order q, we usually just write

$$PSL_n(\mathbb{F}_q) = PSL_n(q).$$

This gives us another infinite family of finite simple groups. One can check that

$$|PSL_n(q)| = \frac{q^{\binom{n}{2}}(q^2-1)(q^3-1)\cdots(q^n-1)}{\gcd(n, q-1)}.$$

There is a sense in which

$$PSL_n(q) \longrightarrow A_n \quad \text{as} \quad q \to 1,$$

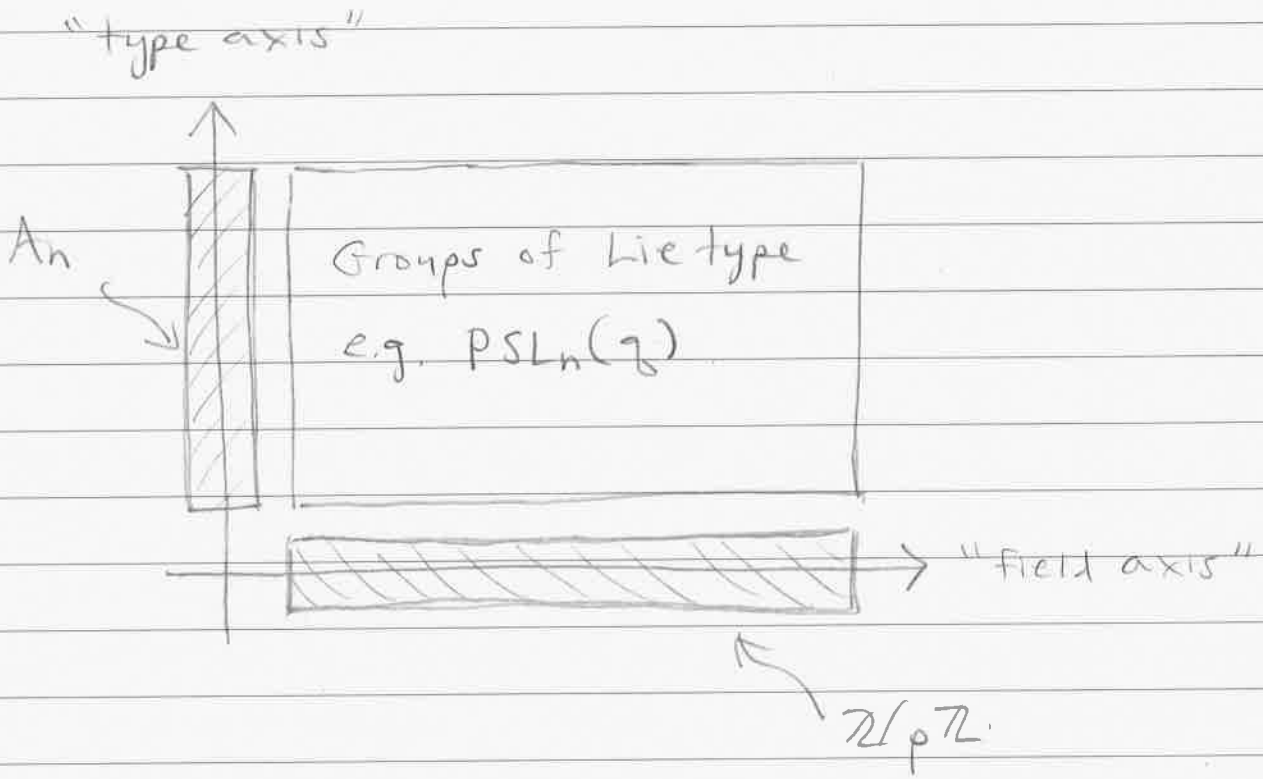
but nobody really knows what this means because there is no such thing as a "field of order 1".

(4) After a century of work an thousands of pages of theorems, the finite simple groups have been classified.

HUGE THEOREM: There are 18 infinite families and 26 "sporadic" finite simple groups. The largest sporadic group is called the Monster $\mathbb{M}$. It has order.

$$|\mathbb{M}| \approx 8 \cdot 10^{53}.$$

The 18 infinite families can be visualized as follows:



The classification of finite groups of Lie type depends on the classification of semisimple Lie algebras.

Apart from classifying all simple groups, the other major problem is to show how to "put together" simple groups to obtain all other groups.

We began to discuss this last time.

Let G be a group and suppose that we can find a chain of subgroups

$$(*) \quad G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_m = 1$$

such that G_{i+1} is a maximal proper normal subgroup in G_i for all i. In this case we say that $(*)$ is a composition series for G. Since G_{i+1} is maximal normal in G_i we know that the quotient G_i/G_{i+1} is a simple group. The groups G_i/G_{i+1} are called "the" composition factors of G.

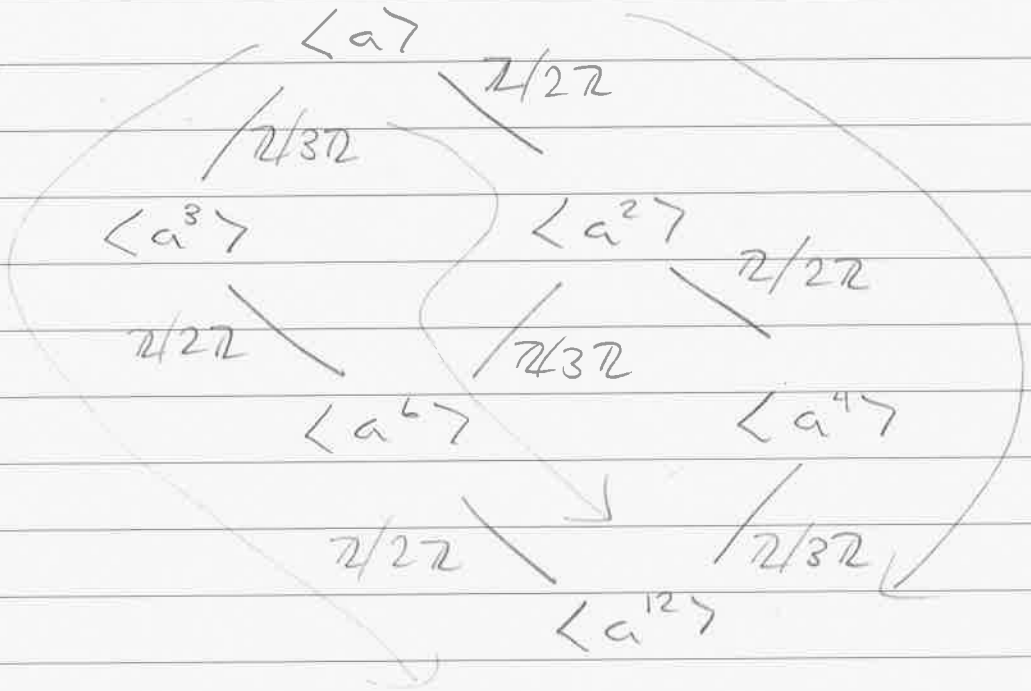
Q: Why "the"?

★ Theorem (Jordan-Hölder): Let G be a group. If G has a composition series then any two composition series are "equivalent" in the sense that

- they have the same length
- the composition factors are isomorphic in pairs (up to a permutation).

Remark: If $G = \mathbb{Z}/n\mathbb{Z}$ then the J.-H. theorem just says that n has a unique prime factorization.

For example, if $n = 12$ then there are three composition series. Let $\mathbb{Z}/12\mathbb{Z} = \langle a \rangle$.

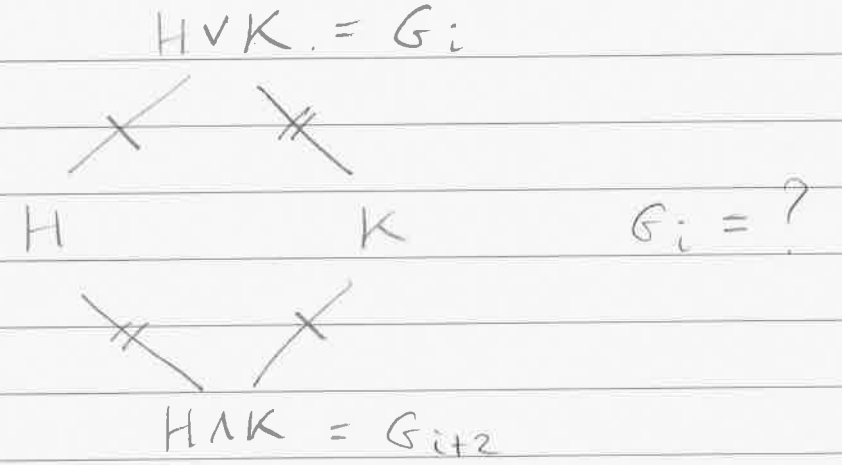


The composition factors are

- $\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}$
- $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}$
- $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}$.

///

Note that the composition series are related by "local swaps". Suppose we have two maximal normal subgroups H, K in G_i such that $H \vee K = G_i$ and $H \wedge K = G_{i+2}$:



We would like to show that

$$\frac{H \vee K}{H} \approx \frac{K}{H \wedge K} \quad \& \quad \frac{H \vee K}{K} \approx \frac{H}{H \wedge K}$$

so we could move from one composition series to another without changing the composition factors. But is this true?

A: Yes. You will prove it on HW3.

We could give a proof of Jordan-Hölder using just this fact, but to get a very slick proof we will use two lemmas that are perfectly defined for the task:

(1) Zassenhaus ("Butterfly") Lemma.
(2) Schreier Refinement Theorem.

Stay tuned...

10/13/15

HW 2 is done.
HW 3 will be due Tues Oct 27.
Let's have the midterm Thurs Oct 29.

Recall the statement of the Jordan-Hölder theorem for groups:

Let G be a group. If G has a composition series, i.e., a chain of subgroups

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_m = 1$$

such that G_i/G_{i+1} is simple for all i, then any two composition series are equivalent in the sense that

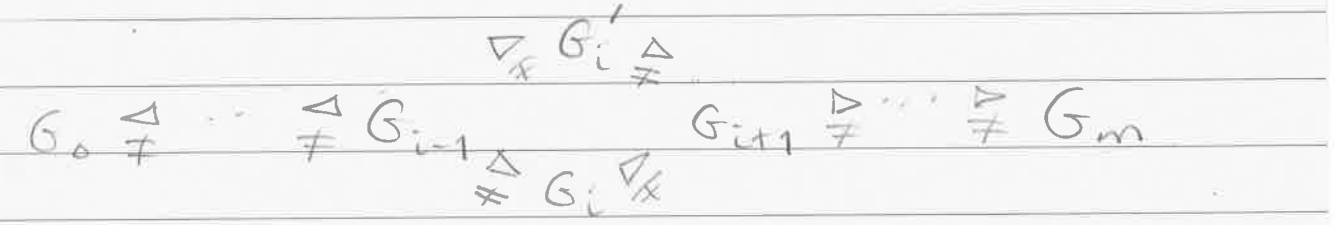
- they have the same length
- the composition factors G_i/G_{i+1} are isomorphic up to a permutation

///

One can prove the Theorem using HW 3 Problem 2 by showing that

§

any two composition series are related by "local swaps" of the form



where $G_i \vee G_i' = G_{i-1}$ & $G_i \wedge G_i' = G_{i+1}$.

[In this case HW 3.2 says that

- $G_{i-1}/G_i \approx G_i'/G_{i+1}$
- $G_i/G_{i+1} \approx G_{i-1}/G_i'$,

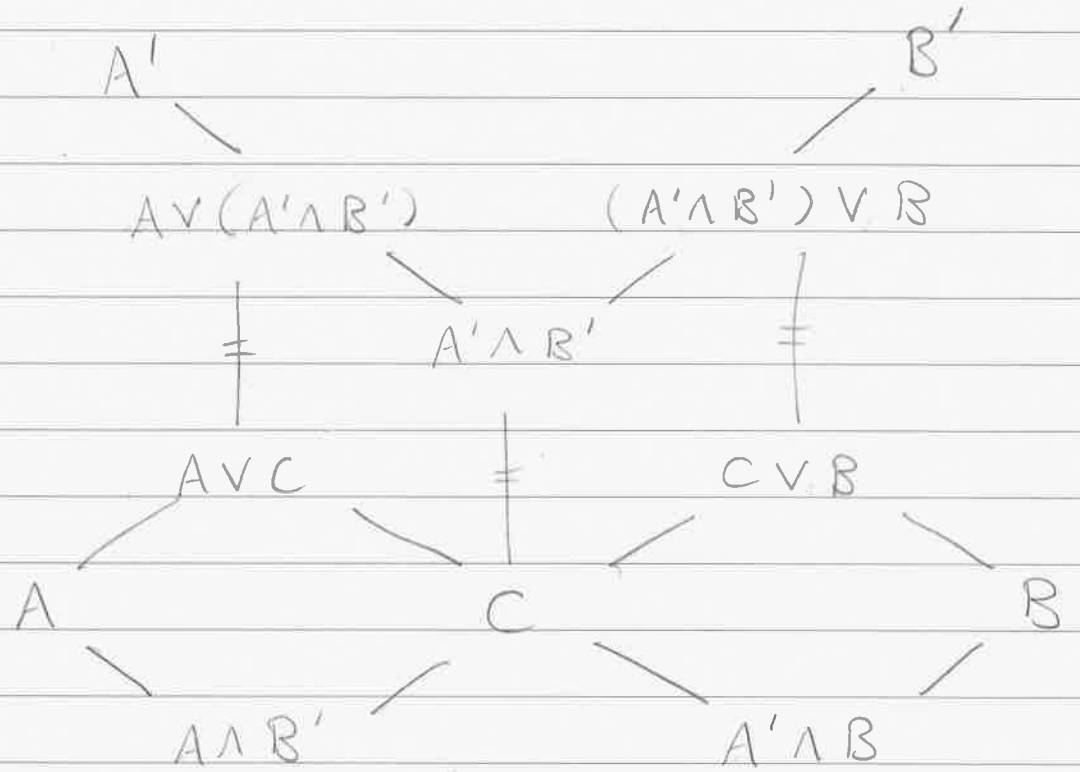
so the composition factors are preserved.]

But I prefer to give the "book proof", using two lemmas that were explicitly designed to give the smoothest proof of Jordan-Hölder.

(1) Zassenhaus ("Butterfly") Lemma.
(2) Schreier Refinement Theorem.

① Zassenhaus Lemma.

If $A, A', B, B' \leq G$ are subgroups with $A \leq A'$ & $B \leq B'$, then we obtain a diagram that looks like an upside-down butterfly:



Here we have defined

$$C := (A \wedge B') \vee (A' \wedge B) .$$

The Lemma says that <u>if</u>

$$A \trianglelefteq A' \quad \& \quad B \trianglelefteq B'$$

then we also have

$$A \vee C \trianglelefteq A \vee (A' \wedge B') \quad \& \quad C \vee B \trianglelefteq (A' \wedge B') \vee B$$

and an isomorphism of groups

$$\frac{A \vee (A' \wedge B')}{A \vee C} \cong \frac{(A' \wedge B') \vee B}{C \vee B}.$$

Finally, since

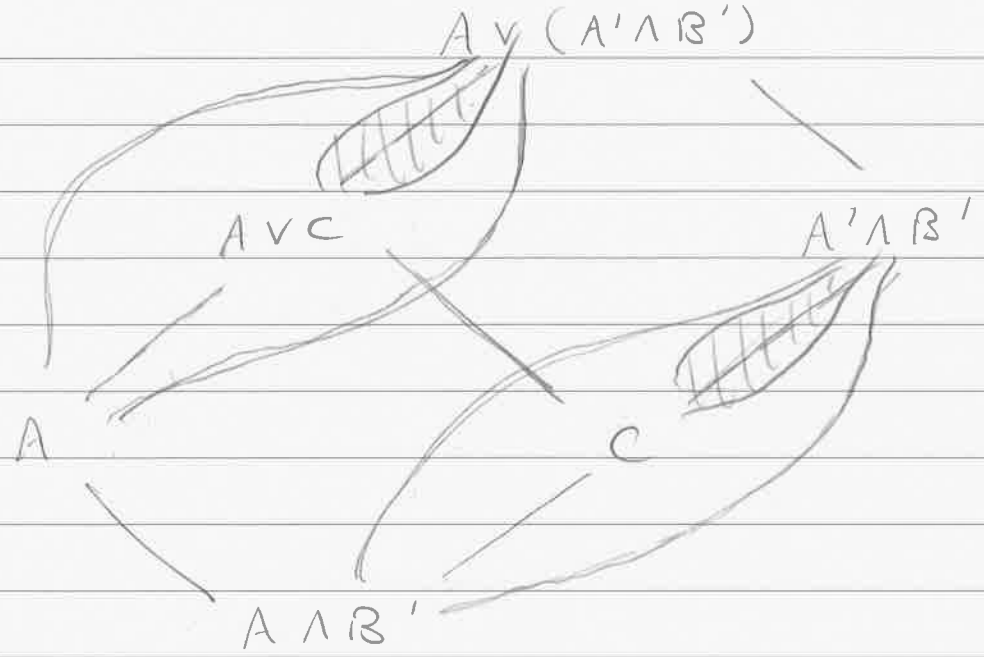
$$\begin{aligned} A \vee C &= A \vee [(A \wedge B') \vee (A' \wedge B)] \\ &= [A \vee (A \vee B')] \vee (A' \wedge B) \\ &= A \vee (A' \wedge B) \end{aligned}$$

$$\begin{aligned} C \vee B &= [(A \wedge B') \vee (A' \wedge B)] \vee B \\ &= (A \wedge B') \vee [(A' \wedge B) \vee B] \\ &= (A \wedge B') \vee B \end{aligned}$$

we obtain an isomorphism

$$\frac{A \vee (A' \wedge B')}{A \vee (A' \wedge B)} \cong \frac{(A' \wedge B') \vee B}{(A \wedge B') \vee B}.$$

Proof: Let $A \trianglelefteq A'$ and $B \trianglelefteq B'$ and consider the diagram



Since $A \trianglelefteq A'$ we have $A \trianglelefteq A \vee (A' \wedge B')$ and $A \wedge B' \trianglelefteq A' \wedge B'$. Then since

$$A \wedge (A' \wedge B') = (A \wedge A') \wedge B' = A \wedge B',$$

HW 3.2 gives an isomorphism

$$\frac{A \vee (A' \wedge B')}{A} \cong \frac{A' \wedge B'}{A \wedge B'}$$

HW 3.1 says that the resulting isomorphism of Lattices

is given explicitly by

$$[A, A \vee (A' \wedge B')] \underset{(-)\wedge(A'\wedge B')}{\overset{A\vee(-)}{\rightleftarrows}} [A \wedge B', A' \wedge B']$$

Note that this isomorphism identifies $A \vee C$ with C. This means that they are both normal or both non-normal. One can check that they are both normal, so we obtain an isomorphism

$$\frac{A \vee (A' \wedge B')}{A \vee C} \cong \frac{A' \wedge B'}{C}$$

A parallel argument gives

$$\frac{A' \wedge B'}{C} \cong \frac{(A' \wedge B') \vee B}{C \vee B}.$$

(2) Schreier Refinement Theorem.

Let G be a group. Then any two chains of subgroups

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_m = 1$$
$$G = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_n = 1$$

have equivalent refinements.

Proof: Refine the first chain by inserting between each $G_i \trianglerighteq G_{i+1}$ the chain of subgroups

$$G_i = G_{i+1}(G_i \wedge H_0) \trianglerighteq \cdots \trianglerighteq G_{i+1}(G_i \wedge H_n) = G_{i+1}.$$

Similarly, refine the second chain by inserting between $H_j \trianglerighteq H_{j+1}$ the chain

$$H_j = (G_0 \wedge H_j)H_{j+1} \trianglerighteq \cdots \trianglerighteq (G_m \wedge H_j)H_{j+1} = H_{j+1}.$$

Now the subquotients of the first refined chain have the form

$$(*) \qquad \frac{G_{i+1}(G_i \wedge H_j)}{G_{i+1}(G_i \wedge H_{j+1})}$$

for all $1 \leq i \leq m$ & $1 \leq j \leq n$. And the subquotients of the second refined chain have the form

$$(**) \qquad \frac{(G_i \wedge H_j) \vee H_{j+1}}{(G_{i+1} \wedge H_j) \vee H_{j+1}}$$

for all $1 \leq i \leq m$ & $1 \leq j \leq n$. Finally, the Zassenhaus Lemma says that the groups (*) & (**) are isomorphic. ///

☆ Proof of Jordan-Hölder:

Consider any two composition series

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_m = 1.$$
$$G = H_0 \rhd H_1 \rhd \cdots \rhd H_n = 1.$$

Since the subquotients are simple, the only way to refine either chain is by repeating some of the groups. The Schreier Refinement Theorem says it is possible to do this so that the composition factors are the same.

↓

If we ignore the trivial subquotients, it follows that the original subquotients were the same.

QED.

Remarks:

- As I mentioned last time, J-H applied to cyclic groups is just the Fundamental Theorem of Arithmetic (unique prime factorization of integers).

- The original motivation for this theorem comes from Galois Theory. Recall: If $f(x) = K[x]$ has irreducible factors that are separable, and splitting field L, then $f(x) = 0$ is solvable by radicals if and only if the group $\mathrm{Aut}(L/K)$ is "solvable". We can now rephrase the definition of solvable groups.

Def: A group G is solvable if its composition factors are abelian; equivalently, if its composition factors are $\mathbb{Z}/p\mathbb{Z}$ for various primes p.

An interesting special case of this says that $f(x) = 0$ is solvable with ruler & compass constructions if and only if the composition factors of $Aut(L/K)$ are all $\mathbb{Z}/2\mathbb{Z}$. [This is a generalization of the Gauss-Wantzel theorem which says that the regular n-gon is constructible if and only if $\varphi(n)$ is a power of 2.]

- Otto Hölder (1859 – 1937) was led to the J-H theorem by his study of Galois theory. Hölder was also the first person to seriously attempt a classification of finite groups. The two steps of this "Hölder Program" are

(i) Classify finite simple groups
(ii) Determine how every finite group can be built up from its simple composition factors.

Part (i) is now completed, as you know. Part (ii) is now called the "extension problem" for groups. It is somehow "dual" to the "factorization problem" that we studied before.

Definition: Let N & Q be groups. We say that a group G is an "extension of N by Q" if G has a subgroup $\tilde{N}$ isomorphic to N such that $G/\tilde{N}$ is isomorphic to Q; equivalently, if there exists a short exact sequence

$$1 \longrightarrow N \longrightarrow G \longrightarrow Q \longrightarrow 1.$$

You will show on HW3 that the easiest kind of group extension is a semi-direct product $G = N \rtimes_\varphi Q$.

The general problem of extensions is very difficult and leads to the subject of "group cohomology".

- The J-H theorem is essentially a theorem of lattice theory. It holds in any modular or semi-modular lattice. The concept of a modular lattice was invented by Dedekind to model the lattice of submodules of a module over a commutative ring. We'll return to this later.

10/15/15

HW3 due Tues Oct 27
Midterm Exam Thurs Oct 29.

Last time we proved that the (simple) composition factors of a group are unique. This leads to a program of research sometimes referred to as "Hölder's Program":

(i) Classify finite simple groups.
(ii) Describe how to reconstruct every finite group from its simple factors.

Part (i) is complete, but Part (ii) is far from complete even in the case of solvable groups (with factors of the form $\mathbb{Z}/p\mathbb{Z}$ for prime p).

For example, suppose finite group G has composition factors H & K. This means that there exists a chain

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 = 1$$

such that $\{G/G_1, G_1\} \approx \{H, K\}$.

Without loss of generality, suppose that $G_1 \cong K$ and $G/G_1 \cong H$. Now consider the maps

$$K \xrightarrow{\sim} G_1 \hookrightarrow G_1 \quad \& \quad G \twoheadrightarrow G/G_1 \xrightarrow{\sim} H$$

α β

The pair of maps

$$K \xhookrightarrow[\alpha]{} G \xrightarrow[\beta]{} H$$

is called exact because $\operatorname{im}\alpha = \ker\beta$ (both are equal to G_1). The notation of "exactness" also gives us a fancy way to say that α is injective and β is surjective. Recall that the trivial group 1 is the zero object in the category of groups (meaning it has a unique map to and from each other group). We will say that a sequence of groups and maps

$$\cdots \xrightarrow{\alpha_{-2}} A_{-1} \xrightarrow{\alpha_{-1}} A_0 \xrightarrow{\alpha_0} A_1 \xrightarrow{\alpha_1} A_2 \xrightarrow{\alpha_2} \cdots$$

is exact at A_i if $\operatorname{im}\alpha_{i-1} = \ker\alpha_i$.

We say that the sequence is exact if it is exact at every position. Now we can rephrase the relationship between K, G, H by saying that the sequence

$$1 \longrightarrow K \xrightarrow{\alpha} G \xrightarrow{\beta} H \longrightarrow 1$$

is exact. Exactness at K means that $\ker \alpha = 1$ (i.e., α is injective) and exactness at H means that $\operatorname{im} \beta = H$ (i.e., β is surjective). A sequence of this form is called a short exact sequence.

Back to the problem at hand: We want to describe G in terms of K & H. There are two "relatively" easy cases:

(1) Suppose there exists a group hom $r : G \longrightarrow K$ such that $r \circ \alpha = id_K$ (this is called a left-inverse or a retract of α). If such an r exists we say that the short exact sequence is "left-split".

In this case I claim that $G \cong K \times H$.

Proof: Define a function $\gamma : G \to K \times H$ by $\gamma(g) := (r(g), \beta(g))$. This is a group hom because r & β are group homs.

- To see that γ is injective, suppose that $\gamma(g) = (1_K, 1_H)$, i.e., $r(g) = 1_K$ & $\beta(g) = 1_H$. Since $\beta(g) = 1_H \Rightarrow g \in \ker\beta$, the condition $\text{im}\,\alpha = \ker\beta$ implies that $g = \alpha(k)$ for some $k \in K$. Then since $k = r(\alpha(k)) = r(g) = 1_K$ we conclude that $g = \alpha(k) = \alpha(1_K) = 1_G$ as desired.

- To see that γ is surjective, consider any $(k, h) \in K \times H$. Since β is surjective, $\exists\ g \in G$ such that $\beta(g) = h$. Now the inverse image $\beta^{-1}(h)$ contains g and is a coset of the kernel, hence

$$\begin{aligned}\beta^{-1}(h) &= g\ker\beta \\ &= g\,\text{im}\,\alpha \\ &= \{g\alpha(k') : k' \in K\}.\end{aligned}$$

To finish, we want to find $k' \in K$ such that $r(g\alpha(k')) = k$

so then we will have

$$\gamma(g\alpha(k')) = (r(g\alpha(k')), \beta(g\alpha(k'))) = (k, h),$$

as desired. Since r is a group hom, we need $k = r(g\alpha(k')) = r(g)\,r(\alpha(k')) = r(g)k'$. So we can take $k' = r(g)^{-1}k$.

We conclude that $\gamma: G \to K \times H$ is a group isomorphism.

Q.E.D.

(2) Suppose there exists a group hom $s: H \to G$ such that $\beta \circ s = id_H$ (this is called a right-inverse or a section of β). If such an s exists then we say the short exact sequence is "right-split".

Note that left-split $\Longrightarrow$ right-split. Indeed, given a retract $r: G \to K$ we can define a section $s: H \to G$ via the isomorphism $\gamma: G \xrightarrow{\sim} K \times H$ by taking $s(h) := \gamma^{-1}(1_K, h)$.

Note that by definition of γ the following square commutes:

$$\begin{array}{ccc} \gamma^{-1}(1_K, h) \in G & \xrightarrow{\beta} & H \ni \beta(\gamma^{-1}(1_K, h)) \\ \gamma \downarrow & & \downarrow id_H \\ (1_K, h) \in K \times H & \xrightarrow[\pi_2]{} & H \ni h \end{array}$$

It follows that

$$\beta(s(h)) = \beta(\gamma^{-1}(1_K, h)) = h \quad \forall\, h \in H .$$

In the category of abelian groups, we also have

$$\text{right-split} \Longrightarrow \text{Left-split},$$

but for general groups this is not true. You will prove on HW3 Problem 5 that in general we have

$$\text{right-split} \Longrightarrow G \cong K \rtimes_\varphi H$$

for some $\varphi : H \to Aut(K)$.

Believe it or not, split exact sequences are regarded as "trivial" in a certain sense (but I don't find the proof trivial).

The easiest example of a non-split s.e.s. is the following short exact sequence of abelian groups

$$(*) \qquad 0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

Note that $\ker(\cdot 2) = 0$, $\operatorname{im}\pi = \mathbb{Z}/2\mathbb{Z}$, and $\operatorname{im}(\cdot 2) = \ker\pi = 2\mathbb{Z}$.

Now suppose we have a homomorphism $s : \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}$. If s is not the zero map then it must send $1 \in \mathbb{Z}/2\mathbb{Z}$ to some $0 \neq a \in \mathbb{Z}$. But then since s is a homomorphism we have

$$\begin{aligned} 2a = a + a &= s(1) + s(1) \\ &= s(1+1) = s(0) = 0. \end{aligned}$$

Contradiction. We conclude that s must be the zero map,

which is certainly not a right-inverse of $\pi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$. Therefore the sequence (*) is not right-split. Since the groups are abelian it follows that (*) is also not left-split, but this can also be checked directly.

Remark: The algebraic fact that (*) doesn't split has a topological interpretation. It says that a möbius band can not be retracted onto its boundary circle.

Proof (for those who have seen some algebraic topology): Consider the möbius band M and its boundary circle ∂M. Let $i : \partial M \hookrightarrow M$ be the inclusion map. A retraction is a continuous map $r : M \twoheadrightarrow \partial M$ such that $r \circ i = id_{\partial M}$.

Recall that the fundamental groups are $\pi_1(M) = \pi_1(\partial M) = \mathbb{Z}$. Applying the π_1 functor to the maps r & i gives homomorphisms $i_* : \pi_1(\partial M) \to \pi_1(M)$ and $r_* : \pi_1(M) \to \pi_2(\partial M)$ §

such that $r_* \circ i_* = id_{\pi_1(\partial M)}$. Since the boundary wraps around twice, we also know that $i_* : \mathbb{Z} \to \mathbb{Z}$ is multiplication by 2.

Finally, the fact that no such map r_* exists is equivalent to the fact that the sequence (*) doesn't split. //

The language of exact sequences emerged from topology but it has also become an important language for algebra.

10/20/15

HW3 due Tues Oct 27
Midterm Exam Thurs Oct 29.

We have discussed the notions of "simplicity" and "solvability" of groups, which emerged from the study of Galois theory. Before moving on, I would like to finish the proof of the Abel–Ruffini Theorem (unsolvability of the quintic). For now I will just assume the Fundamental Theorem of Galois Theory [I hope to prove it next semester].

Consider a polynomial $f(x) \in \mathbb{Q}[x]$ of degree n having n distinct roots

$$r_1, r_2, \cdots, r_n \in \mathbb{C}$$

Let $K = \mathbb{Q}(r_1, r_2, \cdots, r_n)$ be the smallest subfield of $\mathbb{C}$ containing $\{r_1, r_2, \cdots, r_n\}$; i.e., let K be the splitting field of the polynomial $f(x)$.

Then we define the Galois group of the polynomial as

$$G = \mathrm{Aut}(K/\mathbb{Q}).$$

Actually, the "$/\mathbb{Q}$" notation here is superfluous because any field automorphism $\sigma : K \to K$ automatically fixes $\mathbb{Q}$.

I claim that G is finite. Indeed, let $\sigma \in G$ and let r_i be any root of $f(x)$. Then we have

$$f(\sigma(r_i)) = \sigma(f(r_i)) = \sigma(0) = 0,$$

so that $\sigma(r_i) \in \mathbb{C}$ is another root. Thus σ defines a permutation of the set $\{r_1, \dots, r_n\}$. By abuse of notation we will also write $\sigma \in S_n$ for the permutation of $\{1, \dots, n\}$ defined by

$$\sigma(i) = j \iff \sigma(r_i) = r_j.$$

This defines a group homomorphism

$$\begin{array}{ccc} G & \longrightarrow & S_n \\ \sigma & \longmapsto & \sigma \end{array}.$$

Note that the homomorphism is injective since if σ fixes the roots then since $K = \mathbb{Q}(r_1, \cdots, r_n)$ is generated by the roots we conclude that $\sigma : K \to K$ is the identity automorphism.

We have now identified G with a subgroup of S_n, hence

$$|G| \leq |S_n| = n!.$$

[Remark: In Galois' original definition he explicitly thought of G as a group of permutations, which he called "substitutions". Even until Camille Jordan's "Traité des substitutions" (1870), all groups in mathematics were thought of as subgroups of S_n.]

Furthermore, it turns out that for all n there exist (many) polynomials $f(x) \in \mathbb{Q}[x]$ of degree n with

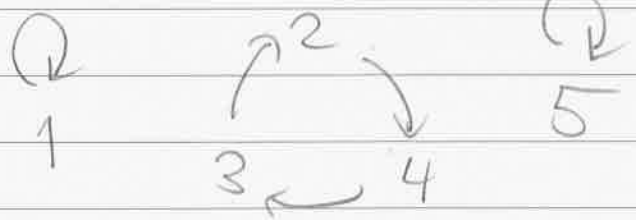
Galois group $G = S_n$.

Now, assuming the FTGT, we can prove the Abel-Ruffini Theorem by proving that for all $n \geq 5$, S_n is <u>not</u> a solvable group.

Recall the cycle notation for permutations. Let $c = (a_1 a_2 \cdots a_k) \in S_n$ be the permutation defined by

- $c(a_i) = a_{i+1 \bmod k}$
- $c(b) = b$ for $b \notin \{a_1, a_2, \cdots, a_k\}$.

For example, the permutation $(243) \in S_5$ has the following diagram:



Every permutation $\sigma \in S_n$ can be written uniquely as a product of commuting cycles

$$\sigma = c_1 c_2 \cdots c_m .$$

By convention, we will omit 1-cycles from the notation. This allows us to think of S_n as a subgroup of S_{n+1}.

The following Lemma is the foundation for the structure theory of S_n.

☆ Lemma: Let $c = (a_1 a_2 \cdots a_k) \in S_n$. Then for all $\pi \in S_n$ we have

$$\pi c \pi^{-1} = (\pi(a_1)\, \pi(a_2) \cdots \pi(a_k)) .$$

Proof: Since the group operation in S_n is composition of functions, we will read products from right to left.

Note that $\pi c \pi^{-1}$ acts on the element $\pi(a_i)$ by

$$\pi(a_i) \xrightarrow{\pi^{-1}} a_i \xrightarrow{c} a_{i+1 \bmod k} \xrightarrow{\pi} \pi(a_{i+1 \bmod k}),$$

and for $\pi(b) \notin \{\pi(a_1), \pi(a_2), \cdots, \pi(a_k)\}$ we have $b \notin \{a_1, a_2, \cdots, a_n\}$, hence

$$\pi c \pi^{-1}(\pi(b)) = \pi(c(b)) = \pi(b).$$

More generally, if $\sigma = c_1 c_2 \cdots c_m$ is a product of cycles then we have

$$\begin{aligned} \pi\sigma\pi^{-1} &= \pi c_1 c_2 \cdots c_m \pi^{-1} \\ &= (\pi c_1 \pi^{-1})(\pi c_2 \pi^{-1}) \cdots (\pi c_m \pi^{-1}), \end{aligned}$$

which is a product of cycles of the same lengths.

Notation: Given $\sigma \in S_n$, define

$$\cdot\, sh(\sigma) = (sh_1, sh_2, sh_3, \cdots)$$

where sh_k is the number of cycles of length k in the unique cycle decomposition of σ.

We call $sh(\sigma)$ the shape or the cycle-type of σ.

Now the above Lemma has the following corollary: $\forall\, \sigma, \pi \in S_n$ we have

$$sh(\pi\sigma\pi^{-1}) = sh(\sigma)$$

"Jordan canonical form"

In other words, conjugate permutations have the same shape. Conversely, it is not difficult to prove that permutations of the same shape are conjugate. Thus, conjugacy classes in S_n are parametrized by "valid shapes", i.e., decompositions of n as a sum of unordered positive integers.

[Remark: "Valid shapes" are more commonly called integer partitions. Let $p(n)$ be the number of partitions of n. Hardy & Ramanujan proved in 1918 that

$$p(n) \sim \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{2n/3}}.$$

]

Now we can prove the Abel-Ruffini Theorem.

✡ Theorem: For $n \geq 5$, S_n is not solvable.

Proof: Let $n \geq 5$ and assume that S_n is solvable, with composition series

$$S_n = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_m = 1.$$

Let $X \subseteq S_n$ be the set of 3-cycles. We will show that $X \subseteq G_i \Rightarrow X \subseteq G_{i+1}$, which implies by induction that $X \subseteq G_m = 1$. Contradiction.

So suppose that $X \subseteq G_i$. If $c_1, c_2 \in X$ then since G_i / G_{i+1} is abelian we have

$$(c_1 c_2 c_1^{-1} c_2^{-1}) G_{i+1}$$

$$= (c_1 G_{i+1})(c_2 G_{i+1})(c_1^{-1} G_{i+1})(c_2^{-1} G_{i+1})$$

$$= (c_1 G_{i+1})(c_2 G_{i+1})(c_1 G_{i+1})^{-1}(c_2 G_{i+1})^{-1}$$

$$= G_{i+1},$$

and hence $c_1 c_2 c_1^{-1} c_2^{-1} \in G_{i+1}$.

Now consider an arbitrary 3-cycle (ijk). Since $n \geq 5$, we can choose $l, m \notin \{i, j, k\}$ and then we have

$$(jkm)(ilj)(jkm)^{-1}(ilj)^{-1}$$

$$= (jkm)(ilj)(jmk)(ijl)$$

$$= (ijk)(l)(m) = (ijk).$$

We conclude that $(ijk) \in G_{i+1}$, and hence $X \subseteq G_{i+1}$, as desired.

QED

[Remark: It's sort of shocking that in the end the proof of the unsolvability of the quintic looks like <u>that</u>. Thank you Galois.]

↓

In fact, we can be more specific. It turns out that the alternating subgroup $A_n \subseteq S_n$ is simple, so the composition factors of S_n are

$$A_n \quad \& \quad \mathbb{Z}^\times = \{\pm 1\}.$$

Furthermore, the s.e.s. sequence

$$1 \longrightarrow A_n \longrightarrow S_n \xrightarrow{\text{sgn}} \mathbb{Z}^\times \longrightarrow 1$$

splits. Proof: Define $s: \mathbb{Z}^\times \to S_n$ by $s(-1) = (12)$ [or any 2-cycle]. Then we have $\text{sgn}(s(-1)) = \text{sgn}((12)) = -1$. ///

It follows that

$$S_n = A_n \rtimes \mathbb{Z}^\times.$$

[I (or you) will prove the simplicity of A_n after we have discussed group actions.]