MATH 25700: Honors Basic Algebra I

Hung Le

December 13, 2024

Course: MATH 25700: Honors Basic Algebra I

Professor: Daniil Rudenko

At: The University of Chicago

Quarter: Autumn 2024

Course materials: None.

This document will inevitably contain some mistakes, both simple typos and serious mathematical errors. I'd appreciate it if you could let me know at conghungletran@gmail.com if you find any. .

Contents

Lecture 1

Revision of the entire thing

10 Dec 2024

Definition 1.1 (Cyclic structure)**.** The **cyclic structure** of a permutation $\sigma \in S_n$ is

$$C(\sigma) = 1^{m_1} 2^{m_2} \dots n^{m_n}$$

where m_i is the number of cycles of length i in the cycle decomposition of σ.

Definition 1.2 (Conjugate)**.** $x, y \in G$ are **conjugate** iff there exists $g \in G$ such that $y = gxg^{-1}$. This is an equivalence relation, and the equivalence classes are called conjugacy classes.

Definition 1.3 (Inversion and Sign)**.** An **inversion** of $\sigma \in S_n$ is (i, j) such that $i < j, \sigma(i) > \sigma(j)$.sign : $S_n \to \{\pm 1\}$ is a homomorphism. $\text{sign}(\sigma) = 1$ iff the number of inversions is even.

Definition 1.4 (Group generators)**.** G is **generated** by $S = \{g_\alpha : \alpha \in I\}$ if for all $g \in G$,

$$g = g_{\alpha_1} \cdots g_{\alpha_n}$$

for $g_{\alpha_i} \in S$ or $g_{\alpha_i}^{-1} \in S$. Say that $G = \langle S \rangle$.

Theorem 1.5 (Types of cyclic groups)**.** Every cyclic group is $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$.

Definition 1.6 (Order of element)**.** The **order** of $g \in G$ is

$$ord(g) = |\langle g \rangle|.$$

Theorem 1.7 (Lagrange)**.** G finite group and $H \leq G$ then $|H|$ divides $|G|$.

Definition 1.8 (Coset equivalence)**.** Let $H \leq G$ then $g_1 \sim g_2 \Leftrightarrow {g_1}^{-1} g_2 \in H \Leftrightarrow g_1 H = g_2 H$. The equivalence classes under this equivalence relation are the **(left) cosets** of H in G. They are denoted $\{gH : g \in G\}$

Remark 1.9. The set of cosets $\{gH : g \in G\}$ doesn't necessarily form a group. H has to/should be normal for the group operation to be well-defined on the set of cosets.

Corollary 1.10. $|G| < \infty$ then $g^{|G|} = e$. Also, if $|G| = p$ then $G \cong \mathbb{Z}/p\mathbb{Z}$.

Definition 1.11 (Normal subgroup)**.** $N \leq G$ is **normal** if $\forall\, n \in N, g \in G$, we have

$$gng^{-1} \in N.$$

This is equivalent to that N is invariant under conjugation, i.e., $gNg^{-1} = N$ for all $g \in G$, or that it is a union of conjugacy classes, or that its left cosets and right cosets are the same, i.e., $gN = Ng$ for all $g \in G$.

We write $N \trianglelefteq G$.

We are then mostly concerned with non-trivial normal subgroups of a certain group, since $\{e\}$ and the entire group obviously satisfy the requirements.

Example 1.12. S_3 has conjugacy classes $\{\{e\}, \{(123), (132)\}, \{(12), (23), (13)\}\}$. $N \trianglelefteq G$ non-trivially has to have 2 or 3 elements. It also has to have e, so the only way is $N = \{e, (123), (132)\} = A_3$.

Example 1.13. S_4 has: 1 element of cyclic structure 1^4, $\binom{4}{2} = 6$ elements of structure $1^2 2^1$, $\binom{4}{3} \times 2 = 8$ elements of structure $1^1 3^1$, $\binom{4}{2}/2 = 3$ elements of structure 2^2, $3! = 6$ elements of structure 4^1 for a total of 24 elements.

$N \trianglelefteq G$ non-trivially therefore can only have $1+3$ or $1+3+8$ elements, corresponding to either $N = \{e, (12)(34), (13)(24), (14)(23)\} = V_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ the Klein 4-group (symmetries of a non-square rectangle), or $N = A_4$.

Definition 1.14 (Simple group). G is **simple** it has no non-trivial normal subgroup.

Proposition 1.15. $\varphi : G_1 \to G_2$ is a homomorphism, then $\ker(\varphi) \trianglelefteq G$.

Definition 1.16 (Quotient group). For $N \trianglelefteq G$, the **quotient group** G/N is the set of cosets (left or right, they are the same) of N with operation

$$g_1 N \cdot g_2 N = (g_1 g_2) N$$

which is only well-defined because

$$g_1 n_1 g_2 n_2 = g_1 g_2 ({g_2}^{-1} n_1 g_2 n_2) \in (g_1 g_2) N.$$

Definition 1.17 (Projection map). Let $N \trianglelefteq G$ then the projection map

$$\begin{aligned} \pi : G &\to G/N \\ g &\mapsto gN \end{aligned}$$

is a surjective homomorphism with $\ker(\pi) = N$.

Theorem 1.18 (Correspondence theorem). $N \trianglelefteq G$ then the projection map induces an order-preserving bijection between subgroups of G containing N and and subgroups of G/N.

Remark 1.19. If $N \trianglelefteq G$ and $N \leq H \leq G$ then clearly $N \trianglelefteq H$, and naturally $H/N \cong \pi(H)$. This is just an instance of the first isomorphism theorem too.

Theorem 1.20 (First isomorphism theorem). Let $f : G \to G$ homomorphism, then $G/\ker(f) \cong \operatorname{im}(f)$.

Definition 1.21 (Normalizer, centralizer, center). Let G be a group.

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

The **centralizer** of $x \in G$ is $C(x) = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\}$, i.e., things that commute with $x \in G$.

The **center** of G is $Z(G) = \{g \in G : gx = xg \ \forall\, x \in G\} = \{g \in G : gxg^{-1} = x \ \forall\, x \in G\}$, i.e., things that commute with everything in G. $Z(G) = \cap_{x \in G} C(x)$.

Proposition 1.22. A few facts on normalizer:

(1) $N_G(H) = G \Leftrightarrow H \trianglelefteq G$.

(2) $H \trianglelefteq N_G(H)$.

(3) This is a tautology, but $A \leq N_G(H)$ simply gives the information that H is invariant under conjugation by elements in A.

Proposition 1.23. A few facts on center:

(1) $Z(S_n) = \{e\} \ \forall\, n \geq 3, Z(GL_n(\mathbb{F})) = \mathbb{F}^\times$.

(2) $Z(G) \trianglelefteq G$ for all G. This is because $gzg^{-1} = z \ \forall\, g \in G$. So we get "free" normal subgroups this way.

(3) Similarly, $\langle z \rangle$ for any $z \in Z(G)$ is normal in G because $gz^k g^{-1} = z^k$.

(4) For $z \in Z(G)$, $Conj(z) = \{z\}$. For the same reason above.

Theorem 1.24 (Second isomorphism theorem). G group with $A, B \leq G$ with $A \leq N_G(B)$ (read: B is invariant under conjugation by elements in A). This is trivially satisfied if B is normal. Then AB is a subgroup of G, and $B \trianglelefteq AB$ and $(A \cap B) \trianglelefteq A$, and

$$A/(A \cap B) \cong (AB)/B$$

Remark 1.25. AB is a priori not guaranteed to be a subgroup (a product of 2 products of 2 things = a product of 4 things, so not necessarily a product of 2 things). The fact that $A \leq N_G(B)$ actually makes sure that this can be brought back to product of 2 things.

Theorem 1.26 (Third isomorphism theorem). $N \leq H \leq G$ and $N, H \trianglelefteq G$. Then $N \trianglelefteq H$ and

$$(G/N)/(H/N) \cong G/H$$

Remark 1.27. The summary of the 3 isomorphism theorems: Isom I talks about homomorphisms from a group to itself, and how ker can go undetected. Isom II talks about the interaction between 2 subgroups of G that are potentially intersecting, and how one can "eliminate" this intersection in different ways. Isom III talks about 3 groups of different "positions in the hierarchy" and how everything passes through nicely as expected.

Definition 1.28 (Action). G group, X any set. Then a **left action** of G on X is a map:

$$a : G \times X \to X$$
$$(g, x) \mapsto gx$$

such that $ex = x, g_1(g_2x) = (g_1g_2)x$. Naturally, for every $g \in G, a(g, \cdot)$ is a bijection $X \to X$.

Theorem 1.29. Let X have n elements. Then there is a bijection between actions of G on X and homomorphisms from $G \to S_n$.

Definition 1.30 (Orbit, stabilizer). We can consider equivalence relation on X where $x_1 \sim x_2 \Leftrightarrow \exists\, g \in G$ s.t. $x_1 = gx_2$, i.e., G can bring x_2 to x_1. Then the equivalence classes are **orbits**, denoted $Gx = \{gx : g \in G\}$.

The **stabilizer** of $x \in X$ is $G_x = \{g \in G : gx = x\}$, i.e., things in G that fixes x under the action. It is a subgroup of G.

Theorem 1.31 (Orbit-Stabilizer theorem). For a particular $x \in X$, there exists a bijection between left cosets $\{gG_x\}$ of G_x and the orbit Gx. A consequence is that

$$|G| = |Gx||G_x|.$$

So the order of the orbit (which is size of subset in X) divides $|G|$. The order of the stabilizer (size of subgroup of G) also divides $|G|$. This has first isomorphism/rank nullity vibes.

Example 1.32. Consider action: $G \times G \to G$ with left multiplication. This (induced) homomorphism was used in Cayley's theorem.

Example 1.33. Consider action: $G \times G \to G$ with conjugation. Then the stabilizer $G_x = C(x)$ is just the centralizer and orbit of x is just $G(x) = Conj(x)$ its conjugacy class. So it implies that $|C(x)| \cdot |Conj(x)| = |G|$.

Proposition 1.34 (Class equation). We get for general X that

$$|X| = \sum |Gx|$$

so

$$|X| = \#\text{ fixed points} + \text{non-trivial orbits}$$

and with G acting on G by conjugation we get

$$|G| = |Z(G)| + \sum |Conj(g)|$$

Theorem 1.35. $|G| = p^n$ with $n \geq 1$. Then G has a non-trivial center $Z(G)$.

Proof. By Orbit-Stabilizer, we have that $|Conj(x)| \mid |G| = p^n$, so $|Conj(x)| = p^{\geq 1}$ for things outside the center. So $p \mid |Z(G)|$ so $Z(G) \geq p \geq 2$. □

Theorem 1.36 (Cauchy's theorem). $|G| < \infty$ with $p \mid |G|$. Then G has an element of order p.

Proof. Consider $X = \{(g_1, \ldots, g_p) : g_1 \ldots g_p = e\}$ has $|G|^{p-1}$ elements. Then define an action $\mathbb{Z}/p\mathbb{Z} = \langle \sigma \rangle$ on X as $\sigma(g_1, \ldots, g_p) = (g_p, g_1, \ldots, g_{p-1})$.

So for any $x \in X$, the size of Gx has to divide p, so either 1 or p. So $|X| = n_1 + pn_p$, so $p \mid n_1$. An easy element with orbit 1 is $(e, e, \ldots, e)$, so there's another one $(g_1, \ldots, g_p) \neq (e, \ldots, e)$. But then that means $(g_1, \ldots, g_p) = \sigma(g_1, \ldots, g_p) = (g_p, \ldots, g_{p-1})$ so $g_1 = \cdots = g_p = g \neq e$. So we have that $g^p = g_1 \ldots g_p = e$. □

Definition 1.37 (Sylow subgroup)**.** Let G be a finite group with $G = p^k m$ with $(p, m) = 1$. A **p-Sylow subgroup** is $S \leq G$ with $|G| = p^k$.

Theorem 1.38 (Sylow I)**.** There exists a p-Sylow subgroup.

Proof. We prove by induction on G (not on k, m). Base case: $|G| = p^k$ for all p then satisfied by G itself.

Case 1: $p \mid |Z(G)|$. Then by Cauchy's theorem, there exists $g \in Z(G)$ such that $ord(g) = p$. Then $N = \langle g \rangle$ is normal in G and $|N| = p$.

It follows that $|G/N| = p^{k-1}m$. By induction, G/N has a p-Sylow subgroup K of size p^{k-1}. By correspondence theorem, $\pi^{Pre}(K) \leq G$ and $\pi^{Pre}(K)/N \cong K$ so $|\pi^{Pre}(K)| = p^{k-1}p = p^k$.

Case 2: $(p, |Z(G)|) = 1$. Then from the Class Equation

$$|G| = |Z(G)| + \sum |Conj(g)|$$

we get that there exists g with $p \nmid |Conj(g)| > 1$. But then $|C(g)||Conj(g)| = |G|$ so $C(g) = p^k m_1$ where $m_1 < m$. By induction, there exists some p-Sylow subgroup of $C(g)$, which is of size p^k and we're done. □

Remark 1.39. Virtue of the proof is as follows: If p divides the order of $Z(G)$ then we can find a normal subgroup of size p which we can quotient by, apply induction hypothesis, then project it back. If p doesn't, then by class equation that means some conjugacy class is also coprime with p. Apply Orbit-Stabilizer (or, Centralizer-Conjugacy Class), then the centralizer is good.

Theorem 1.40 (Sylow II)**.** All p-Sylow subgroups are conjugate.

Proof. $G = p^k m$. Let P, S be p-Sylow subgroups. Then P acts on the set of left cosets $\{g_1 S, \ldots, g_m S\}$ of S with left multiplication. By class equation, we get that

$$m = \#\text{ fixed points} + \text{ non-trivial orbits}$$

but then all orbit sizes have to divide $|P| = p^k$ so they are either 1 or p. So p divides size of all non-trivial orbits. So there's a fixed point because $(m, p) = 1$, say, gS.

So, $\forall\, h \in P, h(gS) = gS \Rightarrow h \in gSg^{-1} \Rightarrow P \subseteq gSg^{-1} \Rightarrow P = gSg^{-1}$. □

Remark 1.41. It's also clear that conjugates of p-Sylow subgroups are p-Sylow subgroups.

Corollary 1.42. Note that we didn't use that $P = p^k$ maximally, and only that P is a p-subgroup. So every p-subgroup of G is contained in some Sylow p-subgroup, i.e., $P \subseteq gSg^{-1}$.

Theorem 1.43 (Sylow III)**.** The number of p-Sylow subgroups n_p satisfies $n_p \mid m$ and $n_p \equiv 1 (\text{mod} p)$.

Proof. Consider $\mathcal{P}$ the set of all p-Sylow subgroups. Consider G acting on $\mathcal{P}$ by conjugation: $a_g : P \mapsto gPg^{-1}$.

By Sylow II, this action is transitive, i.e., there's only 1 orbit of size $|\mathcal{P}| = n_p$. And for a particular $P \in \mathcal{P}$, we have that the stabilizer of P under this action is just $N_G(P)$. Then Orbit-Stabilizer implies that $(G : N_G(P)) = n_p$.

But now we gotta make m pop out, so also note that $P \trianglelefteq N_G(P)$ almost by definition. So

$$(G : N_G(P))(N_G(P) : P) = (G : P) \Rightarrow n_p \mid (G : P) = m.$$

For the next part, consider P acting on $\mathcal{P}$ by conjugation. Let $(N_G(P) : P) = m'$ then $m' \mid m$ so $(m', p) = 1$, and $|N_G(P)| = p^k m'$.

The action is no longer transitive because $P \in \mathcal{P}$ is an obvious fixed point. We claim that it's the unique one.

Suppose that there's another fixed point $Q \in \mathcal{P}$, i.e., such that $\forall\, g \in P, gQg^{-1} = Q$. Then that implies $P \leq N_G(Q)$. But $Q \trianglelefteq N_G(Q)$ too, so they are both p-Sylow subgroups of $N_G(Q)$. But by Sylow II applied to $N_G(Q)$, it follows that P and Q are conjugate in $N_G(Q)$. But conjugate Q with anything in $N_G(Q)$ can only get us Q, so $P = Q$.

Therefore by class equation, $n_p = |\mathcal{P}| = 1 +$ other non-trivial orbits, where the size of non-trivial orbits divides $|P| = p^k$ so p divides them. So $n_p \equiv 1(\text{mod} p)$. □

Proposition 1.44. The only abelian simple groups are $\mathbb{Z}/p\mathbb{Z}$.

Proof. Suppose not. There exists some $p \mid |G| \neq p$. By Cauchy's theorem, there exists $g \in G$ such that $ord(g) = p$. Since it's abelian, $\langle x \rangle \trianglelefteq G$. □

Theorem 1.45 (The big one). If G non-abelian and simple with order ≤ 60 then $G \cong A_5$.

Theorem 1.46. The only normal subgroups of S_n for $n \geq 5$ are $\{e\}, S_n$ and A_n.

Theorem 1.47. A_n is simple for $n \geq 5$.

Remark 1.48. The second theorem is not a corollary of the first theorem. Even if A_n did have a normal subgroup, it does not mean that that subgroup would've been normal in S_n.

Proof (for Theorem 1.47)**.** We've had a proof for the theorem using 3-cycles in pset 6. Here we present a different one specifically for A_5.

The conjugacy classes in S_5 are:

- 5 with $4! = 24$ elements.
- $4 + 1$ with $5 \times 3! = 30$ elements.
- $3 + 1 + 1$ with $10 \times 2! = 20$ elements.
- $2 + 1 + 1 + 1$ with 10 elements.
- $3 + 2$ with $10 \times 2 = 20$ elements.
- $2 + 2 + 1$ with 15 elements.
- $1 + 1 + 1 + 1 + 1$ with 1 element.

and the even ones are 5, $3 + 1 + 1$, $2 + 2 + 1$ and $1 + 1 + 1 + 1 + 1$ for total of $24 + 20 + 15 + 1 = 60$ elements.

The essential idea is that the conjugacy classes of A_5 (which are just permutations) are simply formed by "splitting off" from the conjugacy classes of S_5 (well, they have to have the same cycle structure). Why they might be different is that the orbits under conjugation in A_5 might be smaller compared to S_5, resulting in multiple conjugacy classes within 1 conjugacy class in S_5.

Lemma. Let $Conj(g)$ be a conjugacy class in S_5. Then it is the union of either 1 or 2 conjugacy classes of the same size in A_5.

Proof of Lemma. Let $Conj(g)$ be a conjugacy class in S_5. Let $Conj'(h)$ denote the conjugacy class of h in A_5. Then if $h \in Conj(g)$ then $Conj'(h) \subseteq Conj(g)$ too because they all have the same cycle structure.

So let $X = \{Conj'(h_1), \ldots, Conj'(h_m)\}$ be the set of conjugacy classes of A_5 in $Conj(g)$. Then consider the action S_5 on X by conjugation. Since they are all in $Conj(g)$, it follows that the action is transitive (well, they're all conjugate in S_5), so there's only 1 orbit of size m.

Consider the stabilizer $S(Conj'(h_i)) \leq S_5$ for any i. Then since $Conj'(h_i)$ is a conjugacy class in A_5, conjugation by A_5 fixes $Conj'(h_i)$, i.e., $A_5 \subseteq S(Conj'(h_i))$.

Therefore it follows that $A_5 \leq S(Conj'(h_i)) \leq S_5$, so either $S(Conj'(h_i)) = S_5$ or A_5. If $S(Conj'(h_i)) = S_5$ then that means the orbit size is $m = |S_5|/|S(Conj'(h_i))| = 1$. So $Conj(g) = Conj(h_1)$ is the entire conjugacy class in A_5.

Otherwise, if $S(Conj'(h_i)) = A_5$ then that means the orbit size is $m = 2$ with $Conj'(h_1) \cup Conj'(h_2) = Conj(g)$. However, since $h_1, h_2 \in Conj(g)$, it follows that there exists $\sigma \in S_5$ such that $h_1 = \sigma h_2 \sigma^{-1}$, so $ah_1a^{-1} \mapsto (\sigma a \sigma^{-1})(\sigma h_1 \sigma^{-1})(\sigma a^{-1} \sigma^{-1})$ the conjugation by $(\sigma a \sigma^{-1}) \in A_5$, is a bijection between $Conj'(h_1)$ and $Conj'(h_2)$ so they are of the same size. And we're done with the lemma.

Back to main proof. We can reach some conclusions:

- $Conj((*****))$ has size 24 which doesn't divide 60, so the 5-cycles split into 2 conjugacy classes in A_5.
- $Conj((**)(**))$ has size 15 which is odd, so it's kept as 1 conjugacy class in A_5.

so the only undetermined thing is whether $Conj((***))$ breaks into 2 or not. But that doesn't matter because A_5 is either decomposed as $1+12+12+15+20$ or $1+12+12+15+10+10$ — either way — we can't make a non-trivial normal subgroup out of any union of conjugacy classes. □

Proof (for Theorem 1.46). Let $N \trianglelefteq S_n$ with $n \geq 5$ but $N \neq \{e\}, A_n, S_n$.

Then (similar to Second Isomorphism) we get that $A_n \cap N \trianglelefteq A_n$ since A_n is in the normalizer of N, i.e., S_n. But A_n is simple for all $n \geq 5$, so either $A_n \cap N = A_n$ which implies $A_n \leq N \leq S_n$ which implies $N = A_n$ or $N = S_n$; or $A_n \cap N = \{e\}$ which implies $A_n/(N \cap A_n) \cong A_nN/N$ by Second Isomorphism, which implies A_nN/N of size $|A_n|$. We have that $A_n \leq A_nN \leq S_n$ so either $A_nN = A_n$ or $A_nN = S_n$. If $A_nN = A_n$ then that means $|N| = 1$ which is a contradiction. If $A_nN = S_n$ then that means $|N| = 2$, so $N = \{e, n\}$. N is normal in S_n which means $\sigma n \sigma^{-1} \in N$, in particular it can't be e, so $\sigma n \sigma^{-1} = n \Rightarrow n \in Z(S_n)$.

But $Z(S_n) = \{e\}$ for all $n \geq 3$, so a contradiction. □

Remark 1.49. S_3 has conjugacy classes $(***) = 2, (**) = 3, e = 1$ so the only non-trivial normal subgroup is $\{e, (***)\} = A_3$.

Remark 1.50. S_4 has conjugacy classes $(****) = 6, (***) = 8, (**) = 6, (**)(**) = 3, e = 1$. So the only non-trivial normal subgroups of S_4 are $1+3$ being $\{(**)(**), e\} = V_4$ and $1+3+8$ being $\{e, (***), (**)(**)\} = A_4$.

Definition 1.51. We have that $GL_n(\mathbb{F})$ is the group of $n \times n$ invertible matrices with entries in $\mathbb{F}$. Define $PGL_n(\mathbb{F}) = GL_n(\mathbb{F})/Z(GL_n(\mathbb{F})) = GL_n(\mathbb{F})/\lambda I$ up to scaling of all entries. $SL_n(\mathbb{F})$ is the group of $n \times n$ invertible matrices with determinant 1. Similarly define $PSL_n(\mathbb{F})$.

Remark 1.52. Let's count for $\mathbb{F} = \mathbb{F}_p$ and $n = 2$. Then size of $GL_2(\mathbb{F}_p)$ is $(p^2-1)(p^2-p) = (p-1)^2p(p+1)$. Size of $PGL_2(\mathbb{F}_p)$ is $(p-1)^2p(p+1)/(p-1) = (p-1)p(p+1)$. Size of $SL_2(\mathbb{F}_p)$ is the same (kernel of determinant map). Size of $PSL_2(\mathbb{F}_p)$ is half of that.

Though $PGL_2(\mathbb{F}_p)$ and $SL_2(\mathbb{F}_p)$ have the same number of elements, the fact that we have $PSL_2(\mathbb{F}_p)$ already indicates their difference. $Z(SL_2(\mathbb{F}_p)) = \{\pm I\}$ while $Z(PGL_2(\mathbb{F}_p))$ is trivial for $p \geq 5$.

Definition 1.53. Let V be a vector space over $\mathbb{F}$, then the projective space $P(V)$ is the set of lines (1-dimensional subspaces) of V. Denote $P(\mathbb{F}^n) = P^{n-1}_{\mathbb{F}}$.

In particular, we use homogeneous coordinates for $P^{n-1}_{\mathbb{F}} = \{[x_1 : x_2 : \cdots : x_n] : \text{not all zeros}\}$. For $P^1_{\mathbb{F}} = P(\mathbb{F}^2)$ we get that the lines are $\{[x:1] : x \in \mathbb{F}\} \cup \{[1:0]\} = \mathbb{F} \cup \{\infty\}$.

Then the action $GL_n(\mathbb{F})$ on $\mathbb{F}^n$ induces (just matrix multiplication) an action $PGL_n(\mathbb{F})$ on $P^{n-1}_{\mathbb{F}}$.

Definition 1.54 (General position). $p_1, \ldots, p_n \in P^{n-1}_{\mathbb{F}}$ are in general position if they span $\mathbb{F}_n$.

Theorem 1.55. Consider points $p_1, \ldots, p_{n+1}$ in $P^{n-1}_{\mathbb{F}}$ such that any n are in general position. Similarly $q_1, \ldots, q_{n+1}$. Then there exists uniquely $f \in PGL_n(\mathbb{F})$ such that $f(p_i) = q_i$.

Corollary 1.56. Applying this to $P^1_{\mathbb{F}}$ then given any 3 points in $P^1_{\mathbb{F}}$, and any other 3 points in $P^{\mathbb{F}}_1$, there exists uniquely $f \in PGL_2(\mathbb{F})$ that move them around. It's often helpful to just base everything in moving to/from $\{[0:1], [1:1], [1:0]\} = \{0, 1, \infty\}$.

Definition 1.57 (k-transitive)**.** An action of G on X is **k-transitive** if any k points in X can be moved to any other k points using some $g \in G$. It is **sharply k-transitive** if such g is unique.

Then the action of $PGL_2(\mathbb{F})$ on $P^1_{\mathbb{F}}$ is sharply 3-transitive.

Theorem 1.58. $PGL_2(\mathbb{F}_5) \cong S_5$.

Proof. Consider the action of $PGL_2(\mathbb{F}_5)$ on the projective space $P(\mathbb{F}_5^2) = P^1_{\mathbb{F}_5}$ of six points (projective lines). This induces a homomorphism:

$$\psi : PGL_2(\mathbb{F}_5) \to S_6$$

$A \in \ker(\psi)$ fixes all 6 points. Since $PGL_2(\mathbb{F}_5)$ is sharply 3-transitive, $A = I$ uniquely. So ψ is injective. So we have $H = \text{im}(\psi) \leq S_6$ is a subgroup of index $\frac{6!}{(5^2-1)(5^2-5)/4} = 720/120 = 6$.

Lemma. (Pretty generic) If $H \leq S_n$ of index n then $H \cong S_{n-1}$ for $n \geq 5$. In particular, if $H \leq S_6$ of index 6 then $H \cong S_5$.

Proof of lemma. We prove for $n = 6$ and easily generalizable. Consider the action of H on the cosets $\{H, g_2H, \dots, g_6H\}$ by left multiplication. Then an obvious fixed point is H. So this action induces a homomorphism:

$$\varphi : H \to S_5$$

$|H| = |S_5| = 120$ so it remains to show that $\ker(\varphi) = \{e\}$. We get that

$$\ker(\varphi) = \{h \in H : \forall\, g \in S_6, hgH = gH\} = \bigcap_{g \in S_6} gHg^{-1}$$

but it is easy to see that it is normal in S_6. But the only normal subgroups of S_6 are $\{e\}, A_6, S_6$. And $\ker(\varphi)$ has size ≤ 120, so it has to be that $\ker(\varphi) = \{e\}$. ☐

Proposition 1.59. Some facts from HW:

(1) $H \leq G$ finite. If $(G : H) = 2$ then H is normal. $(G : H) = 3$ then not necessarily.

(2) For $n \neq 6$, any automorphism of S_n is given by conjugation.

(3) Let $k \leq n$ be even. Then every element in S_n can be written as a product of k-cycles.

(4) If G is a p-group and $H \subset G$ has index p then it is normal in G. Proof by considering action of G on set of p cosets of H by left multiplication.

Proposition 1.60. $PSL_2(\mathbb{F}_5) \cong A_5$.

Proof. We know that $PGL_2(\mathbb{F}_5) \cong S_5$. $PSL_2(\mathbb{F}_5)$ is of index 2 in $PGL_2(\mathbb{F}_5)$, so it is normal. The only normal subgroups of S_5 are $\{e\}, A_5, S_5$. So $PSL_2(\mathbb{F}_5) \cong A_5$. ☐

Proposition 1.61. Groups of order p^n are not simple for $n \geq 2$.

Proof. Let G have p^n elements. By the class equation we get that

$$p^n = |Z(G)| + \sum |Conj(g)|$$

And we know that the sizes have to be the form p^*. So $|Z(G)| \geq p \geq 2$. Furthermore, $Z(G) \neq G$ because if so then G is abelian – but the only abelian simple groups are $\mathbb{Z}/p\mathbb{Z}$. It follows that $Z(G)$ is a non-trivial normal subgroup of G, so G is not simple. ☐

Theorem 1.62 (Simple group of order 60)**.** If G is of order 60 and G is simple then $G \cong A_5$.

Proof. $60 = 2^2 \times 3 \times 5$. Easy to see from Sylow III + too few Sylow p-subgroups that $n_3 = 10, n_5 = 6$. Only indecision is if $n_2 = 5$ or $n_2 = 15$.

Case 1: If $n_2 = 5$ we get that the transitive action of G on the set of 2−Sylow subgroups by conjugation induces a homomorphism

$$\psi : G \to S_5$$

Clearly $\ker(\psi) = \{e\}$.

Compose with sign then we get homomorphism

$$\text{sign} \circ \psi : G \to \{\pm 1\}$$

and $\ker(\text{sign} \circ \psi)$ can't be $\{e\}$ (size) so has to be G, so has to be all even permutations.

Case 2: If $n_2 = 15$ then we gotta do some counting. There are 20 elements of order 3 and 24 elements of order 5. So there are 16 left. If all 2-Sylow subgroups (each of size 4) have trivial intersection then there are too many elements. So there exists S_1, S_2 that are 2-Sylow subgroups such that $|S_1 \cap S_2| = 2$.

Note that S_1, S_2 of order 4 so abelian, so if we consider $N = N_G(S_1 \cap S_2)$ then $S_1, S_2 \leq N_G(S_1 \cap S_2)$. So size of normalizer is at least 6, and divisible by 4. It also has to divide 60. So either $4 \times 3 = 12$ or $4 \times 5 = 20$.

If N of size 20 then G acts on G/N of size 3 by left multiplication. Too small.

If N of size 12 then G acts on G/N of size 5 by left multiplication. Again we have a homomorphism to S_5, and by the same argument A_5. □

Definition 1.63 (Composition series)**.** For any G finite group, there exists a composition series:

$$\{e\} = G_0 \trianglelefteq G_1 \cdots \trianglelefteq G_n = G$$

where the relations are strict and all G_k/G_{k-1} are simple. Moreover, the sequence of quotient groups is unique up to permutation. In particular, the length of the maximal chain is unique/well-defined.

Proposition 1.64. Some claims on groups of order not being simple. Overarching idea is that G acting on $\mathcal{P}$ set of p-Sylow subgroups by conjugation induces homomorphism $\psi : G \to S_{n_p}$. If $n_p > 1$ (the interesting case), we know that this homomorphism is not trivial (i.e., not everything is sent to *id* because by Sylow II all p-Sylow subgroups are conjugate). So $\ker(\psi) \neq G$. So has to be $\ker(\psi) = \{e\}$. So $|G| \leq |S_{n_p}| = n_p!$ which causes trouble when n_p is too small.

Let $p < q < r$ here

(1) p^n not simple as above

(2) pq has $n_q = 1$. In fact any pq^*.

(3) p^2q has $n_q = p^2 \equiv 1 \bmod p$ implies $p = 2, q = 3$. So 12. But $n_2 = 3$ too few.

(4) p^2q^2 has $p = 2, q = 3$ but so 36 but $n_q = 4$ too few.

(5) p^3q. If $n_q = p^2$ then same as above. If $n_q = p^3$ then $p^3(q-1)$ elements of order q. so only p^3 elements left, and that's the only p-Sylow subgroup left. But then $n_p = 1$.

(6) p^4q argument seems to only work for below 60. Then $p = 2, q = 3$ and whatever.

(7) $2 \times 3 \times 5$ or $2 \times 3 \times 7$. Either count elements or too few Sylow subgroups.