Math 322: Introduction to Group Theory
Lecture Notes

Lior Silberman

These are rough notes for the Fall 2015 course. Solutions to problem sets were posted on an internal website.

Contents

Introduction

Lior Silberman, lior@Math.UBC.CA, http://www.math.ubc.ca/~lior
Office: Math Building 229B
Phone: 604-827-3031

0.1. Administrivia

- Problem sets will be posted on the course website.
  - To the extent I have time, solutions may be posted on Connect.
- Textbooks
  - Rotman
  - Dummit and Foote
  - Algebra books
- There will be a midterm and a final. For more details see syllabus.
  - Policies, grade breakdown also there.

0.2. Motivation

Coxeter came to Cambridge and he gave a lecture, then he had this problem ... I left the lecture room thinking. As I was walking through Cambridge, suddenly the idea hit me, but it hit me while I was in the middle of the road. When the idea hit me I stopped and a large truck ran into me ... So I pretended that Coxeter had calculated the difficulty of this problem so precisely that he knew that I would get the solution just in the middle of the road ... One consequence of it is that in a group if $a^2 = b^3 = c^5 = (abc)^{-1}$, then $c^{610} = 1$.

J.H. Conway, Math. Intelligencer v. 23 no. 2 (2001)

- Groups = Symmetry (see slides)
  - In geometry
  - In physics
  - Combinatorially
  - In mathematics
- Course also (mainly?) about formal mathematics.

0.3. Course plan (subject to revision) (Lecture 1, 10/9/2015)

- Examples / Calculation: $\mathbb{Z}$,S_n, $\mathrm{GL}_n(\mathbb{R})$.
- Basics
  - Groups and homomorphisms.
  - Subgroups; Cosets and Lagrange's Theorem.
  - Normal subgroups and quotients.
  - Isomorphism Theorems
  - Direct and semidirect products
- Group Actions
  - Conjugation; class formula
  - Symmetric groups; Simplicity of A_n
  - Group actions
- Sylow Theorems
  - p-Groups
  - Sylow Theorems
  - Groups of small order
- Finitely Generated abelian groups.
- Free groups; Generators and relations.
- Other topics if time permits.

CHAPTER 1

Some explicit groups

1.1. $\mathbb{Z}$

FACT 1 (Properties of the Integers). *Integers can be added, multiplied, and compared.*

0. *The usual laws or arithmetic hold.*
(1) *$<$ is a linear order, and it respects addition and multiplication by positive numbers.*
(2) *(Well-ordering) If $A \subset \mathbb{Z}$ is bounded below, it contains a least element. 1 is the least positive integer.*

EXERCISE 2. Every positive integer is of the form $1+1+\cdots+1$ (hint: consider the least positive integer not of this form and subtract 1).

We first examine the additive structure, and then the multiplicative structure.

LEMMA 3. *Well-ordering is equivalent to the principle of induction (if $A \subset \mathbb{Z}$ has $0 \in A$ and $(n \in A \Rightarrow (n+1) \in A)$ then $\mathbb{N} \subset A$.*

PROOF ($\Rightarrow$). Let $A \subset \mathbb{Z}$ satisfy $0 \in A$ and $(n \in A \Rightarrow (n+1) \in A)$. Let $B = \mathbb{N} \setminus A$. Suppose B is non-empty; then by the well-ordering principle there is $c = \min B$. □

1.1.1. The group $(\mathbb{Z}, +)$. We note the following properties of addition: for all $x, y, z \in \mathbb{Z}$

- Associativity: $(x+y)+z = x+(y+z)$
- Zero: $0+x = x+0 = x$
- Inverse: there is $(-x) \in \mathbb{Z}$ such that $x+(-x) = (-x)+x = 0$.
- Commutativity: $x+y = y+x$.

PROBLEM 4. Which subsets of $\mathbb{Z}$ are closed under addition and inverses? (analogues of "subspaces" of a vector space)

EXAMPLE 5. $\{0\}$, all even integers. What else?

LEMMA 6 (Division with remainder). *Let $a, b \in \mathbb{Z}$with $a > 0$. Then there are unique q, r with $0 \le r < a$ such that*

$$b = qa + r .$$

PROOF. (Existence) Given b, a let A be the set of all positive integers c such that $c = b - qa$ for some $q \in \mathbb{Z}$. This is non-empty (for example, $b - (-(|b|+1))a \ge a + |b|(a-1) \ge 0$), and hence has a least element r, say $r = b - qa$. If $r \ge a$ then $0 \le r - a < r$ and $r - a = b - (q+1)a$, a contradiction.

(Uniqueness) Suppose that there are two solutions so that

$$b = qa + r = q'a + r' .$$

We then have

$$r - r' = a\left(q' - q\right) .$$

If $r = r'$ then since $a \neq 0$ we must have $q = q'$. Otherwise wlog $r > r'$ and then $q' > q$ so $q' - q \geq 1$ and $r - r' \geq a$, which is impossible since $r - r' \leq r \leq a - 1$. □

PROPOSITION 7. *Let $H \subset \mathbb{Z}$ be closed under addition and inverses. Then either $H = \{0\}$ or there is $a \in \mathbb{Z}_{>0}$ such that $H = \{xa \mid x \in \mathbb{Z}\}$. In that case a is the least positive member of H.*

PROOF. Suppose H contains a non-zero element. Since it is closed under inverses, it contains a positive member. Let a be the least positive member, and let $b \in H$. Then there are q, r such that $b = qa + r$. Then $r = b - qa \in H$ (repeatedly add a or $(-a)$ to b). But $r < a$, so we must have $r = 0$ and $b = qa$. □

OBSERVATION 8. *To check if b was divisible by a we divide anyway and examine the remainder.*

Review of Lecture 1: two key techniques.

(1) To prove something by induction, consider the "least counterexample", use the truth of the proposition below that to get a contrdiction.
(2) To check if $a|b$ divide b by a and examine the remainder.

1.1.2. Multiplicative structure (Lecture 2, 15/9/2015).

DEFINITION 9. Let $a, b \in \mathbb{Z}$. Say "*a divides b*" and write $a|b$ if there is c such that $b = ac$. Write $a \nmid b$ otherwise.

EXAMPLE 10. ± 1 divide every integer. Only ± 1 divide ± 1. Every integer divides 0, but only 0 divides 0. $2|14$ but $3 \nmid 14$. $|a|$ divides a.

THEOREM 11 (Bezout). *Let $a, b \in \mathbb{Z}$ not be both zero, and let d be the greatest common divisor of a, b (that is, the greatest integer that divides both of them). Then there are $x, y \in \mathbb{Z}$ such that $d = ax + by$, and every common divisor of a, b divides d.*

PROOF. Let $H = \{ax + by \mid x, y \in \mathbb{Z}\}$. Then H is closed under addition and inverses and contains a, b hence is not $\{0\}$. By Proposition 7 there is $d \in \mathbb{Z}_{>0}$ such that $H = \mathbb{Z}d$. Since $a, b \in H$ it follows that $d|a$, $d|b$ so d is a common divisor. Conversely, let x, y be such that $d = ax + by$ and let e be another common divisor. then $e|a, e|b$ so $e|ax, e|by$ so $e|ax + by = d$. In particular, $e \leq d$ so d is the *greatest* common divisor. □

ALGORITHM 12 (Euclid). *Given a, b set a_0, a_1be $|a|, |b|$ in decreasing order. Then $a_0, a_1 \in H$. Given $a_{n-1} \geq a_n > 0$ divide $a_{n-1}$by a_n, getting:*

$$a_{n-1} = q_n a_n + r_n \,.$$

Then $r_n = a_{n-1} - q_n a_n \in H$ (closed under addition!) and we can set set $a_{n+1} = r_n < a_n$. The sequence a_n is strictly decreasing, so eventually we get $a_{n+1} = 0$.

CLAIM 13. When $a_{n+1} = 0$ we have$a_n = \gcd(a, b)$.

PROOF. Let $e = a_n$. Since $a_n \in H$ we have $\gcd(a, b)|e$. We have $e|a_n$ (equal) and $e|a_{n-1}$ (remainder was zero!). Since $a_{n-2} = q_{n-1}a_{n-1} + a_n$ we see $e|a_{n-2}$. Continuing backwards we see that $e|a_0, a_1$so $e|a, b$. It follows that e is a common divisor $e|\gcd(a, b)$ and we conclude they are equal. □

REMARK 14. It is also not hard to show (exercise!) that $\gcd(a_{n-1}, a_n) = \gcd(a_n, a_{n+1})$. It follows by induction that this is $\gcd(a, b)$, and we get a different proof that the algorithm works, and hence of Bezout's Theorem.

EXAMPLE 15. $(69,51) = (51,18) = (18,15) = (15,3) = (3,0) = (3)$. In fact, we also find $18 = 69-51$, $15 = 51-2\cdot 18 = 3\cdot 51 - 2\cdot 69$, $3 = 18-15 = 3\cdot 69 - 4\cdot 51$.

1.1.3. Modular arithmetic and $\mathbb{Z}/n\mathbb{Z}$.

- Motivation: (1) New groups (2) quotient construction.

DEFINITION 16. Let $a,b,n \in \mathbb{Z}$ with $n \geq 1$. Say *a is congruent to b modulu n*, and wite $a \equiv b\ (n)$ if $n|b-a$.

LEMMA 17. *This is an equivalence relation.*

- Aside: Equivalence relations
  - Notion of equivalence relation.
  - Equivalence classes, show that they partition the set,

LEMMA 18. *Suppose $a \equiv a'$, $b \equiv b'$. Then $a+b \equiv a'+b'$, $ab \equiv a'b'$.*

PROOF. $(a'+b') - (a+b) = (a'-a) + (b'-b)$; $a'b' - ab = (a'-a)b' + a(b'-b)$. □

- Aside: quotient by equivalence relations
  - Set of equivalence classes

DEFINITION 19. Let $\mathbb{Z}/n\mathbb{Z}$ denote the quotient of $\mathbb{Z}$ by the equivalence relation $\equiv (n)$. Define on it arithmetic operations by

$$[a]_n \pm [b]_n \stackrel{\text{def}}{=} [a+b]_n\ ,$$
$$[a]_n \cdot [b_n] \stackrel{\text{def}}{=} [ab]_n\ .$$

OBSERVATION 20. *Then laws of arithmetic from $\mathbb{Z}$ still hold. Proof: they work for the representatives.*

- Warning: actually needed to check that the operations were well-defined. That's the Lemma.
- Get additive group $(\mathbb{Z}/n\mathbb{Z},+)$.
- Note the "quotient" homomorphism $(\mathbb{Z},+) \to (\mathbb{Z}/n\mathbb{Z},+)$.

1.1.4. The multiplicative group (Lecture 3, 11/9/2015). Let $(\mathbb{Z}/n\mathbb{Z})^{\times} = \{a \in \mathbb{Z}/n\mathbb{Z} \mid (a,n) = 1\}$.

LEMMA 21. *$(\mathbb{Z}/n\mathbb{Z})^{\times}$ is closed under multiplication and inverses.*

PROOF. Suppose $ax+ny = 1$, $bz+nw = 1$. multiplying we find

$$(ab)(xz) + n(axw + ybz + nyw) = 1$$

so $(ab,n) = 1$. For inverses see PS1. □

REMARK 22. Why exclude the ones not relatively prime? These can't have *inverse*s.

DEFINITION 23. This is called the *multiplicative group* mod n.

- Addition tables.
- Multiplication tables.
- Compare $(\mathbb{Z}/2\mathbb{Z},+)$, $(\mathbb{Z}/3\mathbb{Z})^{\times}$, $(\mathbb{Z}/4\mathbb{Z})^{\times}$.
- Compare $(\mathbb{Z}/4\mathbb{Z},+)$, $(\mathbb{Z}/5\mathbb{Z})^{\times}$ but $(\mathbb{Z}/8\mathbb{Z})^{\times}$.

REMARK 24. In general, $(\mathbb{Z}/p\mathbb{Z})^{\times} \simeq (\mathbb{Z}/(p-1)\mathbb{Z},+)$ – but the isomorphism is *computationally hard* (relevant hardness of discrete log hence cryptography).

DEFINITION 25. *Euler's totient function* is the function $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^{\times}$.

LEMMA 26. $\sum_{d|n}\phi(n) = n$.

PROOF. For each $d|n$ let $A_d = \{0 \le a < n \mid \gcd(a,n) = d\}$. Then $\left\{\frac{a}{d} \mid a \in A_d\right\} = \left\{0 \le b < \frac{n}{d} \mid \gcd(b,\frac{n}{d}) = 1\right\}$ In particular, $\#A_d = \phi\left(\frac{n}{d}\right)$. □

1.1.5. Primes and unique factorization.

DEFINITION 27. Call *p prime* if it has no divisors except 1 and itself.

Note that p is prime iff $(\mathbb{Z}/p\mathbb{Z})^{\times} = \left\{\bar{1},\cdots,\overline{p-1}\right\}$.

COROLLARY 28. *$p|ab$ iff $p|a$ or $p|b$.*

PROOF. Suppose $p \nmid a$ and $p \nmid b$. Then $[a]_p, [b]_p$ are relatively prime to p hence invertible, say with inverses a', b'. Then $(ab)(a'b') \equiv (aa')(bb') \equiv 1\cdot 1 \equiv 1\,(p)$ so ab is invertible mod p hence not divisible by p. □

THEOREM 29 (Unique factorization). *Every non-zero integer can be uniquely written in the form $\varepsilon\prod_{p\ prime} p^{e_p}$ where $\varepsilon \in \{\pm 1\}$ and almost all $e_p = 0$.*

PROOF. Supplement to PS2. □

1.1.6. The Chinese Remainder Theorem. We start with our second example of a non-trivial homomorphism.

Let $n_1|N$. Then the map $[a]_N \mapsto [a]_{n_1}$ respects modular addition and multiplication (pf: take representatives in $\mathbb{Z}$). Now suppose that $n_1,n_2|n$ and consider the map

$$[a]_N \mapsto \left([a]_{n_1}, [a]_{n_2}\right).$$

This also respects addition and multiplication (was OK in every coordinate).

DEFINITION 30. Call *n,m relatively prime* if $\gcd(n,m) = 1$.

Next comes our first non-trivial isomorphism.

THEOREM 31 (Chinese Remainder Theorem). *Let $N = n_1n_2$ with n_1,n_2 relatively prime. Then the map*

$$f\colon \mathbb{Z}/N\mathbb{Z} \to (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z})$$

constructed above is a bijection which respect addition and multiplication (that is, an isomorphism of the respective algebraic structures).

PROOF. For surjectivity, let x,y be such that

$$n_1x_1 + n_2y = 1.$$

Let $b_1 = n_2y$ and let $b_2 = n_1x$. Then:

$$\begin{aligned} f([b_1]_N) &= ([1]_{n_1},[0]_{n_2}) \\ f([b_2]_N) &= ([0]_{n_1},[1]_{n_2}). \end{aligned}$$

It follows that $\{b_1, b_2\}$ is a "basis" for this product structure: for any a_1, a_2 mod n_1, n_2 respectively we have

$$\begin{aligned} f\left([a_1b_1 + a_2b_2]_N\right) &= \left([a_1]_{n_1} \cdot [1]_{n_1}, [a_1]_{n_2} \cdot [0]_{n_2}\right) + \left([a_2]_{n_1} \cdot [0]_{n_1}, [a_2]_{n_2} \cdot [1]_{n_2}\right) \\ &= \left([a_1]_{n_1}, [0]_{n_2}\right) + \left([0]_{n_1}, [a_2]_{n_2}\right) = \left([a_1]_{n_1}, [a_2]_{n_2}\right) . \end{aligned}$$

Injectivity now following from the pigeon-hole principle (supplement to PS2). □

REMARK 32. Meditate on this. Probably first example of a non-obvious isomorphism, and a non-obvious "basis".

1.2. S_n (Lecture 4, 22/9/2015)

1.2.1. Permutations: concerete and abstract.

DEFINITION 33. Let X be a set. A *permutation* on X is a bijection $\sigma\colon X \to X$ (a function which is $1:1$ and onto). The set of all permutations will be denoted S_X and called the *symmetric group*.

Recall that the *composition* of functions $f\colon Y \to Z$ and $g\colon X \to Y$ is the function $f \circ g\colon X \to Z$ given by $(f \circ g)(x) = f(g(x))$.

LEMMA 34. *Composition of functions is associative. The identity function* $\mathrm{id}_X : X \to X$ *belongs to the symmetric group and is an identity for composition.*

EXAMPLE 35. $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$. The identity map. Non-example $\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$.

LEMMA 36. *Let* $\sigma\colon X \to X$ *be a function.*

(1) $\sigma\colon X \to X$ *is a bijection iff there is a "compositional inverse"* $\bar{\sigma}\colon X \to X$ *such that* $\sigma \circ \bar{\sigma} = \bar{\sigma} \circ \sigma = \mathrm{id}$.
(2) S_X *is closed under composition and compositional inverse.*
(3) Suppose $\sigma \in S_X$ *and that* $\sigma\tau = \mathrm{id}$ *or that* $\tau\sigma = \mathrm{id}$. *Then* $\tau = \bar{\sigma}$. *In particular, the compositional inverse is* unique *and will be denoted* σ^{-1}.
(4) $(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$.

PROOF. (2) Suppose $\sigma, \tau \in S_X$ and let $\bar{\sigma}, \bar{\tau}$ be as in (1). Then σ satisfies $\sigma \circ \bar{\sigma} = \bar{\sigma} \circ \sigma = \mathrm{id}$ so $\bar{\sigma} \in S_X$. Also, $(\bar{\tau}\bar{\sigma})(\sigma\tau) = (\bar{\tau}(\bar{\sigma}\sigma))\tau = (\bar{\tau}\,\mathrm{id})\tau = \mathrm{id}$ and similarly in the other order, so $\sigma\tau \in S_X$.

(3) Suppose $\sigma\tau = \mathrm{id}$. Compose with $\bar{\sigma}$ on the left. Then $\bar{\sigma} = \bar{\sigma}(\sigma\tau) = (\bar{\sigma}\sigma)\tau = \mathrm{id}\,\tau = \tau$. □

REMARK 37. Note that S_X is not commutative! $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ but $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$.

Also, note that $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ – can have $\sigma^{-1} = \sigma$ ("involution").

LEMMA 38. $\#S_n = n!$.

PROOF. n ways to choose $\sigma(1)$, $n-1$ ways to choose $\sigma(2)$ and so on. □

1.2.2. Cycle structure.

DEFINITION 39. For $r \geq 2$ call $\sigma \in S_X$ an *r-cycle* if there are distinct $i_1, \ldots, i_r \in X$ such that $\sigma(i_j) = i_{j+1}$ for $1 \leq j \leq r-1$, suich that $\sigma(i_r) = i_1$, and that $\sigma(i) = i$ if $i \neq i_j$ for all j.

EXAMPLE 40. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$.

DEFINITION 41. Let $\sigma \in S_X$. Set $\mathrm{supp}(\sigma) = \{i \in X \mid \sigma(i) \neq i\}$.

LEMMA 42. *σ, σ^{-1} have the same support. Suppose σ, τ have disjoint supports. Then $\sigma\tau = \tau\sigma$.*

PROOF. $\sigma(i) = i$ iff $\sigma^{-1}(i) = i$. If $i \in \mathrm{supp}(\sigma)$ then $j = \sigma(i) \in \mathrm{supp}(\sigma)$ (else $i = \sigma^{-1}(j) = j$ a contradiction). Thus $\sigma(i) \in \mathrm{Fix}(\tau)$ so $\tau\sigma(i) = \sigma(i)$. Also, $i \in \mathrm{Fix}(\tau)$ so $\sigma\tau(i) = \sigma(i)$). Similarly if $i \in \mathrm{supp}(\tau)$. If i is fixed by both σ, τ there's nothing to prove. $\square$

THEOREM 43 ("Prime factorization"). *Every permutation on a finite set is a product of disjoint cycles. Furthermore, the representation is essentially unique: if we add a "1-cycle"(i) for each fixed point, the factorization is unique up to order of the cycles.*

PROOF. Let σ be a counterexample with mininal support. Then $\sigma \neq \mathrm{id}$, so it moves some i_1. Set $i_2 = \sigma(i_1)$, $i_3 = \sigma(i_3)$ and so on. They are all distinct (else not injective) and since X is finite eventually we return, which must be to i_1 (again by injectivity). Let κ be the resulting cycle. Then $\kappa^{-1}\sigma$ agrees with σ off $\{i_j\}$ and fixes each i_j. Factor this and multiply by κ.

For uniqueness note that the cycles can be intrinsically defined. $\square$

EXAMPLE 44. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 2 & 1 & 5 & 7 & 4 \end{pmatrix} = (1674)(23)(5)$.

1.2.3. Odd and even permutations; the sign. (Taken from Rotman page 8) We now suppose $X = [n]$ is finite.

LEMMA 45. *Every permutation is a product of transpositions.*

PROOF. By induction $(i_1 \cdots i_r) = (i_1 i_2) \cdots (i_{r-1} i_r)$, that is every cycle i $\square$

DEFINITION 46. Let A_n (the "alternating" group) be the set of permutations that can be written as a product of an even number of transpositions.

REMARK 47. A_n is closed under multiplication and inverses, so it is a subgroup of S_n.

LEMMA 48. *Let $1 \leq k \leq n$. Then*

$$(a_1 a_k)(a_1 \ldots a_n) = (a_1 \ldots a_{k-1})(a_k \ldots a_n)$$
$$(a_1 a_k)(a_1 \ldots a_{k-1})(a_k \ldots a_n) = (a_1 \ldots a_n)$$

PROOF. First by direct evaluation, second follows from first on left multiplication by the transposition. $\square$

Discussion: cycle gets cut in two, or two cycles glued together. What is not a_1? cyclicity of cycles.

EXAMPLE 49. $(17)(1674)(23)(5) = (16)(74)(23)(5)$ while $(12)(1674)(23)(5) = (167423)(5)$.

DEFINITION 50. Let $\sigma = \prod_{j=1}^{t} \beta_j$ be the cycle factorization of $\sigma \in S_n$, *including one cycle for each fixed point*. Then $\operatorname{sgn}(\alpha) = (-1)^{n-t}$ is called the *sign* of σ.

LEMMA 51. *Let τ be a transposition. Then* $\operatorname{sgn}(\tau\sigma) = -\operatorname{sgn}(\sigma)$.

PROOF. Suppose $\tau = (a_1 a_k)$. Either both are in the same cycle or in distinct cycles – in either case the number of cycles changes by exactly 1. □

THEOREM 52. *For all $\tau, \sigma \in S_n$ we have* $\operatorname{sgn}(\tau\sigma) = \operatorname{sgn}(\tau)\operatorname{sgn}(\sigma)$.

PROOF. Let $H = \{\tau \in S_n \mid \forall\sigma : \operatorname{sgn}(\tau\sigma) = \operatorname{sgn}(\tau)\operatorname{sgn}(\sigma)\}$. Then H contains all transpositions. Also, H is closed under multiplication: if $\tau, \tau' \in H$ and $\sigma \in S_n$ then

$$\begin{aligned}
\operatorname{sgn}\left((\tau\tau')\sigma\right) &\overset{\text{(assoc)}}{=} \operatorname{sgn}\left(\tau(\tau'\sigma)\right) \\
&\overset{\tau\in H}{=} \operatorname{sgn}(\tau)\operatorname{sgn}\left(\tau'\sigma\right) \\
&\overset{\tau'\in H}{=} \operatorname{sgn}(\tau)\operatorname{sgn}(\tau')\operatorname{sgn}(\sigma) \\
&\overset{\tau\in H}{=} \operatorname{sgn}\left(\tau\tau'\right)\operatorname{sgn}(\sigma).
\end{aligned}$$

By Lemma 45 we see that $H = S_n$ and the claim follows. □

COROLLARY 53. *If $\sigma = \prod_{i=1}^{r} \tau_i$ with each τ_i are transposition then* $\operatorname{sgn}(\tau) = (-1)^r$, *and in particular the parity of r depends on σ but not on the representation.*

COROLLARY 54. *For $n \geq 2$, $\#A_n = \frac{1}{2}\#S_n$.*

PROOF. Let τ be any fixed transposition. Then the map $\sigma \mapsto \tau\sigma$ exchanges the subsets A_n, $S_n - A_n$ of S_n and shows they have the same size. □

EXERCISE 55. A_n is generated by the cycles of length 3.

1.3. $\mathrm{GL}_n(\mathbb{R})$

Let $\mathrm{GL}_n(\mathbb{R}) = \{g \in M_n(\mathbb{R}) \mid \det(g) \neq 0\}$. It is well-known that matrix multiplication is associative and I_n is an identity (best proof of associativity: matrix multiplication corresponds to composition of linear maps and composition of functions is associative).

LEMMA 56. *Every $g \in \mathrm{GL}_n(\mathbb{R})$ has an inverse.*

SUMMARY 57. $(\mathrm{GL}_n(\mathbb{R}), \cdot)$ is a group.

Nex, recall that the map $\det\colon \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ respects multiplication: $\det(gh) = (\det g)(\det h)$. This is one of our first examples of a *group homomorphism.*

EXERCISE 58. (Some subgroups)

(1) Show that $\{g \in \mathrm{GL}_n(\mathbb{R}) \mid g(\mathbb{R}\underline{e}_i) = (\mathbb{R}\underline{e}_i)\}$ is closed under multiplication and taking inverses.
(2) Show that if $\tau i = j$ then $\tau \operatorname{Stab}(i)\tau^{-1} = \operatorname{Stab}(j)$
(3) Show that intersecting some parabolics gives block-diagonal parabolic.

1.4. The dihedral group

Let P_n be the regular polygon with n sides. Let $D_{2n} = \mathrm{Aut}(P_n)$ be the set of maps of the plan that map P_n to itself.

- Label vertices $0, 1, \cdots, n-1$ (in fact, label them using $\mathbb{Z}/n\mathbb{Z}$).
- Then have a map $c \in D_{2n}$ ("cycle"), with $c([i]) = [i+1]$. Note that $c^j([i]) = [i+j]$.
- And a map $r \in D_{2n}$ ("reflection" by the vertical axis) with $r([i] = -[i])$. Note that $r^2 = \mathrm{id}$ and that $rcr = c^{-1}$.

LEMMA 59. *Suppose $g \in D_{2n}$ fixes $[0]$. Then g is either id or r. Any $g \in D_{2n}$ can be written uniquely in the form $c^j r^\varepsilon$ for $j \in \mathbb{Z}/n\mathbb{Z}$ and $\varepsilon \in \mathbb{Z}/2\mathbb{Z}$.*

PROOF. For the first claim if we fix $[0]$ then we either fix $[1]$, at which point we fix everything by induction or we map $[1]$ to $[-1]$ at which point we reverse signs by induction.

For the second, suppose $g(0) = j$. Then $c^{-j}g$ fixes zero, so either $c^{-j}g = \mathrm{id}$ or $c^{-j}g = r$. For uniqueness, suppose $c^j r^\varepsilon = c^k r^\delta$. Then $c^{j-k} = r^{\delta-\varepsilon}$ so c^{j-k} fixes 0 so $j \equiv k\,(n)$. This means that also $r^\varepsilon = r^\delta$ so $\varepsilon = \delta$. $\square$

COROLLARY 60. *$\#D_{2n} = 2n$.*

LEMMA 61. *$c^j r^\varepsilon c^k r^\delta = c^{j+\sigma k} r^{\varepsilon+\delta}$ where $\sigma = +$ if $\varepsilon = 0$ and $\sigma = -$ if $\varepsilon = 1$.*

PROOF. if $\varepsilon = 0$ clear. If $\varepsilon = 1$ we have

$$c^j r c^k r r r^\delta = c^j \left(rcr\right)^k r^{1+\delta} = c^{j-k} r^{1+\delta}.$$

$\square$

REMARK 62. We saw that D_{2n} is *generated* by r, c.

CHAPTER 2

Groups and homomorphisms

2.1. Groups, subgroups, homomorphisms (Lecture 6, 29/9/2015)

2.1.1. Groups.

DEFINITION 63 (Group). A *group* is a pair $(G,\cdot)$ where G is a set and $\cdot\colon G\times G\to G$ is a binary operation satisfying:

(1) *Associativity*: $\forall x,y,z\in G:(xy)z=x(yz)$.
(2) *Neutral element*: $\exists e\in G\forall x\in G:ex=x$.
(3) *Left inverse*: $\forall x\in G\exists\bar{x}\in G:\bar{x}x=e$.

If, in addition, we have $\forall x,y\in G:xy=yx$ we call the group *commutative* or *abelian*.

Fix a group G.

LEMMA 64 (Unit and inverse). *(1) $\bar{x}$ is a two-sided inverse: $x\bar{x}=e$ as well.*
(2) e is a two-sided identity: $\forall x:xe=x$.
(3) The identity and inverse are unique.
(4) $\bar{\bar{x}}=x$.

PROOF. (1) For any $x\in G$ we have $\bar{x}=e\bar{x}=(\bar{x}x)\bar{x}=\bar{x}(x\bar{x})$. Multiplying on the left by $\bar{\bar{x}}$ we see that

$$e=\bar{\bar{x}}\bar{x}=\bar{\bar{x}}(\bar{x}(x\bar{x}))=(\bar{\bar{x}}\bar{x})(x\bar{x})=e(x\bar{x})=x\bar{x}.$$

(2) For any $x\in G$ we have $xe=x(\bar{x}x)=(x\bar{x})x=ex=x$.
(3) Let e' be another left identity. Then $e=e'e=e'$. Let $\bar{x}'$ be another left inverse. Then

$$\bar{x}'x=e.$$

Multiplying on the right by $\bar{x}$ we get

$$\bar{x}'=\bar{x}.$$

(4) We have $\bar{\bar{x}}\bar{x}=e$. Now multiply on the right by x. □

NOTATION 65. We write x^{-1} for the unique inverse to x. Then $\left(x^{-1}\right)^{-1}=x$.

REMARK 66. Because of this Lemma, quite often the axioms call for a two-sided identity and a two-sided inverse.

COROLLARY 67 (Cancellation laws). *Suppose $xy=xz$ or $yx=zx$ holds. Then $x=y$.*

PROOF. Multiply by x^{-1} on the appropriate side. □

COROLLARY 68. *e is the unique element of G satisfying $xx=x$.*

PROOF. Multiply by x^{-1}. □

EXAMPLE 69 (Examples of groups). (0) The trivial group.

(1) $\mathbb{Z}$, S_n, $\mathrm{GL}_n(\mathbb{R})$.
(2) $\mathbb{R}^+$, additive group of vector space.
(3) $\mathbb{Q}^\times$, $\mathbb{R}^\times$, $\mathbb{C}^\times$.
(4) $C_n \simeq (\mathbb{Z}/n\mathbb{Z}, +)$, $(\mathbb{Z}/n\mathbb{Z})^\times$.
(5) Symmetry groups.
  (a) Graph automorphisms.
  (b) Orthogonal groups.

EXAMPLE 70 (Non-groups). (1) $(\mathbb{Z}_{\geq 0}, +)$.
(2) $(\mathbb{Z}, \times)$, $(M_n(\mathbb{R}), +)$.
(3) $(\mathbb{Z}_{\geq 1}, \mathrm{gcd})$. $(\mathbb{Z}_{\geq 1}, \mathrm{lcm})$.

2.1.2. Homomorphisms.

PROBLEM 71. Are $(\mathbb{Z}/2\mathbb{Z}, +)$ and $(\{\pm 1\}, \times)$ the same group? Are $\mathbb{R}^+$and $\mathbb{R}^\times_{>0}$ the same group?

DEFINITION 72. Let $(G, \cdot), (H, *)$ be a groups. A *(group) homomorphism* from G to H is function $f\colon G \to H$ such that $f(x \cdot y) = f(x) * f(y)$ for all $x, y \in G$. Write $\mathrm{Hom}(G, H)$ for the set of homomorphisms.

EXAMPLE 73. Trivial homomorphism, $\mathrm{sgn}\colon S_n \to \{\pm 1\}$, $\det\colon \mathrm{GL}_n \to \mathrm{GL}_1$, the quotient map $\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$.

LEMMA 74. *Let $f\colon G \to H$ be a homomorphism. Then*
(1) $f(e_G) = e_H$.
(2) $f(g^{-1}) = (f(g))^{-1}$.

PROOF. (1) e_G, e_H are the unique solutions to $xx = x$ in their respective groups.
(2) We have $f(g)f(g^{-1}) = f\left(gg^{-1}\right) = f(e_G) = e_H$ so $f(g), f(g^{-1})$ are inverses. □

DEFINITION 75. $f \in \mathrm{Hom}(G, H)$ is called an *isomorphism* if it is a bijection.

PROPOSITION 76. *f is an isomorphism iff there exists $f^{-1} \in \mathrm{Hom}(H, G)$ such that $f \circ f^{-1} = \mathrm{id}_H$ and $f^{-1} \circ f = \mathrm{id}_G$.*

PROOF. PS4 □

LEMMA 77. *Let $g\colon G \to H$, $f\colon H \to K$ be group homomorphisms. Then $f \circ g\colon G \to K$ is a group homomorphism.*

PROOF. PS4. □

EXAMPLE 78. $(\mathbb{Z}/5\mathbb{Z})^\times$ and $(\mathbb{Z}/8\mathbb{Z})^\times$ are non-isomorphic groups of order 4.

PROOF. On the right we have $g \cdot g = 1$ for all g. On the left this fails. □

2.1.3. Subgroups.

LEMMA 79. *Let $(G, \cdot)$be a group, and let $H \subset G$ be non-empty and closed under $\cdot$ and under inverses, or under $(x, y) \mapsto xy^{-1}$. Then $e \in H$ and $(H, \cdot \restriction_{H \times H})$ is a group.*

PROOF. Let $x \in H$ be any element. under either hypothesis we have $e = xx^{-1} \in H$. In the second case we now have for any $y \in H$ that $y^{-1} = ey^{-1} \in H$ and hence that for any $x,y \in H$ that $xy = x(y^{-1})^{-1} \in H$. Thus in any case $\cdot \restriction_{H\times H}$ is H-valued, and satisfies the existential axioms. The associative law is universal. $\square$

DEFINITION 80. Such H is called a *subgroup* of G.

Group homomorphisms have kernels and images, just like linear maps.

DEFINITION 81 (Kernel and image). Let $f \in \mathrm{Hom}(G,H)$. Its *kernel* is the set $\mathrm{Ker}(f) = \{g \in G \mid f(g) = e_H\}$. Its *image* is the set $\mathrm{Im}(f) = \{h \in H \mid \exists g \in G : f(g) = h\}$.

PROPOSITION 82. *The kernel and image of a homomorphism are subgroups of the respective groups.*

PROOF. (not given in class) Since $f(e_G) = e_H$ we have $e_G \in \mathrm{Ker}(f)$ and $e_H \in \mathrm{Im}(f)$ so both are non-empty. Let $g,g' \in \mathrm{Ker}(f)$. Then $f(g^{-1}) = f(g)^{-1} = e_H^{-1} = e_H$ and $f(gg') = f(g)f(g') = e_He_H = e_H$.
Similarly let $h,h' \in \mathrm{Im}(f)$. Choose preimages $g \in f^{-1}(h)$ and $g' \in f^{-1}(h')$. Then $h^{-1} = f(g)^{-1} = f(g^{-1}) \in \mathrm{Im}(f)$ and $hh' = f(g)f(g') = f(gg') \in \mathrm{Im}(f)$. $\square$

QUESTION 83. *Is every subgroup the kernel of some homomorphism?*

EXERCISE 84. Is every subspace of a vector space the kernel of a linear map?

LEMMA 85. *f in injective iff* $\mathrm{Ker} f = \{e\}$.

PROOF. (not given in class) Suppose f is injective. Then for $g \neq e$, $f(g) \neq f(e)$ so $\mathrm{Ker}(f) = e$. Conversely, suppose $\mathrm{Ker}(f) = e$ and that $f(g) = f(g')$. Then

$$f(g^{-1}g') = f(g)^{-1}f(g') = f(g)^{-1}f(g) = e$$

so $g^{-1}g' \in \mathrm{Ker}(f)$. By hypothesis this means $g^{-1}g' = e$ so $g' = g$ and f is injective. $\square$

2.2. Examples (Lecture 7, 1/10/2015)

2.2.1. Isomorphism and non-isomorphism; orders of elements.

EXAMPLE 86. In $(\mathbb{Z}/8\mathbb{Z})^\times$ every element has $x^2 = 1$. But this isn't the case in $(\mathbb{Z}/5\mathbb{Z})^\times$.

DEFINITION 87. Say $[3] \in (\mathbb{Z}/8\mathbb{Z})^\times$ has *order* 2 but $[3] \in (\mathbb{Z}/5\mathbb{Z})^\times$ has *order* 4.

2.2.2. Cyclic groups.

DEFINITION 88. Let G be a group, $g \in G$. We set $g^0 = e$, for $n \geq 0$ define by recursion $g^{n+1} = g^n g$, and for $n < 0$ set $g^n = \left(g^{-1}\right)^{-n}$.

PROPOSITION 89 (Power laws). *For $n,m \in \mathbb{Z}$we have (1) $g^{n+m} = g^n g^m$ (that is, the map $n \mapsto g^n$ is a group homomorphism $(\mathbb{Z},+) \to G$) and (2) $(g^n)^m = g^{nm}$.*

PROOF. PS3. $\square$

LEMMA 90. *The image of the homomorphism $n \mapsto g^n$ is the smallest subgroup containing g, denoted $\langle g \rangle$ and called the* cyclic subgroup *generated by g.*

PROOF. The image is a subgroup and is contained in any subgroup containing g. $\square$

DEFINITION 91. A group G is *cyclic* if $G = \langle g \rangle$for some $g \in G$.

PROPOSITION 92. *Let G be cyclic, generated by g, and let $f(n) = g^n$ be the standard homomorphism. Then either:*

(1) $\operatorname{Ker} f = \{0\}$*and* $f \colon \mathbb{Z} \to G$ *is an isomorphism.*
(2) $\operatorname{Ker} f = n\mathbb{Z}$*and* f *induces an isomorphism* $\mathbb{Z}/n\mathbb{Z} \to G$.

NOTATION 93. The isomorphism class of $\mathbb{Z}$ is called the *infinite cyclic group*. The isomorphism class of $(\mathbb{Z}/n\mathbb{Z}, +)$ is called the *cyclic group of order n* and denoted C_n.

REMARK 94. The generator isn't unique (e.g. $\langle g \rangle = \langle g^- \rangle$).

PROOF. f is surjective by definition. If $\operatorname{Ker} f = \{0\}$ then f is injective, hence an isomorphism. Otherwise, by Proposition 7 we have $\operatorname{Ker} f = n\mathbb{Z}$ for some n. We now define $\bar{f} \colon \mathbb{Z}/n\mathbb{Z} \to G$ by $\bar{f}([a]_n) = g^a$.

- This is well-defined: if $[a]_n = [b]_n$ then $a - b = cn$ for some c and then by the power laws, $f(a) = f(b + cn) = f(b) f(cn) = f(b)$ since $cn \in \operatorname{Ker} f$.
- This is a homomorphism: $\bar{f}([a]_n + [b]_n) = \bar{f}([a+b]_n) = f(a+b) = f(a)f(b) = \bar{f}([a]_n)\,\bar{f}([b]_n)$.
- This is injective: $[a]_n \in \operatorname{Ker} \bar{f} \iff f(a) = e \iff a \in n\mathbb{Z} \iff [a]_n = [0]_n$.

□

DEFINITION 95. The *order* of $g \in G$ is the size of $\langle g \rangle$.

COROLLARY 96. *The order of g is the least positive m such that $g^m = e$ (infinity if there is no such m).*

OBSERVATION 97. *If G is finite, then every $g \in G$ has finite order.*

EXAMPLE 98. In $\mathrm{GL}_2(\mathbb{R})$, $\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$ has infinite order while $\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$ has order 2 and $\begin{pmatrix} & -1 \\ 1 & \end{pmatrix}$ has order 4.

LEMMA 99. *If G is finite, and $H \subset G$ is non-empty and closed under $(x,y) \mapsto xy$ it is a subgroup.*

PROOF. If g has order n then $g^{-1} = g^{n-1}$ can be obtained from g by repeated multiplication.

□

2.2.3. "Philosophy": automorphism groups. X set with "structure". Then $\operatorname{Aut}(X) = \{g \colon X \to X \mid g, g^{-1}$ "pr
is a group. Use it to learn information about X.

EXAMPLE 100. X is $\mathbb{R}^n$ with Euclidean distance. The automorphism group is the *isometry group of Euclidean space*.
X a graph (more below)
G a group. $\operatorname{Aut}(G) = \operatorname{Hom}(G,G) \cap S_G$.

2.2.4. Dihedral groups (see practice problems).

DEFINITION 101. A *(simple) graph* is an ordered pair $\Gamma = (V, E)$ where V is a set ("vertices") and $E \subset V \times V$ is a set ("edges") such that $(x,x) \notin E$ and $(x,y) \in E \leftrightarrow (y,x) \in E$.

Example: K_n, cycle ...

DEFINITION 102. An *automorphism* of Γ is a map $f \in S_{V(\Gamma)}$ such that $(x,y) \in E \leftrightarrow (f(x), f(y)) \in E$.

LEMMA 103. $\mathrm{Aut}(\Gamma) < S_\Gamma$ *is a subgroup.*

EXAMPLE 104. $\Gamma = K_n$, $\mathrm{Aut}(\Gamma) = S_n$.

We concentrate on the cycle.

DEFINITION 105. $D_{2n} = \mathrm{Aut}(n\text{-cycle})$.

This contains n *rotations* (a subgroup isomorphic to C_n), n *reflections.*

LEMMA 106. $|D_{2n}| = 2n$.

PROOF. Enough to give an upper bound. Label the cycle by $\mathbb{Z}/n\mathbb{Z}$. Let $f \in D_{2n}$ and suppose that $f([0]) = a$. Then $f([1]) \in \{a+1, a-1\}$ and this determines the rest. $\square$

LEMMA 107. $C_n < D_{2n}$ *is normal.*

2.3. Subgroups and coset spaces (Lecture 8, 6/10/2015)

2.3.1. The lattice of subgroups; generation.

LEMMA 108. *The intersection of any family of subgroups is a subgroup.*

DEFINITION 109. Given $S \subset G$, the *subgroup generated by* S, is the subgroup $\langle S \rangle = \bigcap \{H < G \mid S \subset G\}$.

Note that this is the smallest subgroup of G containing S.

DEFINITION 110. A *word* in S is an expression $\prod_{i=1}^{r} x_i^{\varepsilon_i}$ where $x_i \in S$ and $\varepsilon_i \in \{\pm 1\}$.

By induction on r, if H is a subgroup containing S and w is a word in S of length r then $w \in H$.

PROPOSITION 111. $\langle S \rangle$ *is the set of elements of* G *expressible as words in* S.

PROOF. Let W be the set of elements expressible as words. Then W non-empty (trivial word) and is closed under products (concatenation) and inverses (reverse order exponents), so $W \supset \langle S \rangle$. On the other hand we just argued that $W \subset \langle S \rangle$. $\square$

2.3.2. Coset spaces and Lagrange's Theorem. Fix a group G and a subgroup H.

Define a relation on G by $g \equiv_L g' \, (H)$ iff $\exists h \in H : g' = gh$ iff $g^{-1}g' \in H$. Example: $g \equiv_L e \, (H)$ iff $g \in H$.

LEMMA 112. *This is an equivalence relation. The equivalence class of* g *is the set* gH.

DEFINITION 113. The equivalence classes are called *left cosets*.

REMARK 114. Equivalently, we can define right cosets Hg which are the equivalence classes for the relation $g' \equiv_R g \, (H) \leftrightarrow g'g^{-1} \in H$.

DEFINITION 115. Write G/H for the *coset space* $G/\equiv_L (H)$ (this explains the notation $\mathbb{Z}/n\mathbb{Z}$ from before). The *index* of H in G, denoted $[G:H]$, is the cardinality of G/H.

LEMMA 116. *The map* $gH \mapsto Hg^{-1}$ *is a bijection between* $H\backslash G$ *and* G/H. *In particular, the index does not depend on the choice of left and right cosets.*

THEOREM 117 ("Lagrange's Theorem"). $|G| = [G:H] \times |H|$. *In particular, if G is finite then $|H|$ divides $|G|$.*

PROOF. Let $R \subset G$ be a *system of representatives* for G/H, that is a set intersecting each coset at exactly one element. The function $R \to G/H$ given by $r \mapsto rH$ is a bijection, so that $|R| = [G:H]$. Finally, the map $R \times H \to G$ given by $(r,h) \mapsto rh$ is a bijection. $\square$

COROLLARY 118. *Let G be a finite group. Then the order of every $g \in G$ divides the order of G. In particular, $g^{\#G} = e$.*

PROOF. Let g have order m. Then $m = |\langle g \rangle|$ is the order of a subgroup of G. Moreover, $g^{\#G} = (g^m)^{\#G/m} = e$. $\square$

REMARK 119. Lagrange stated a special case in 1770. The general case is probably due to Galois; a proof first appeared in Gauss's book in 1801.

FACT 120. *It is a Theorem of Philip Hall that if G is finite, then $H\backslash G$ and G/H always have a* common *system of representatives.*

EXAMPLE 121. Let p be prime. Then every group of order p is isomorphic to C_p.

PROOF. Let G have order p, and let $g \in G$ be a non-identity element, say of order $k = |\langle g \rangle|$. Then $k|p$, but $k \neq 1$ ($g \neq e$) so $k = p$ and $\langle g \rangle = G$. $\square$

EXAMPLE 122 (Fermat's Little Theorem; Euler's Theorem). Let $a \in \mathbb{Z}$. Then:

(1) If $\gcd(a,p) = 1$ then $a^{p-1} \equiv 1\,(p)$.
(2) $a^p \equiv a\,(p)$.
(3) If $\gcd(a,n) = 1$ then $a^{\phi(n)} \equiv 1\,(n)$.

PROOF. For (1), $(\mathbb{Z}/p\mathbb{Z})^\times$ is a group of order $p-1$. (2) follows from (1) unless $[a] = 0$, when the claim is clear. (3) is the same for $(\mathbb{Z}/n\mathbb{Z})^\times$, a group of order $\phi(n)$. $\square$

2.4. Normal subgroups and quotients (Lectures 9–10)

2.4.1. Normal subgroups (Lecture 9, 8/10/2015). HW: Every subgroup is normal in its normalizer.

We will answer Question 83. To start with, we identify a constraint on kernels.

LEMMA 123. *Let $f \in \mathrm{Hom}(G,H)$ and let $g \in G$. Then $g\,\mathrm{Ker}(f)g^{-1} = \mathrm{Ker}(f)$.*

PROOF. Let $g \in G$, $n \in \mathrm{Ker}(f)$. Then $f\left(gng^{-1}\right) = f(g)f(n)f(g^{-1}) = f(g)f(g)^{-1} = e$ so $gng^{-1} \in \mathrm{Ker}\,f$ as well. $\square$

DEFINITION 124. Call $N < G$ *normal* if $gN = Ng$ for all $g \in G$, equivalently if $gNg^{-1} = N$ for all $g \in G$. In that case we write $N \lhd G$.

LEMMA 125. *Enough to check $gNg^{-1} \subset N$.*

PROOF. PS5 Practice problem P4. $\square$

EXAMPLE 126. $\{e\}, G$ always normal; Any subgroup of an abelian group.
$\mathrm{SL}_n(\mathbb{R}) \lhd \mathrm{GL}_n(\mathbb{R})$ (kernel of determinant), $A_n \lhd S_n$ (kernel of sign). Translations in $\mathrm{Isom}(\mathbb{E}^n)$.

LEMMA 127. *The intersection of any family of normal subgroups is normal.*

DEFINITION 128. The *normal closure* of $S < G$ is the normal subgroup $\langle S \rangle^{\mathrm{N}} = \bigcap \{N \lhd G \mid S \subset N\}$.

2.4.2. Quotients.

LEMMA 129. *The subgroup $N < G$ is normal iff the relation $\equiv (N)$ respects products and inverses.*

PROOF. Suppose N is normal, and suppose that $g \equiv g' (N)$ and that $h \equiv h' (N)$. Then

$$(gh)^{-1} \left(g'h'\right) = h^{-1} \left(g^{-1}g'\right) h' = \left[h^{-1} \left(g^{-1}g'\right) h\right] \left(h^{-1}h'\right) \in N .$$

Also, $g \equiv_L g' (N)$ iff $g^{-1} \equiv_R \left(g'\right)^{-1} (N)$ but if N is normal then the two relations are the same.
The converse is practice problem 5 of PS5. □

COROLLARY 130. *Defining group operations via representatives endows G/N with the structure of a group.*

DEFINITION 131. This is called the quotient *of G by N*.

LEMMA 132. *The quotient map $g \mapsto gN$* is a surjective group homomorphism with kernel N.

EXAMPLE 133. $\mathbb{Z}$ is commutative, so every subgroup is normal, and we get a group $\mathbb{Z}/n\mathbb{Z}$.

Motivation: "kill off" the elements of N.

2.4.3. Isomorphism Theorems (Lecture 10, 13/10/2015).

THEOREM 134 (First isomorphism theorem). *Let $f \in \mathrm{Hom}(G,H)$ and let $K = \mathrm{Ker}(f)$. Then f induces an isomorphism $G/K \to \mathrm{Im}(f)$.*

PROOF. Define $\bar{f}(gK) = f(g)$. This is well-defined: if $gK = g'K$ then $g' = gk$ for some $k \in K$ and then $f(g') = f(gk) = f(g)f(k) = f(g)$ since $k \in K$. It is a group homomorphism by definintion of the product structure on G/K. The image is the same as f by construction. As to the kernel, $\bar{f}(gK) = e_H$ iff $f(g) = e_H$ iff $g \in K$ iff $gK = K = e_{G/K}$. □

THEOREM 135 (Second isomorphism theorem). *Let $N,H < G$ with N normal. Then $N \cap H$ is normal in H, and the natural map $H \to HN$ induces an isomorphism*

$$H/\left(H \cap N\right) \xrightarrow{\simeq} HN/N .$$

PROOF. Composing the inclusion $\iota \colon H \to HN$ and the quotient map $\pi \colon HN \to HN/N$ gives a homomorphism $f = \pi \circ \iota \colon H \to HN/N$. f is surjective: we have $(hn)N = h(nN) = hN$ for any $h \in H$, $n \in N$ so every coset has a representative in the image of ι. We now compute its kernel. Let $h \in H$. Then $h \in \mathrm{Ker} f$ iff $f(h) = e_{HN/N}$ iff $\pi(h) = N$ iff $hN = N$ iff $h \in N$ iff $h \in N \cap H$. Thus $\mathrm{Ker} f = H \cap N$ and the claim follows from the previous Theorem. □

THEOREM 136 (Third isomorphism theorem). *Let $K < N < G$ be subgroups with K,N normal in G. Then N/K is normal in G/K and there is a natural isomorphism $G/N \to (G/K)/(N/K)$.*

PROOF. Let $nK \in N/K$ and let $gK \in G/K$. Then $(gK)(nK)(gK)^{-1} \stackrel{\text{def}}{=} gng^{-1}K \in N/K$ so $N/K \lhd G/K$. Now Let f be the composition of the quotient maps $G \to G/K \to (G/K)/(N/K)$. Then f is surjective (composition of surjective maps) and $g \in \mathrm{Ker} f$ iff $gK \in N/K$ iff $g \in N$. □

2.4.4. Simplicity of A_n.

DEFINITION 137. G is *simple* if it has no normal subgroups except for $\{e\}, G$ ("prime")

LEMMA 138 (Generation and conjugacy in A_n). *The pairs* (123),(145) *and* $(12)(34)$, $(12)(35)$ *are conjugate in* A_5.

PROOF. Conjugate by $(24)(35)$ and (345) respectively. □

LEMMA 139 (Generation and conjugacy in A_n). *Let* $n \geq 5$.

(1) All cycles of length 3 *are conjugate in* A_n *and generate the group..*
(2) All elements which are a product of two disjoint transpositions are conjugate in A_n *and generate the group.*

PROOF. PS3 □

THEOREM 140. A_n *is simple if* $n \geq 5$.

PROOF. Let $N \lhd A_n$ be normal and non-trivial and let $\sigma \in N \setminus \{\text{id}\}$ have minimal support, wlog $\{1, \ldots, k\}$.

Case 1. $k = 1$ would make $\sigma = \text{id}$.
Case 2. $k = 2$ would make σ a transposition.
Case 3. $k = 3$ makes σ a 3-cycle. By Lemma 139(1), N contains all 3-cycles and thus equals A_n.
Case 4. $k = 4$ makes σ of the form $(12)(34)$ since 4-cycles are odd. We are then done by Lemma 139(2).
Case 5. $k \geq 5$ and σ has a cycle of length at least 3. We may then assume $\sigma(1) = 2$, $\sigma(2) = 3$ and let $\gamma = (345)\sigma(345)^{-1}\sigma^{-1} \in N$. Then γ fixes every point that σ does, and also $\gamma(2) = 2$, but $\gamma(3) = 4$, so $\gamma \neq \text{id}$ – a contradiction.
Case 6. $k \geq 5$ and σ is a product of disjoint transpositions (necessarily at least 4), say $\sigma = (12)(34)(56)(78)\cdots$. Then the same γ again fixes every point that σ fixes, and also $1,2$ – but it still exchanges $7,8$ – another contradiction.

□

2.4.5. Alternative proofs.

2.4.5.1. *(taken from Rotman's book).*

(1) $A_n$is generated by 3-cycles if $n \geq 5$.
(2) A_5 is simple:
   (a) The conjugacy classes of (123) and $(12)(34)$ generate A_5.
   (b) The other conjugacy classes id, (12345) (13542) have sizes $1, 12, 12$ which do not add up to a divisor of 60.
(3) A_6 is simple:
   (a) Let $N \lhd A_6$ be normal and non-trivial. For $i \in [6]$, let $P_i = \text{Stab}_{A_6}(i) \simeq A_5$. Then $N \cap P_i$ is normal in P_i. If this is non-trivial then by (1), $P_i \subset N$ and hence N contains a 3-cycle, so $N = A_6$. Otherwise every element of N has full support.
   (b) The possible cycle structures are $(123)(456)$ and $(12)(3456)$. In the second case the square is a non-trivial element of N with a fixed point. In the first case conjugate with (234) to get a fixed point.

(4) For $n \geq 6$ let $N \triangleleft A_n$ be normal. Let $\sigma \in N$ be non-identity with, say, $\sigma(1) = 2$. Then κ=(234) does not commute with σ ($\kappa\sigma(1) = 3$ but $\sigma\kappa(1) = 2$).

(5) The element $\gamma = [\sigma, \kappa] = \sigma\kappa\sigma^{-1}\kappa^{-1} = \sigma\left(\kappa\sigma^{-1}\kappa^{-1}\right) \in N$ is also non-identity. But writing this element as $\left(\sigma\kappa\sigma^{-1}\right)\kappa^{-1}$we see that it is a product of two 3-cycles and hence has support of size at most 6. This therefore belongs to a copy A^* of A_6 inside A_n. But $N \cap A^*$ is normal, and $A_6$is simple. Thus N contains A^* and in particular a 3-cycle.

2.4.5.2. *Induction.*

(1) A_5 is simple: see above.

(2) Suppose A_n simple, and let $N \triangleleft A_{n+1}$ be non-trivial. If $N \cap P_i$ is non-trivial for $i \in [n+1]$ then $P_i \subset N$ so N contains a 3-cycle and $N = A_{n+1}$. Otherwise every element of N has full support.

(3) Let $\sigma \in N$ be non-trivial, say $\sigma(1) = 2$, and $\sigma(3) = 4$ (move every element!). Let $\tau = (12)(45)$. Then $(\sigma\tau)(3) = 4$ while $\tau\sigma(3) = 5$, so $\sigma\tau\sigma^{-1}\tau^{-1} \in N$ is non-trivial and fixes $1, 2$ – a contradiction.

CHAPTER 3

Group Actions

3.1. Group actions (Lecture 11, 15/10/2015)

DEFINITION 141 (Group action). An *action* of the group G on the set X is a binary operation $\cdot\colon G\times X\to X$ such that $e_G\cdot x=x$ for all $x\in X$ and such that $g\cdot(h\cdot x)=(gh)\cdot x$ for all $g,h\in G$, $x\in X$. A *G-set* is a pair $(X,\cdot)$ where X is a set and $\cdot$ is an action of G on X. We sometimes write $G\curvearrowright X$.

We discus Examples of group actions

(0) For any X,G we have the *trivial action* $g\cdot x=x$ for all x.
(1) S_X acting on X. Key example.
(2) F field, V F-vector space. Then scalar multiplication is an action $F^\times\curvearrowright V$.
  - Orbit of non-zero vector is (roughly) the 1d subspace it spans.
(3) X set with “structure”, $\mathrm{Aut}(X)=\left\{\sigma\in S_X\mid\sigma,\sigma^{-1}\text{ "preserve the structure"}\right\}$ acts on X.
  - Can always restrict actions: if $\cdot\colon G\times X\to X$ is an action then $\cdot\restriction_{H\times X}$ is an action of H.

  (a) D_{2n} acting on cycle, inside of there’s C_n acting on te cycle; $\mathrm{Aut}(\Gamma)$ acting on Γ.
  (b) $\mathrm{GL}_n(\mathbb{R})$ acting on $\mathbb{R}^n$, $\mathrm{GL}(V)$ acting on V.
  (c) G group; $\mathrm{Aut}(G)$ acting on G.
(4) Induced actions (see Problem Set): suppose G acts on X,Y.
  (a) G acts on Y^X by $(g\cdot f)(x)\stackrel{\text{def}}{=}g\cdot\left(f\left(g^{-1}\cdot x\right)\right)$ (in particular, action of G on the vector space F^X where X is a G-set).
  (b) G acts on $P(X)$ by $g\cdot A=\{g\cdot a\mid a\in A\}$.
  (c) etc.

3.1.1. The regular action and the homomorphism picture.

The *regular action*: G acting on itself by left multiplication: For $g\in G$ and $x\in G$ let $g\cdot x=gx$. Action by group axioms.

We now obtain a different point of view on actions. For this let G act on X, fix $g\in G$ and consider the function $\sigma_g\colon X\to X$ given by

$$\sigma_g(x)\stackrel{\text{def}}{=}g\cdot x.$$

LEMMA 142 (Actions vs homomorphisms). *In increasing level of abstraction:*

(1) $\sigma_g\in S_X$ for all $g\in G$.
(2) $g\mapsto\sigma_g$ is a group homomorphism homomorphism $G\to S_X$.
(3) The resulting map from group actions to $\mathrm{Hom}(G,S_X)$ *is a bijection*

$$\{\textit{actions of } G \textit{ on } X\}\leftrightarrow\mathrm{Hom}(G,S_X).$$

PROOF. We first show $\sigma_g \circ \sigma_h = \sigma_{gh}$. Indeed for any $x \in X$:

$$\begin{aligned}
(\sigma_g \circ \sigma_h)(x) &= \sigma_g(\sigma_h(x)) && \text{def of } \circ \\
&= g \cdot (h \cdot x) && \text{def of } \sigma_g, \sigma_h \\
&= (gh) \cdot x && \text{def of gp action} \\
&= \sigma_{gh}(x) && \text{def of } \sigma_{gh}\,.
\end{aligned}$$

This doesn't give (2) because we don't yet know (1). For that we use the axiom that $\sigma_e = \mathrm{id}$ to see that

$$\sigma_g \circ \sigma_{g^{-1}} = \mathrm{id} = \sigma_{g^{-1}} \circ \sigma_g$$

and hence that $\sigma_g \in S_X$ at which point we get (1),(2).

For (3), if $\sigma \in \mathrm{Hom}(G, S_X)$ then set $g \cdot x \stackrel{\mathrm{def}}{=} (\sigma(g))(x)$. This is indeed an action, and evidently this is the inverse of the map constructed in (2). □

REMARK 143. This Lemma will be an important source of homomorphisms, and therefore of normal subgroups (their kernels).

We now get the first payoff of our theory:

THEOREM 144 (Cayley 1878). *Every group G is isomorphic to a subgroup of S_G. In particular, every group of order n is isomorphic to a subgroup of S_n.*

PROOF. Consider the left-regular action of G on itself. This corresponds to a homomorphism $L_G \colon G \to S_G$. We show that $\mathrm{Ker}(L_G) = \{e\}$, so that L_G will be an isomorphism onto its image. For that let $g \in \mathrm{Ker}(L_G)$. Then $L_G(g) = \mathrm{id}_G$, and in particular this means that g fixes e: $g \cdot e = e$. But this means $g = e$ and we are done. □

REMARK 145. Can make this quantitative: [**1**] asks for the minimal m such that G is isomorphic to a subgroup of S_m.

LEMMA 146. *For any prime p, C_p is isomorphic to a subgroup of S_n iff $n \geq p$.*

PROOF. If $n \geq p$ then S_n includes a p-cycle. Conversely, by Lagrange's Theorem 117, if S_n has a subgroup isomorphic to C_p then $p | n!$. Since p is prime this means $p | k$ for some $k \leq n$ so that $p \leq k \leq n$. □

REMARK 147. Johnson shows that if G has order n and embeds in S_n but no smaller S_m then either $G \simeq C_p$ or G has order 2^k for some k, and for each such order there is a unique group with the property.

3.2. Conjugation (Lecture 12, 22/10/2015)

This is another action on G on itself, but it's not the regular action!

3.2.1. Conjugacy of elements.

DEFINITION 148. For $g \in G$, $x \in G$ set ${}^g x = gxg^{-1}$. Set $\gamma_g(x) = gxg^{-1}$.

LEMMA 149. *This is a group action of G on itself, and it is an action by* automorphisms*: $\gamma_g \in \mathrm{Aut}(G)$.*

PROOF. Check. □

DEFINITION 150. Say "x is conjugate to y" if there is $g \in G$ such that ${}^g x = y$.

LEMMA 151. *This is an equivalence relation.*

PROOF. See PS3, problem 2(a). $\square$

DEFINITION 152. The equivalence classes are called *conjugacy classes. Write $G\backslash X$ for the set of equivalence classes.*

EXAMPLE 153. The class of e is $\{e\}$. More generally, the class of x is $\{x\}$ iff $x \in Z(G)$ (proof).

REMARK 154. Why is conjugacy important? Because

(1) The action is by *automorphisms*, so conjugate elements have identical group-theoretic properties (same order, conjugate centralizers etc).
(2) These automorphisms are readily available.

In fact, the map $g \mapsto \gamma_g$ is a group homomorphism $G \to \mathrm{Aut}(G)$ (this is Lemma 142(2)).

DEFINITION 155. The image of this homomorphism is denoted $\mathrm{Inn}(G)$ and called the group of *inner automorphisms*.

EXERCISE 156. The kernel is exactly $Z(G)$, so by Theorem 134, $\mathrm{Inn}(G) \simeq G/Z(G)$. Also, if $f \in \mathrm{Aut}(G)$ then $f \circ \gamma_g \circ f^{-1} = \gamma_{f(g)}$ so $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$.

DEFINITION 157. Call $\mathrm{Out}(G) \stackrel{def}{=} \mathrm{Aut}(G)/\mathrm{Inn}(G)$ the *outer automorphism group* of G.

EXAMPLE 158. $\mathrm{Aut}(\mathbb{Z}^d) \simeq \mathrm{GL}_d(\mathbb{Z})$ but all inner automorphisms are trivial (the group is commutative).

On the other hand, if $\#X \geq 3$ then $\mathrm{Inn}(S_X) = S_X$ (the center is trivial).

FACT 159. $\mathrm{Out}(S_n) = \{e\}$ *except that* $\mathrm{Out}(S_6) \simeq C_2$.

LEMMA 160. *There is a bijection between the conjugacy class of x and the quotient $G/Z_G(x)$. In particular, the number of conjugates of x is $[G : Z_G(x)]$.*

PROOF. Map $gZ_G(x) \to {}^g x$. This is <u>well-defined</u>: if $g' = gz$ with $z \in Z$ then ${}^{g'}x = {}^{gz}x = {}^g({}^z x) = {}^g x$. It is surjective: the conjugat${}^g x$ is the image of $gZ_G(x)$, and finally if ${}^g x = {}^{g'}x$ then $x = {}^{g^{-1}g}x = {}^{g^{-1}g'}x$ so $g^{-1}g' \in Z_G(x)$ and $g'Z_G(x) = g'Z(x)$. $\square$

THEOREM 161 (Class equation). *Let G be finite. Then*

$$\#G = \#Z(G) + \sum_{\{x\}} [G : Z_G(x)] ,$$

where the sum is over the non-central conjugacy classes.

PROOF. G is the disjoint union of the conjugacy classes. $\square$

3.2.2. Conjugacy of subgroups. We consider a variant on the previous construction.

DEFINITION 162. For $g \in G$, $H < G$ set ${}^g H = gHg^{-1} = \gamma_g(H)$.

LEMMA 163. *This is a group action of G on its set of subgroups.*

PROOF. Same: ${}^e H = eHe^{-1} = H$. Given ${}^g H$ we have ${}^{g^{-1}}{}^g H = H$. Finally, ${}^g\left({}^h H\right) = {}^{gh} H$. $\square$

EXAMPLE 164. The class of H is $\{H\}$ iff H is normal in G.

LEMMA 165. *Conjugacy of subgroups is an equivalence relation.*

PROOF. Same. $\square$

LEMMA 166. *There is a bijection between the conjugates of H and $G/N_G(H)$.*

PROOF. Same. $\square$

3.3. Orbits, stabilizers and counting (Lecture 13, 27/10/2015)

We now observe that the results of Section 3.2 depend only on the fact that conjugation is a group action, and not on the details of the action. The ultimate result is Proposition 173.

3.3.1. Orbits, stabilizers, and the orbit-stabilizer Theorem. Fix a group G acting on a set X.

DEFINITION 167. Say $x, y \in X$ are *in the same orbit* if there is $g \in G$ such that $gx = y$.

LEMMA 168. *This is an equivalence relation.*

PROOF. Repeat. $\square$

DEFINITION 169. The equivalence classes are called orbits.

REMARK 170. Why orbits? Consider action of $\mathbb{R}^+$ on phase space by time evolution (idea of Poincaré).

DEFINITION 171. Write $G \cdot x$ or $\mathcal{O}(x)$ for the orbit of $x \in X$. Write $G\backslash X$ for the set of orbits. For $x \in X$ set $\mathrm{Stab}_G(x) = \{g \in G \mid g \cdot x = x\}$.

LEMMA 172. $\mathrm{Stab}_G(x)$ *is a subgroup.*

PROOF. $e \cdot x = x$, if $g \cdot x = x$ then $g^{-1} \cdot x = x$ and if $gx = x$ and $hx = x$ then $(hg)x = h(gx) = hx = x$. $\square$

PROPOSITION 173 (Orbit-Stabilizer Theorem). *There is a bijection between the orbit $\mathcal{O}(x) \subset X$ and $G/\mathrm{Stab}_G(x)$. Moreover, the stabilizers of an orbit of G is a conjugacy class in of subgroups.*

PROOF. Same. $\square$

COROLLARY 174 (General class equation). *We have*

$$\#X = \sum_{\mathcal{O}(x) \in G\backslash X} [G : \mathrm{Stab}_G(x)] .$$

PROOF. X is the disjoint union of the orbits. $\square$

DEFINITION 175. $\mathrm{Fix}(G) = \{x \in X \mid \mathrm{Stab}_G(x) = G\}$.

COROLLARY 176. *Suppose G has order p^k and X is finite. Then $\#X \equiv \#\mathrm{Fix}(X)$ (p).*

PROOF. Every non-fixed point is an orbit of size at least 2, hence its stabilizer is a non-1 divisor of p^k so it is divisible by p. $\square$

EXAMPLE 177. Zagier's slick proof of Fermat's Theorem

3.4. Actions, orbits and point stabilizers (handout)

In this handout we gather a list of examples of group actions. We find the orbits, stabilizers,

3.4.1. G acting on G/H. Let G be a group, H a subgroup. The regular action of G on itself induces an action on the subsets of G.

- Let $C = xH$ be a coset in G/H and let $g \in G$. Then gC is also a coset: $gC = g(xH) = (gx)H$. Accordingly G acts on G/H.

(1) Orbits: for any two cosets xH, yH let $g = yx^{-1}$. Then $g(xH) = yx^{-1}xH = yH$ so there is only one orbit.
  - We say the action is *transitive*.

(2) Stabilizers: $\{g \mid gxH = xH\} = \{g \mid gxHx^{-1} = xHx^{-1}\} = \{g \mid g \in xHx^{-1}\} = xHx^{-1}$ $\mathrm{Stab}_G(xH) = xHx^{-1}$ – the point stabilizers are exactly the conjugates of H.

PROPOSITION 178. *Let G act on X. For $x \in X$ let $H = \mathrm{Stab}_G(x)$ and let $f\colon G/H \to \mathcal{O}(x)$ be the bijection $f(gH) = gx$ of Proposition 173.* Then f is a map of G-sets*: for all $g \in G$ and coset $C \in G/H$ we have*

$$f(g \cdot C) = g \cdot f(C)$$

where on the left we have the action of g on $C \in G/H$ and on the left we have the action of g on $f(C) \in \mathcal{O}(x) \subset X$.

3.4.2. $\mathrm{GL}_n(\mathbb{R})$ acting on $\mathbb{R}^n$.

- For a matrix $g \in G = \mathrm{GL}_n(\mathbb{R})$ and vector $\underline{v} \in \mathbb{R}^n$ write $g \cdot \underline{v}$ for the matrix-vector product. This is an action (linear algebra).

(1) Orbits: We know that for all g, $g\underline{0} = \underline{0}$ so $\{\underline{0}\}$ is one orbit. For all other non-zero vectors we have:

CLAIM 179. Let V be a vector space, $\underline{u}, \underline{v} \in V$ be two non-zero vectors. Then there is a linear map $g \in \mathrm{GL}(V)$ such that $g\underline{u} = \underline{v}$.

We need a fact from linear algebra

FACT 180. *Let V, W be vector spaces and let $\{\underline{u}_i\}_{i \in I}$ be a basis of V. Let $\{\underline{w}_i\}_{i \in I}$ be any vectors in W. Then there is a unique linear map $f\colon V \to W$ such that $f(\underline{u}_i) = \underline{w}_i$.*

PROOF OF CLAIM. Complete $\underline{u}, \underline{v}$ to a bases $\{\underline{u}_i\}_{i \in I}, \{\underline{v}_i\}_{i \in I}$ ($\underline{u}_1 = \underline{u}$, $\underline{v}_1 = \underline{v}$). There is a unique linear map $g\colon V \to V$ such that $g\underline{u}_i = \underline{v}_i$ (because $\{\underline{u}_i\}$ is a basis) and similarly a unique map $h\colon V \to V$ such that $h\underline{v}_i = \underline{u}_i$. But then for all i we have $(gh)\underline{v}_i = \underline{v}_i = \mathrm{Id}\,\underline{v}_i$ and $(hg)\underline{u}_i = \underline{u}_i = \mathrm{Id}\,\underline{u}_i$, so by the uniqueness prong of the fact we have $gh = \mathrm{Id} = hg$ and $g \in \mathrm{GL}(V)$. $\square$

(2) Stabilizers: clearly all matrices stabilizer zero. For other vectors we compute:

$$\mathrm{Stab}_{\mathrm{GL}_n(\mathbb{R})}(\underline{e}_n) = \left\{ g \mid g \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \right\} = \left\{ g = \begin{pmatrix} h & \underline{0} \\ \underline{u} & 1 \end{pmatrix} \mid h \in \mathrm{GL}_{n-1}(\mathbb{R}), \underline{u} \in \mathbb{R}^{n-1} \right\}.$$

EXERCISE 181. Show that the block-diagonal matrices $M=\left\{\begin{pmatrix} h & \underline{0} \\ \underline{0} & 1\end{pmatrix} \mid h\in \mathrm{GL}_{n-1}(\mathbb{R})\right\}$ are a subgroup of $\mathrm{GL}_n(\mathbb{R})$ isomorphic to $\mathrm{GL}_{n-1}(\mathbb{R})$. Show that the matrices $N=\left\{\begin{pmatrix} I_{n-1} & \underline{0} \\ \underline{u} & 1\end{pmatrix} \mid \underline{u}\in \mathbb{R}^{n-1}\right\}$ are a subgroup isomorphic to $\left(\mathbb{R}^{n-1},+\right)$. Show that $\mathrm{Stab}_{\mathrm{GL}_n(\mathbb{R})}\left(\underline{e}_n\right)$ is the semidirect product $M\ltimes N$.

3.4.3. $\mathrm{GL}_n(\mathbb{R})$ acting on pairs of vectors (assume $n\geq 2$ here).

EXERCISE 182. If G acts on X and G acts on Y then setting $g\cdot(x,y)=(g\cdot x,g\cdot y)$ gives an action of G on $X\times Y$.

We study the example where $G=\mathrm{GL}_n(\mathbb{R})$ and $X=Y=\mathbb{R}^n$.

(1) Orbits:
  (a) Clearly $(\underline{0},\underline{0})$ is a fixed point of the action.
  (b) If $\underline{u}\neq\underline{0}$, $\underline{v}\neq\underline{0}$, the previous discussion constructed g such that $g\underline{u}=\underline{v}$and hence $g\cdot(\underline{u},\underline{0})=(\underline{v},\underline{0})$ and $g\cdot(\underline{0},\underline{u})=(\underline{0},\underline{v})$. Since $G\cdot(\underline{u},\underline{0})\subset\mathbb{R}^n\times\{\underline{0}\}$, we therefore get two more orbits: $\{(\underline{u},\underline{0})\mid \underline{u}\neq 0\}$ and $\{(\underline{0},\underline{u})\mid\underline{u}\neq 0\}$.
  (c) We now need to understand when there is g such that $g\cdot(\underline{u}_1,\underline{u}_2)=(\underline{v}_1,\underline{v}_2)$. In hte previuos discussion we saw that if $\{\underline{u}_1,\underline{u}_2\}$ are linearly independent as are $\{\underline{v}_1,\underline{v}_2\}$ then completing to a basis will provide such g. Conversely, if $\{\underline{u}_1,\underline{u}_2\}$ are independent then so are $\{g\underline{u}_1,g\underline{u}_2\}$ for any invertible g (g preserves the vector space structure hence linear algebra properties like linear independence). We therefore have an orbit
$$\{(\underline{u}_1,\underline{u}_2)\mid \text{ the vectors are linearly independent}\}\,.$$
  (d) The case of linear dependence remains, so we need to consider the orbit of $(\underline{u}_1,\underline{u}_2)$ where both are non-zero and $\underline{u}_2=a\underline{u}_1$ for some scalar a, necessarily non-zero. But in that case $g\cdot(\underline{u}_1,\underline{u}_2)=(g\underline{u}_1,g(a\underline{u}_1))=(g\underline{u}_1,a(g\underline{u}_1))$ so we conclude that the orbit is contained in
$$\{(\underline{u}_1,a\underline{u}_1)\mid\underline{u}_1\neq\underline{0}\}\,.$$
  Conversely, this is an orbit because if $\underline{u}_1,\underline{u}_2$ are both non-zero then if $g\underline{u}_1=\underline{u}_2$ then $g\cdot(\underline{u}_1,a\underline{u}_1)=(\underline{v}_1,a\underline{v}_1)$.
  Summary: the orbits are $\{(\underline{0},\underline{0})\}$, $\{(\underline{u},\underline{0})\mid\underline{u}\neq 0\}$,$\{(\underline{0},\underline{u})\mid\underline{u}\neq 0\}$, $\{(\underline{u}_1,\underline{u}_2)\mid \dim\mathrm{Span}_F\{\underline{u}_1,\underline{u}_2\}=2$ and for each $a\in F^\times$ the set $\{(\underline{u}_1,a\underline{u}_1)\mid\underline{u}_1\neq\underline{0}\}$.

(2) Point stabilizers:
  (a) $(\underline{0},\underline{0})$ is fixed by the whole group.
  (b) $g(\underline{u},\underline{0})=(\underline{u},\underline{0})$ iff $g\underline{u}=\underline{u}$, so this is the case solved before. Similarly for $g\cdot(\underline{u},a\underline{u})=(\underline{u},a\underline{u})$ which holds iff $g\underline{u}=\underline{u}$.
  (c) $g\left(\underline{e}_{n-1},\underline{e}_n\right)=\left(\underline{e}_{n-1},\underline{e}_n\right)$ holds iff the last two columns of g are $\underline{e}_{n-1},\underline{e}_n$ so
$$\mathrm{Stab}_{\mathrm{GL}_n(\mathbb{R})}\left(\underline{e}_{n-1},\underline{e}_n\right)=\left\{g=\begin{pmatrix} h & 0\\ y & I_2\end{pmatrix}\mid h\in\mathrm{GL}_{n-2}(\mathbb{R}),y\in M_{2,n-2}(\mathbb{R})\right\}.$$

EXERCISE 183. Show that the block-diagonal matrices $M=\left\{\begin{pmatrix} h & \underline{0} \\ \underline{0} & I_2\end{pmatrix} \mid h\in \mathrm{GL}_{n-2}(\mathbb{R})\right\}$ are a subgroup of $\mathrm{GL}_n(\mathbb{R})$ isomorphic to $\mathrm{GL}_{n-2}(\mathbb{R})$. Show that the matrices $N=\left\{\begin{pmatrix} I_{n-2} & \underline{0} \\ y & 1\end{pmatrix} \mid y\in M_{2,n-2}(\mathbb{R})\right\}\simeq$

are a subgroup isomorphic to $\left(\mathbb{R}^{2(n-2)},+\right)$. Show that $\mathrm{Stab}_{\mathrm{GL}_n(\mathbb{R})}\left(\underline{e}_{n-1},\underline{e}_n\right)$ is the semidirect product $M \ltimes N$.

3.4.4. $\mathrm{GL}_n(\mathbb{R})$ **and** $\mathrm{PGL}_n(\mathbb{R})$ **acting on** $\P^{n-1}(\mathbb{R})$**.**

DEFINITION 184. Write $\mathbb{P}^{n-1}(\mathbb{R})$ for the set of 1-dimensional subspaces of $\mathbb{R}^n$ (this set is called "projective space of dimension $n-1$").

- Let $L \in \mathbb{P}^{n-1}(\mathbb{R})$ be a line in $\mathbb{R}^n$ (one-dimensional subspace. Let $g \in \mathrm{GL}_n(\mathbb{R})$. Then $g(L) = \{g\underline{v} \mid \underline{v} \in L\}$ is also a line (the image of a subspace is a subspace, and invertible linear maps preserve dimension), and this defines an action of $\mathrm{GL}_n(\mathbb{R})$ on $\mathbb{P}^{n-1}(\mathbb{R})$ (a restriction of the action of $\mathrm{GL}_n(\mathbb{R})$ on all subsets of $\mathbb{R}^n$ to the set of subsets which are lines).

(1) The action is transitive: suppose $L = \mathrm{Span}\{\underline{u}\}$ and $L' = \mathrm{Span}\{\underline{v}\}$ for some non-zero vectors $\underline{u}, vv$. Then the element g such that $g\underline{u} = \underline{v}$ will also map $gL = L'$.
(2) Suppose $L = \mathrm{Span}\{\underline{e}_n\}$. Then $gL = L$ means $g\underline{e}_n$ spans L, so $g\underline{e}_n = a\underline{e}_n$ for some non-zero a. It follows that

$$\mathrm{Stab}_{\mathrm{GL}_n(\mathbb{R})}(F \cdot \underline{e}_n) = \left\{ g = \begin{pmatrix} h & 0 \\ \underline{u} & a \end{pmatrix} \mid h \in \mathrm{GL}_{n-1}(\mathbb{R}), a \in \mathbb{R}^\times\ \underline{u} \in \mathbb{R}^{n-1} \right\}.$$

- Repeat Exercize 181 from before, now with $M = \left\{ \begin{pmatrix} h & 0 \\ \underline{0} & a \end{pmatrix} \mid h \in \mathrm{GL}_{n-1}(\mathbb{R}), a \in \mathbb{R}^\times \right\} \simeq \mathrm{GL}_{n-1}(\mathbb{R}) \times \mathbb{R}^\times$.

This can be generalized. Write

$$\mathrm{Gr}(n,k) = \{L \subset \mathbb{R}^n \mid L \text{ is a subspace and } \dim_{\mathbb{R}^n} L = k\}.$$

Then $\mathrm{GL}_n(\mathbb{R})$ still acts here (same proof), the action is still transitive (for any L, L', take bases $\{\underline{u}_i\}_{i=1}^k \subset L$, $\{\underline{v}_i\}_{i=1}^k \subset L'$, complete both to bases of $\mathbb{R}^n$ and get a map), and the stabilizer will have the form $M \ltimes N$ with $M \simeq \mathrm{GL}_{n-k}(\mathbb{R}) \times \mathrm{GL}_k(\mathbb{R})$ and $N \simeq \left(M_{k,n-k}(\mathbb{R}),+\right)$.

3.4.5. $\mathrm{O}(n)$ **acting on** $\mathbb{R}^n$**.** Let the orthogonal group $\mathrm{O}(n) = \{g \in \mathrm{GL}_n(\mathbb{R}) \mid g^t g = \mathrm{Id}\}$ act on $\mathbb{R}^n$.

- This is an example of *restriction* the action of $\mathrm{GL}_n(\mathbb{R})$ to a subgroup.

(1) Orbits: we know that if $g \in \mathrm{O}(n)$ and $\underline{v} \in \mathbb{R}^n$ then $\|g\underline{v}\| = \|\underline{v}\|$. Conversely, for each $a \geq 0$ $\{\underline{v} \in \mathbb{R}^n \mid \|vv\| = a\}$ is an orbit. When $a = 0$ this is clear (just the zero vector) and otherwise let $\underline{u}, \underline{v}$both have norm a. Let $\underline{u}_1 = \frac{1}{a}vu$, $\underline{v}_1 = \frac{1}{a}\underline{v}$ and complete $\underline{u}_1, \underline{v}_1$ to orthonormal bases $\{\underline{u}_i\}, \{\underline{v}_i\}$ respectively. Then the unique invertible linear map $g \in \mathrm{GL}_n(\mathbb{R})$ such that $g\underline{u}_i = \underline{v}_i$ is orthogonal (linear algebra exercize) and in particular we have $g \in \mathrm{O}(n)$ such that $g\underline{u}_1 = \underline{v}_1$ and then $g\underline{u} = g(a\underline{u}_1) = ag\underline{u}_1 = a\underline{v}_1 = vv$.

3.4.6. $\mathrm{Isom}(\mathbb{R}^n)$ **acting on** $\mathbb{R}^n$**.** Let $\mathrm{Isom}(\mathbb{R}^n)$ be the *Euclidean group*: the group of all *ridig motions* of $\mathbb{R}^n$ (maps $f\colon \mathbb{R}^n \to \mathbb{R}^n$ which preserve distance, in that $\|f(\underline{u}) - f(\underline{v})\| = \|\underline{u} - \underline{v}\|$).

(1) The action is transitive: for any fixed $\underline{a} \in \mathbb{R}^n$ the *translation* $T_{\underline{a}}\underline{x} = \underline{x} + \underline{a}$ preserves distances, and for any $\underline{u}, \underline{v}$ we have $T_{\underline{v}-\underline{u}}(\underline{u}) = \underline{v}$.
(2) The point stabilizer of zero is exactly the orthogonal group!

PROOF. Let $f \in \mathrm{Isom}(\mathbb{R}^n)$ satisfy $f(\underline{0}) = \underline{0}$. We show that f preserves inner products. For this first note that for any $\underline{x}$,

$$\|f(\underline{x})\| = \|f(\underline{x}) - \underline{0}\| = \|f(\underline{x}) - f(\underline{0})\| = \|\underline{x} - \underline{0}\| = \|\underline{x}\| \; .$$

Second since $\left\|\underline{x} - \underline{y}\right\|^2 = \|\underline{x}\|^2 + \left\|\underline{y}\right\|^2 - 2\left\langle \underline{x}, \underline{y}\right\rangle$ we have the *polarization identity*

$$\left\langle \underline{x}, \underline{y}\right\rangle = \frac{1}{2}\left[\|\underline{x}\|^2 + \left\|\underline{y}\right\|^2 - \left\|\underline{x} - \underline{y}\right\|^2\right]$$

so that

$$\begin{aligned}
\left\langle f(\underline{x}), f(\underline{y})\right\rangle &= \frac{1}{2}\left[\|f(\underline{x})\|^2 + \left\|f(\underline{y})\right\|^2 - \left\|f(\underline{x}) - f(\underline{y})\right\|^2\right] \\
&= \frac{1}{2}\left[\|\underline{x}\|^2 + \left\|\underline{y}\right\|^2 - \left\|\underline{x} - \underline{y}\right\|^2\right]
\end{aligned}$$

Now let $\{\underline{e}_i\}_{i=1}^n$ be the standard orthonormal basis. It follows that $\underline{u}_i = f(\underline{e}_i)$ also form an orthonormal basis, and we let $g \in \mathrm{O}(n)$ be the map such that $g\underline{e}_i = \underline{u}_i$. Finally, let $\underline{x} \in \mathbb{R}^n$ and let $a_i = \langle \underline{x}, \underline{e}_i\rangle$. Then $\underline{x} = \sum_i a_i \underline{e}_i$ and since

$$\langle f(\underline{x}), \underline{u}_i\rangle = \langle f(\underline{x}), f(\underline{e}_i)\rangle = \langle \underline{x}, \underline{e}_i\rangle = a_i$$

that also

$$f(\underline{x}) = \sum_i a_i \underline{u}_i = \sum_i a_i g \underline{e}_i = g\left(\sum_i a_i \underline{e}_i\right) = g\underline{x}$$

so that f agrees with g. $\square$

EXERCISE 185. Let $V = \left\{T_{\underline{a}} \mid \underline{a} \in \mathbb{R}^n\right\} \subset \mathrm{Isom}(\mathbb{R}^n)$ be the group of translations. This is a subgroup isomorphic to $\mathbb{R}^n$, and $\mathrm{O}(n)$ is the semidirect product $\mathrm{O}(n) \ltimes V$.

EXERCISE 186. The orbits of $\mathrm{Isom}(\mathbb{R}^n)$ on the space of pairs $\mathbb{R}^n \times \mathbb{R}^n$ are exactly the sets $D_a = \left\{(\underline{x}, \underline{y}) \mid \left\|\underline{x} - \underline{y}\right\| = a\right\}$ $(a \geq 0)$.

CHAPTER 4

p-Groups and Sylow's Theorems

4.1. p groups (Lecture 14, 29/10/2015)

We start with a partial converse to Lagrange's Theorem.

THEOREM 187 (Cauchy 1845). *Suppose that $p|\#G$. Then G has an element of order p.*

PROOF. Let G be a minimal counterexample. Consider the class equation

$$\#G = \#Z(G) + \sum_{i=1}^{h} [G : Z_G(g_i)]$$

$\{g_i\}_{i=1}^{h}$ are representatives for the non-central conjugacy classes. Then $Z_G(g_i)$ are proper subgroups, so by induction their order is prime to p. It follows that their index is divisible by p, so $p|\#Z(G)$ as well, and this group is non-trivial. Now let $x \in Z(G)$ be non-trivial. If the order of x is divisible by p we are done. Otherwise, the subgroup $N = \langle x \rangle$ is central, hence normal, and of order prime to p. Then Z/N has order divisible by p, and by induction an element $\bar{y}$ of order p. Let $y \in Z$ be any preimage. Then the order of y in Z is a multiple of the order of y in Z/N, hence a multiple of p and we are done. □

Here's another proof:

PROOF. Let $X = \left\{\underline{g} \in G^p \mid \prod_{i=1}^{p} g_i = e\right\}$. Then $\#X = (\#G)^{p-1}$ is divisible by p. The group C_p acts on X by permuting the coordinates. Let $Y \subset X$ be the set of fixed points. Then $\#Y \equiv \#X\,(p)$, so $p|\#Y$. But Y is in bijection with the set of elements of order divisible by p, which is non-empty since e is there. □

COROLLARY 188. *The number of elements of order exactly p is congruent to -1 mod p (in particular, it is non-zero).*

COROLLARY 189. *Let G be a finite group, p a prime. Then every element of G has order a power of p iff the order of G is a power of p.*

DEFINITION 190. Call G a p-group if every element of G has order a power of p.

Observe that if G is a finite p-group then the index of every subgroup is a power of p. It follows that every orbit of a G-action has either size 1 or size divisible by p. By the class equation we conclude that if G is a finite p-group and X is a finite G-set, we have:

$$|X| \equiv |\{x \in X \mid \mathrm{Stab}_G(x) = G\}| \mod p\,. \tag{4.1.1}$$

THEOREM 191. *Let G be a finite p-group. Then $Z(G) \neq 1$.*

PROOF. Let G act on itself by conjugation. The number of conjugacy classes of size 1 must be divisible by p. □

LEMMA 192. *If $G/Z(G)$ is cyclic it is trivial and G is commutative.*

PROOF. Suppose that $G/Z(G)$ is generated by the image of $g \in G$. We first claim that every $x \in G$ is of the form $x = g^k z$ for some $k \in \mathbb{Z}$, $z \in Z(G)$. Indeed, the image of x mod $Z(G)$ is in the cyclic subgroup generated by g, so there is k such that

$$x \equiv g^k \,(Z(G))$$

which means

$$x = g^k z\,.$$

Now suppose that $x = g^k z$ and $y = g^l w$ where $k,l \in \mathbb{Z}$ and $z,w \in Z(G)$. Then

$$\begin{aligned} xy &= g^k z g^l w = g^k g^l z w = g^{k+l} z w \\ yx &= g^l w g^k z = g^l g^k w z = g^{k+l} z w\,. \end{aligned}$$

□

PROPOSITION 193 (Groups of order p^2, p^3). .

(1) Let G have order p^2. Then G is abelian, in fact isomorphic to one of C_{p^2} and $C_p \times C_p$.
(2) Let G be an abelian group of order p^3. Then G is one of C_{p^3}, $C_{p^2} \times C_p$, $C_p \times C_p \times C_p$.
(3) Let G be non-commutative, of order p^3. Then $Z(G) \simeq C_p$ and $G/Z(G) \simeq C_p \times C_p$.

PROOF.

(1) The order of $Z(G)$ is a divisor of p^2, not equal to 1. If it was p then $G/Z(G)$ would have order p and be cyclic. It follows that $Z(G) = G$ and G is abelian. If G has an element of order p^2 then $G \simeq C_{p^2}$. Otherwise the order of each element of G divides p.
   (a) Let $x \in G$ have order p, and let $y \in G - \langle x \rangle$. Then $y \neq e$ so y also has order p. Consider the map $(\mathbb{Z}/p\mathbb{Z})^2 \to G$ given by $f(a,b) = x^a y^b$. This is a well-defined homomorphism, which is injective and surjective.
   (b) Write the group law of G additively. For $k \in \mathbb{Z}$, $x \in G$ write $k \cdot g$ for $g^k = g + \cdots + g$ (k times). Since $g^p = e$ this is really defined for $k \in \mathbb{Z}/p\mathbb{Z}$. This endows G with the structure of a vector space over $\mathbb{F}_p$. It has p^2 elements so dimension 2, and fixing a basis gives an identificationwith $\left(\mathbb{F}_p^2, +\right) \simeq C_p^2$.

(2) We need to identify each possibility. There is $x \in G$ of order p^3 $G \simeq C_{p^3}$. If every non-identity $x \in G$ has order p then the argument of (1) gives $G \simeq C_p \times C_p \times C_p$. Otherwise there are some elements of order p^2, but none of order p^3. Now the map $g \mapsto g^p$ is a homomorphism $G \to G$. Its kernel is the elements of order dividing p (must be non-trivial!) so its image is a proper subgroup, to be detnoed G^p. This subgroup is non-trivial because the pth power of an element of order p^2 has order p. Suppose first G^p has order p^2. It can't be $\simeq C_{p^2}$ (if $x^p \in G^p$ had order p^2 then x has order p^3 and G would be cyclic) so it would be $C_p \times C_p$. Now let $x \in G$ have order p^2. Then $x^p \in G^p$ is non-trivial. By part (a) there is $y \in C^p$ such that $G^p = \langle x^p \rangle \langle y \rangle$. Then $\langle y \rangle$ is disjoint from $\langle x \rangle$ and we get $G = \langle x \rangle \langle y \rangle \simeq C_{p^2} \times C_p$, a contradiction (since for this group $G^p \simeq C_p$). We conclude that $G^p \simeq C_p$. Let $x \in G$ have order p^2, so that x^p generate G^p. Let $y \in G \setminus \langle x \rangle$. If y has order p we are done. Suppose y has order p^2. Then $y^p \in G^p = \langle x^p \rangle$ is non-trivia, hence of the form x^{kp} for some k prime to p. Let $\bar{k}$ be inverse to k mod p. Then $z = y^{\bar{k}}$ has $\langle z \rangle = \langle y \rangle$so

it still has order p^2 and still lies outside $\langle x\rangle$. Finally, by contruction $z^p = x^p$ so $zx^{-1} \notin \langle x\rangle$ has order p and we are done.

□

4.2. Example: groups of order pq (Lecture 15, 3/11/2015)

4.2.1. Classification of groups of order 6. To start with, we know C_6, S_3, D_6. C_6 is not isomorphic to the other two (it is abelian, they are not). $S_3 \simeq D_6$. For this note that D_6 is the isometry group of a the complete graph on 3 vertices, so isomorphic to S_3. We now show that C_6, D_6 are the only two isomorphism classes at order 6.

REMARK 194. For every n we have the group C_n, so that group must be there.

Accordingly, fix a group G of order 6. By Cauchy's Theorem 187, is it has a subgroup P of order 2, a subgroup Q of order 3. Note that the subgroup $P \cap Q$ must have order dividing both $2,3$ so it is trivial.

LEMMA 195. *Let $P, Q < G$ satisfy $P \cap Q = \{e\}$. Then the (set) map $P \times Q \to PQ$ given by $(x,y) \mapsto xy$ is a bijection.*

PROOF. If $xy = x'y'$ then $x^{-1}x' = y(y')^{-1} \in P \cap Q = \{e\}$so $x = x'$ and $y = y'$. □

REMARK 196. In general there is a bijection between $PQ \times P \cap Q \leftrightarrow P \times Q$.

It follows that $\#PQ = \#P \times \#Q = 6 = \#G$ so $G = PQ$.

CLAIM. Q is normal (Can simply say that Q has index 2, but we give a different argument which generalizes).

PROOF. Let $\mathcal{C} = \left\{gQg^{-1} \mid g \in G\right\}$ be the congugacy class of Q. Since $G = PQ$ we have

$$\begin{aligned} \mathcal{C} &= \left\{xyQy^{-1}x^{-1} \mid x \in P, y \in Q\right\} \\ &= \left\{xQx^{-1} \mid x \in P\right\} \\ &= \left\{Q, aQa^{-1}\right\} \end{aligned}$$

if we parametrize $P = \{1,a\}$. Suppose that $Q' = aQa^{-1} \neq Q$. Now $Q \simeq Q' \simeq C_3$, and $Q' \cap Q$ is a subgroup of both. It's not of order 3 (this would force $Q = Q'$) so it is trivial. It now follows from the Lemma that $\#QQ' = 9 > \#G$, a contrdiction. □

It follows that $G = PQ$ where Q is a normal subgroup and $P \cap Q = \{e\}$, that is $G = P \ltimes Q$.
Note that if $xy, x'y' \in PQ$ then

$$(x'y')(xy) = \left[x'x\right]\left[(x^{-1}y'x)y\right].$$

In particular, to the product structure on $P \ltimes Q$ is determined by the conjugation action of P on Q. Parametrizing $P = \{e,a\}$, the action of e is trivial, so it remains to determine aya^{-1} for $y \in Q$. We note that $(aya^{-1})^2 = aya^{-1}aya^{-1} = ay^2a^{-1}$ so parametrizing $Q = \left\{1, b, b^2\right\}$ it remains to choose aba^{-1}. This must be one of b, b^2 (non-identity elements are not conjugate to the identity), so there are most two isomorphism classes.

REMARK 197. Having constructed two non-isomorphic groups, we are done, but we'd like to discover them anew.

Case 1. If $aba^{-1} = b$ then a, b commute, so P, Q commute, so $G \simeq P \times Q$ (internal direct product). But this means $G \simeq C_2 \times C_3 \simeq C_6$ by the Chinese Remainder Theorem 31.

Case 2. If $aba^{-1} = b^2 = b^{-1}$ then also $ab^2a = (b^2)^{-1}$ and we have D_6: $\{1, b, b^2\}$ are the rotations, and a is the reflection.

4.2.2. Classification of groups of order pq**.** Let $p < q$ be distinct primes (the case $p = q$ was dealt with before). Fix a group G of order pq. By Cauchy's Theorem 187, is it has a subgroup P of order p, a subgroup Q of order q. Note that the subgroup $P \cap Q$ must have order dividing both p, q so it is trivial.

Again by Lemma 195 we have $\#PQ = pq = \#G$ so $G = PQ$.

CLAIM. Q is normal (now$[G : Q] = p$ can be greater than 2).

PROOF. Let $\mathcal{C} = \{gQg^{-1} \mid g \in G\}$ be the congugacy class of Q. Since $G = PQ$ we have

$$\begin{aligned} \mathcal{C} &= \{xyQy^{-1}x^{-1} \mid x \in P, y \in Q\} \\ &= \{xQx^{-1} \mid x \in P\} . \end{aligned}$$

In other words, $\mathcal{C}$ is a single orbit for the action of P by conjugation. By the orbit-stabilizer theorem (Lemma 195), this must have size dividing $\#P = p$ so either 1 or p. Assume Q not normal, so the size is p. Now consider the action of Q on $\mathcal{C}$ by conjugation. Each Q-orbit can have size q or 1, but since $q > p$ there is no room for an orbit of size 1. We conclude that every $Q' \in \mathcal{C}$ is normalized by Q.

Since $p \geq 2$ there is some $Q' \in C_c$ different than Q, and again we have $Q \cap Q' = \{e\}$ since these groups are different, and hence $\#(QQ') = q^2 > pq = \#G$, a contradiction. □

It follows that $G = PQ$ where Q is a normal subgroup and $P \cap Q = \{e\}$, that is $G = P \ltimes Q$. Again the product structure on $P \ltimes Q$ is determined by the conjugation action of P on Q. Let a, b generate P, Q respectively. Then $aba^{-1} = b^k$ for some k. We claim that this fixed the whole action.

First, by induction on j, we have $ab^ja^{-1} = (b^j)^k$ so $aya^{-1} = y^k$ for all $y \in Q$. Second, by induction on i, $a^iya^{-i} = y^{(k^i)}$ (composition of homomorphisms). We see that it remains to choose k.

Note that $a^p = e$ and that $b = a^pba^{-p} = b^{k^p}$ so we must have $k^p \equiv 1\,(q)$, that is k must have order dividing p in $(\mathbb{Z}/q\mathbb{Z})^\times$.

Case 1. If $aba^{-1} = b$ then a, b commute, so P, Q commute and $G \simeq C_p \times C_q \simeq C_{pq}$ by the Chinese Remainder Theorem 31.

Case 2. If $aba^{-1} = b^k$ for $k \not\equiv 1\,(q)$. Then k has order exactly p in $(\mathbb{Z}/q\mathbb{Z})^\times$. Lagrange's Theorem then forces $p | q-1$ so $q \equiv 1\,(p)$. Conversely, suppose that this is the case. Then by Cauchy's theorem, $(\mathbb{Z}/q\mathbb{Z})^\times$ has elements of order p, so a non-commutative semidirect product exists. Since $(\mathbb{Z}/q\mathbb{Z})^\times$ is cyclic, the elements of order p form a unique cyclic subgroups, so they are all powers of each other. In particular, replacing a with a power gives an isomorphism, and we see there is only one isomorphism class of non-commutative groups in this case, of the form:

$$\left\langle a, b \mid a^p = b^q = e, aba^{-1} = q^k \right\rangle$$

where k is an element of order p in $(\mathbb{Z}/q\mathbb{Z})^\times$.

4.2.3. More detail, and examples (Lecture 16, 5/11/2015).

- Explicitely parametrize G as $\left\{a^i b^j \mid i \mod p, j \mod q\right\}$.
  - Every hom $C_n \to C_n$ must be of the form $x \mapsto x^k$. Composing two such gives the hom $x \mapsto x^{kl}$, so have an *automorphism* if k is invertible mod q. In other words, $\mathrm{Aut}(C_n) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.
  - For any k mod q can try to define the product
  $$\left(a^{i'}b^{j'}\right)\left(a^i b^j\right) = a^{i'+i}b^{j'k^{-i}+j}$$
  where k^{-r} is the power in $\mathbb{Z}/q\mathbb{Z}$.
  - Makes sense only if $k^p \equiv 1\,(q)$ so that a^p acts correctly. This can happen only if $q \equiv 1\,(p)$.
  - If $q \equiv 1\,(p)$ then by Cauchy there are elements of order p and we can make the definition.
  - If we replace k by k^r we can replace a with a^r (with $a^{\bar{r}}$) to get isomorphism of the semidirect products, so only one semidirect product
- Understand in detail how a group of order 3 cannot act on a group of order 5.
- Understand in details that the two actions of C_3 on C_7 give isomorphic groups $C_3 \ltimes C_7$.

4.3. Sylow's Theorems (Lectures 16–18)

We substantially strengthen Cauchy's Theorem.

4.3.1. The Sylow Theorems (Lecture 17, 10/11/2015). Fix a group G of order n, and let $n = p^r m$ where $p \nmid m$.

THEOREM 198 (Sylow I). *If $p^i | n$ then G contains a subgroup of order p^i.*

PROOF. By induction on i, the case $i = 0$ being trivial. Accordingly let p^{i+1} divide the order of G, and let $H < G$ be a subgroup of order p^i. Let H act from the left on G/H. Since H is a p-group, $\#\mathrm{Fix}(H) \equiv \#(G/H)\ (p)$, so $p | \#\mathrm{Fix}(H)$. Now $gH \in \mathrm{Fix}(H)$iff for all $h \in H$ we have
$$hgH = gH \iff hgHg^{-1} = gHg^{-1} \iff h \in gHg^{-1}$$
so $gH \in \mathrm{Fix}(H)$ iff $H \subset gHg^{-1}$. Since these groups have the same order, we see that $gH \in \mathrm{Fix}(H)$ iff $g \in N_G(H)$, so $\mathrm{Fix}(H) = N_G(H)/H$. It follows that the group $N_G(H)/H$ has order divisible by p. By Cauchy's Theorem (Theorem 187), it has a subgroup C of order p, whose inverse image in $N_G(H)$ has order $p \cdot p^i = p^{i+1}$. □

REMARK 199. Note that we actually showed that if G contains a subgroup H of order p^i, and if $[G : H]$ is divisible by p^j, then H is contained in a subgroup of order p^{i+j}.

COROLLARY 200. *Then every maximal (by inclusion) p-subgroup of G has order p^r.*

DEFINITION 201. A maximal p-subgroup of G is called a *p-Sylow subgroup* of G. We write $\mathrm{Syl}_p(G)$ for the set of such subgroup and $n_p(G) = \#\mathrm{Syl}_p(G)$ for their number.

Note that a subgroup conjugate to a Sylow subgroup is a again a Sylow subgroup.

LEMMA 202. *Let P be a normal p-Sylow subgroup of G. Then P contains every p-subgroup of G, and in particular is the* unique *p-Sylow subgroup.*

PROOF. Let P' be any p-subgroup of G. Then PP' is a p-subgroup of G containing P, hence equal to P. It follows that $P' < P$. $\square$

THEOREM 203 (Sylow II,III). *The p-Sylow subgroups of G are all conjugate (in particular, $n_p(G)|n$). Furthermore, $n_p(G) \equiv 1\,(p)$ (so actually $n_p(G)|m$).*

PROOF. Let P be a p-Sylow subgroup, and consider the action of P on $\mathrm{Syl}_p(G)$ by conjugation. Then P fixes $P' \in \mathrm{Syl}_p(G)$ iff $P < N_G(P')$. This would make both P, P' be p-Sylow subgroups of $N_G(P')$, so by the Lemma $P = P'$. It follows that P has a unique fixed point, so $n_p(G) \equiv 1$.

Now let $\{P^g\}_{g\in G} \subset \mathrm{Syl}_p(G)$ be the set of p-Sylow subgroups conjugate to P. The size of this set is $[G : N_G(P)] \Big| [G : P]$ and is therefore prime to p (in fact, it is $\equiv 1\,(p)$ by the previous argument). Let P' be any p-Sylow subgroup. Then P' acts on $\{P^g\}_{g\in G}$ by conjugation; the number of fixed points is prime to p, and hence is non-zero. But the only fixed point of P' on $\mathrm{Syl}_p(G)$ is P' itself, so P' is conjugate to P. It follows that $n_p(G) = [G : N_G(P)]$, which divides n. $\square$

REMARK 204. If $n = p^k m$ with $p \nmid m$, then we actually saw $n_p(G) | [G : P] = m$.

4.3.2. Applications I (Lecture 18, 12/11/2015).

EXAMPLE 205. The only groups of order 12 are C_{12}, $C_2 \times C_6$, A_4, $C_2 \times S_3$ and $C_4 \ltimes C_3$.

PROOF. G be a group of order 12. Then $n_2(G)|3$, so $n_2(G) \in \{1,3\}$, and $n_3(G)|4$ while $\equiv 1\,(3)$ so $n_3(G) \in \{1,4\}$.

Case 1. $n_3(G) = 4$. Then the action of G by conjugation on $\mathrm{Syl}_3(G)$ gives a homomorphism $G \to S_4$. We have $N_G(P_3) = P_3$ and since this isn't normal and has no non-trivial subgroups, the kernel of the map is trivial. The group G contains 8 elements of order 3, and S_4 has $2\binom{4}{3} = 8$ such elements, so the image contains all elements of order 3, hence the subgroup A_4 generated by them. But A_4 has order 12, so $G \simeq A_4$

Case 2. $n_3(G) = 1$. Then $G \simeq P_2 \ltimes P_3$, and it remains to classify the actions of a group of order 4 on a group of order 3.

- *Case* i. The action is trivial ($G \simeq P_2 \times P_3$). Then either $G \simeq C_4 \times C_3 \simeq C_{12}$ or $G \simeq C_2 \times C_2 \times C_3$. Here $n_2(G) = 1$.
- *Case* ii. The action is non-trivial and $P_2 \simeq V$. Since $\mathrm{Aut}(C_3) \simeq C_2$, we can write $V \simeq K \times C_2$ where K is the kernel of the action. Then $G \simeq K \times (C_2 \ltimes C_3) \simeq C_2 \times S_3$. Here $n_2(G) = 3$ since P_2 does not commute with P_3.
- *Case* iii. The action is non-trivial and $P_2 \simeq C_4$. Since there is a unique non-trivial homomorphism $C_4 \to C_2$ (reduction mod 2), there is a unique semidirect product $C_4 \ltimes C_3$. Here also $n_2(G) = 3$.

$\square$

EXAMPLE 206. There is no simple group of order 30.

PROOF. Let G be a simple group of order 30. Numerology gives $n_3 \in \{1,10\}$ and $n_5(G) \in \{1,6\}$, but can't have a unique p-Sylow subgroup, so $n_3(G) = 10$, $n_5(G) = 6$. This means G has 20 elements of order 2, 24 elements of order 5, which add up to more than 30 elements. $\square$

4.3.3. Applications II (Lecture 19, 17/11/2015).

EXAMPLE 207. Let G be a simple group of order 60. Then $G \simeq A_5$

PROOF. Numerology gives $n_2(G) \in \{1,3,5,15\}$, $n_3(G) \in \{1,4,10\}$ and $n_5(G) \in \{1,6\}$.

Can't have $n_p(G) = 1$ by simplicity. In fact, can't have $n_p(G) \leq 4$ since a hom to S_4 would have kernel, so have

$$n_2 \in \{5,15\}\,, n_3 = 10, n_5 = 6\,.$$

In particular, there are $10 \cdot (3-1) = 20$ elements of order 3 and $6 \cdot (5-1) = 24$ elements of order 4.

Case 1. $n_2(G) = 5$. Then the action of G by conjugation on $\mathrm{Syl}_3(G)$ gives a homomorphism $G \to S_5$. The kernel is a proper subgroup of any P_3, so is trivial. The image contains 20 elements of order 3, while S_5 has $\frac{5\cdot 4\cdot 3}{3} = 20$ such, so it contains all of them. They generate A_5, so the image is A_5.

Case 2. $n_2(G) = 15$. We have at most $60-20-24-1 = 15$ non-identity 2-elements, which means that the 2-Sylow subgroups must intersect. Accordingly let $x \in G$ be a non-identity element belonging to two distinct 2-Sylow subgroups. Then $C_G(x)$ properly contains a 2-Sylow subgroup, its index properly divides 15 (but isn't 1 since $Z(G)$ is normal). This gives an action on a set of size 3 or 5. The first case is impossible.

$\square$

EXAMPLE 208 (PS9). No group of order p^2q is simple.

CHAPTER 5

Finitely Generated Abelian Groups

5.1. Statements: Lecture 20, 19/11/2015

5.1.1. Prime factorization. Let A be a finite Abelian group of order n. For each $p|n$ let

$$A_p = A[p^\infty] = \bigcup_{j=0}^{\infty} A[p^j] = \left\{a \in A \mid \exists j : p^j a = 0\right\} .$$

This is a subgroup (increasing union of subgroups) containing all p-elements, hence the unique p-Sylow subgroup. By PS9 we have

$$A \simeq \prod_p A_p \,,$$

and the A_p are unique. Thus, to classify finite abelian groups it's enough to classify finite abelian p-groups.

5.1.2. Example: groups of order 8. Order 8: if some element has order 8, we have C_8. Otherwise, find an element of order 4. This gives all elemetns of order 4 mod elemetns of order 2, so find another element of order 2 and get $C_4 \times C_2$. If every element has order 2 we have C_2^3.

5.1.3. Theorems.

THEOREM 209 (Classification of finite abelian groups). *Every finite abelian group can be written as a product of cyclic p-groups, uniquely up to permutation of the factors.*

COROLLARY 210 (Invariant factors). *Every finite abelian group can be uniquely written in the form $\prod_{j=1}^{d} C_{d_j}$ with the* invariant factors $d_1|d_2|\cdots|d_r$.

What about infinite groups? We call a group *finitely generated* if it has a finite generating set (for example, any finite group is).

THEOREM 211 (Fundamental theorem of finitely generated abelian groups). *Let A be a finitely generated abelian group. Then $A \simeq \mathbb{Z}^r \times A_{tors}$ for a unique integer r, the* free rank *of A.*

5.1.4. Examples.

5.2. Proofs

The material in this section is not examinable.

5.2.1. Uniqueness in the finite case. By the reduction before, enough to consider abelian p-groups.

PROPOSITION 212. *Suppose* $\prod_{i=1}^{r} C_{p^{e_i}} \simeq \prod_{j=1}^{s} C_{p^{f_j}}$. *Then* $r = s$ *and* $f_j = e_{\sigma(j)}$ *for some* $\sigma \in S_r$.

PROOF. Let $A \simeq \prod_{i=1}^{r} C_{p^{e_i}}$. Then $a \in A$ has order p iff has order p in each factor, so $A[p] \simeq C_p^r$; in particular r is uniquely defined and $r = s$. Next, we have

$$A/A[p] \simeq \prod_{i=1}^{r} \left(C_{p^{e_i}}/C_p\right) \simeq \prod_{e_i > 1} C_{p^{e_i - 1}}$$

and for the same reason

$$A/A[p] \simeq \prod_{f_j > 1} C_{p^{f_j - 1}}\,.$$

By induction on the order of A, both products have the same number of factors, so in particular $r' = \#\{i \mid e_i > 1\} = \#\left\{i \mid f_j > 1\right\}$ so both products have the same number of factors isomorphic to C_p $(r - r')$. Ordering them to be last, we also have $\sigma \in S_{r'}$ such that $f_j - 1 = e_{\sigma(j)} - 1$ and this shows that the e_i and f_j are the same up to reordering. $\square$

5.2.2. Existence in the finite case. By the reduction before, enough to consider abelian p-groups. In this section we write the group operation additively.

PROPOSITION 213. *Let A be a finite abelian p-group. Then A is isomorphic to a product of cyclic groups.*

Let e be maximal such that A has elements of order p^e, and consider the map $A \to A$ given by $f_e(a) = p^{e-1} \cdot a$. The image lies in $A[p]$, so is a subspace there.

- Let $\{c_{e,i}\}_{i=1}^{I_e} \subset f_e(A)$ be a basis.
- Let $b_{e,i} \in A$ be such that $f_e(b_{e,i}) = c_{e,i}$.

CLAIM 214. The map $h_e \colon (\mathbb{Z}/p^e\mathbb{Z})^{I_e} \to A$ given by

$$h_e(\underline{x}^e) = \sum_i x_i^e b_{e,i}$$

is an isomorphism onto its image $B_e = \langle \{b_{e,i}\} \rangle$.

PROOF. Each $b_{e,i}$ has $p^e b_{e,i} = 0$ so the map is well-defined. Its image is a subgroup containing B_e and consisting of words in the $\{b_{e,i}\}$ hence equal to B_e. To compute the kernel, let $k \leq e$ be maximal such that there are $x_i' \in \mathbb{Z}$, not all divisible by p, for which $\underline{x} = p^k \underline{x}' \in \mathrm{Ker}(h_e)$. For such k and x_i' we have

$$\sum_i p^k x_i' b_{e,i} = 0\,.$$

Suppose $k \leq e - 1$. Raising to the power p^{e-1-k} we get

$$\sum_i x_i' c_{e,i} = 0$$

where not all x_i' are prime to p, which contradicts the linear independence of the $\{c_{e,i}\}$ over $\mathbb{Z}/p\mathbb{Z}$. $\square$

Continuing recursively

CLAIM 215. We have $A = B_e + A[p^{e-1}]$.

PROOF. By construction $f_e(B_e)$ contains a basis for $f_e(A)$ so $f_e(B_e) = f_e(A)$. Accordingly let $a \in A$. Then there is $b \in B_e$ such that $f_e(a) = f_e(b)$. Then $a - b \in \mathrm{Ker}(f_e) = A[p^{e-1}]$ so $a \in b + A[p^{e-1}] \subset B_e + A[p^{e-1}]$. □

Unfortunately this sum is not direct, so we have to work harder.

- Let $f_{e-1} \colon A[p^{e-1}] \to A[p]$ be given by $f_{e-1}(a) = p^{e-2} \cdot a$.
- Since $pB_e \subset A[p^{e-1}]$ and since $f_{e-1}(pa) = f_e(a)$ we see that $f_{e-1}\left(A[p^{e-1}]\right) \supset f_e(A)$.
- Let $\left\{c_{e-1,i}\right\}_{i=1}^{I_{e-1}} \subset f_{e-1}\left(A[p^{e-1}]\right)$ extend $\{c_{e,i}\}_{i=1}^{I_e}$ to a basis of $f_{e-1}\left(A[p^{e-1}]\right)$.
- Let $\left\{b_{e-1,i}\right\}_{i=1}^{I_{e-1}} \subset A[p^{e-1}]$ be such that $f_{e-1}(b_{e-1,i}) = c_{e-1,i}$.

PROOF. Now let $a \in A$. We have $a^{p^{e-1}}$ in the image of the map, so we can remove an element of A_{p^e} and get an element of $A[p^{e-1}]$. It follows that it is enough to generate that. □

Accordingly consider the map $A[p^{e-1}] \to A[p]$ given by $a \mapsto a^{p^{e-2}}$. The image contains the image of the previous map; extend the previous basis to a new basis, and pull back $\left\{b_{e-1,i}\right\}_{i=1}^{I_{e-1}}$.

CLAIM 216. The map $h_{e-1} \colon (\mathbb{Z}/p^e\mathbb{Z})^{I_e} \times \left(\mathbb{Z}/p^{e-1}\mathbb{Z}\right)^{I_{e-1}} \to A$ given by

$$h_{e-1}(\underline{x}^e, \underline{x}^{e-1}) = \sum_i x_i^e b_{e,i} + \sum_i x_i^{e-1} b_{e-1,i}$$

is an isomorphism onto its image $B_e \oplus B_{e-1} = \left\langle \{b_{e,i}\} \cup \left\{b_{e-1,i}\right\} \right\rangle$.

PROOF. Each $b_{e-1,i}$ has $p^{e-1} b_{e,i} = 0$ so the map is well-defined. Its image is clearly generated by $\{b_{e,i}\} \cup \left\{b_{e-1,i}\right\}$. To compute the kernel suppose

$$h_{e-1}(\underline{x}^e, \underline{x}^{e-1}) = 0\,.$$

Applying f_e (which kills the $b_{e-1,i}$) and using that $\{c_{e,i}\}$ are linearly independent over $\mathbb{F}_p$ we see that x_i^e are all divisible by p. Now let $k \le e-1$ be maximal such that there is $(\underline{x}^e, \underline{x}^{e-1}) \in \mathrm{Ker}\, h_{e-1}$ with $\underline{x}^{e-1}$ divisible by p^k, $\underline{x}^e$ divisible by p^{k+1}. Multiply by p^{e-1-k} we get $\bar{x}_i^e, \bar{x}_i^{e-1}$, not all zero mod p, such that

$$\sum_i \bar{x}_i^e c_{e,i} + \sum_i \bar{x}_i^{e-1} c_{e-1,i} = 0\,.$$

But this is a contradiction to the choice of the basis for $f_{e-1}\left(A[p^{e-1}]\right)$. □

CLAIM 217. We have $A = (B_e \oplus B_{e-1}) + A[p^{e-2}]$.

PROOF. Enough to show $A[p^{e-1}] = B_{e-1} + A[p^{e-2}]$ which has the same proof as before. □

Now continue recursively.

5.2.3. Finitely generated abelian groups.

PROPOSITION 218. *$\mathbb{Z}^d$ is free.*

LEMMA 219. *Let A be a finitely generated torsion-free abelian group. Then A has primitive elements.*

PROOF. Let $S \subset A$ be a finite generating set. Then it spans the vector space $\mathbb{Q} \otimes_{\mathbb{Z}} A$. Let $S_0 \subset S$ be a basis. Then $\langle S_0 \rangle \simeq \mathbb{Z}^{\#S_0}$ and every element of S, hence A, has bounded denominator wrt S_0. □

THEOREM 220. *Every finitely-generated torsion-free abelian group is free.*

PROOF. By induction on $\dim_{\mathbb{Q}}(\mathbb{Q} \otimes_{\mathbb{Z}} A)$. Let $a \in A$ be primitive. Then $\dim_{\mathbb{Q}}(\mathbb{Q} \otimes_{\mathbb{Z}} (A/\langle a \rangle)) = \dim_{\mathbb{Q}}(\mathbb{Q} \otimes_{\mathbb{Z}} A/\mathbb{Q}a) < \dim_{\mathbb{Q}}(\mathbb{Q} \otimes_{\mathbb{Z}} A)$. Thus $A/\langle a \rangle$ is free, say $A/\langle a \rangle \simeq \mathbb{Z}^{r-1}$. Choose a section, and get a direct sum decomposition. □

THEOREM 221. *Every finitely generated abelian group is of the form $\mathbb{Z}^r \oplus A_{tors}$ for a finite abelian group A_{tors}.*

PROOF. Let A_{tors} be the torsion subgroup. Then A/A_{tors} is finitely generated and torsion-free, hence isomorphic to $\mathbb{Z}^r$ for some r. Let $s \colon \mathbb{Z}^r \to A$ be a section for the quotient map (exists since $\mathbb{Z}^r$ is free). The map is injective (apply quotient map) so image is disjoint from the torsion, so $A \simeq \mathbb{Z}^r \times A_{\mathrm{tors}}$. This shows $A_{\mathrm{tors}} \simeq A/\mathbb{Z}^r$ so A_{tors} is also finitely generated, hence finite. □

CHAPTER 6

Solvable and Nilpotent groups

6.1. Nilpotence: Lecture 21

6.1.1. Nilpotent groups. In PS9 studied G such that $G/Z(G)$ is abelian – groups which are "nilpotent of order 2". Kick it up a notch: consider G such that $G/Z(G)$ are nilpotent of order 2 – call these "nilpotent of order 3".

DEFINITION 222. Call G nilpotent of order 0 if it is trivial; nilpotent of order $d+1$ if $G/Z(G)$ is nilpotent of order d.

EXAMPLE 223. Finite p-groups are nilpotent.

PROOF. By induction on the order: $Z(G)$ is always non-trivial, and $G/Z(G)$ is smaller. □

EXAMPLE 224. Products of p-groups.

FACT 225. *A finite group is nilpotent iff it is a direct product of p-groups.*

In more detail, let G be a group. Let $Z^0(G) = \{1\}$, $Z^{i+1}(G)$ the containing $Z^i(G)$ and corresponding to $Z\left(G/Z^i(G)\right)$. For example $Z^1(G) = Z(G)$.

LEMMA 226. *$Z^i(G)$ is an increasing sequence of normal subgroups.*

PROOF. $Z\left(G/Z^i(G)\right)$ is normal in $G/Z^i(G)$, now apply the correspondence theorem. □

DEFINITION 227. This is called the *ascending central series*.

EXAMPLE 228. Let $U_n = \left\{ \begin{pmatrix} 1 & * & * \\ & \ddots & * \\ & & 1 \end{pmatrix} \right\} \subset \mathrm{GL}_n(F)$ be the group of upper-triangular matrices with 1s on the diagonal. For example, $U_2 \simeq (F,+)$ and U_3 is the Heisenberg group.

EXERCISE 229. $Z(U_n)$ has zeroes everywhere except the upper right corner. $Z^2(U_n)$ has zeroes everywhere except the upper two diagonals and so on.

6.1.2. Solvable groups.

DEFINITION 230 (Normal series).

DEFINITION 231. G is solvable if it has a normal series with each quotient abelian.

EXAMPLE 232. Abelian groups. Upper-triangular group. Non-example: S_n, $n \geq 5$.

6.1.3. Motivation: Galois theory.

- Construction of Galois group of $f \in \mathbb{Q}[x]$.
- Main Theorem

6.2. Solvable groups: Lecture 22

LEMMA 233. *Any subgroup of a solvable group is solvable.*

THEOREM 234. *Let $N \lhd G$. Then G is solvable iff $N, G/N$ are.*

EXAMPLE 235. Every group of order pq, p^2q is abelian.

THEOREM 236 (Frobenius). *Every group of order $p^a q^b$ is solvable.*

DEFINITION 237 (Derived subgroup). $G' = [G,G]$ is the subgroup generated by all the commutators.

LEMMA 238. *G/N is abelian iff $G' \subset N$.*

Now let $G = G_0 \rhd G_1 \rhd \cdots \rhd G_k = \{e\}$ with G_i/G_{i+1} abelian. Then $G' \subset G_1$. Replace G_1 with G'. Then $G_2 \cap G' \lhd G'$ with abelian quotient (2nd isom theorem). So replace G_2 with $G^{(2)} = G''$. Continue.

THEOREM 239. *The derived series is the fastest descending series with abelian quotients.*

COROLLARY 240. *G is solvable iff $G^{(k)} = \{e\}$ for some k.*

PROPOSITION 241. *$K \operatorname{char} N \operatorname{char} G \Rightarrow K \operatorname{char} G$. In particular, $G^{(i)}$ are all normal in G.*

CHAPTER 7

Topics

7.1. Minimal normal subgroups

7.1.1. Characteristically free subgroups.

7.1.2. The Socle.

7.1.3. Hall subgroups.

DEFINITION 242. Let G be a finite group. A *Hall subgroup* is a subgroup $H < G$ such that $\gcd(H, [G : H]) = 1$.

THEOREM 243 (M. Hall). *Let G be a solvable group of order mn with $(m,n) = 1$. Then G has a subgroup of order m.*

PROOF. Let G be a minimal counter-example, and let $M \lhd G$ be a minimal normal subgroup. Then M is elementary abelian (it is solvable), say of order p^r. If $p^r | m$ it suffices to pull back a subgroup of G/M of order m/p^r. Otherwise pulling back a subgroup of order m of G/M we may assume that $\#G = m \cdot p^r$. □

THEOREM 244 (Schur 1904, Zassenhaus 1937). *Let $H < G$ be a normal Hall subgroups. Then $G = Q \ltimes H$ for some $Q < G$.*

PROOF. Let $M \lhd G$ be a minimal normal subgroup, and let $\bar{Q}$ be a complement to $\bar{H} = HM/M$ in G/M. If $M \cap H = \{e\}$ then Q is a complement to H. Otherwise $M \subset H$, $Q \cap H = M$ and it's enough to find a complement to M in Q, that is assume that H is a minimal normal subgroup.

Now let $P < H$ be a non-trivial Sylow subgroup. By the Frattini argument, $G = HN_G(P)$. If $N_G(P)$ is a proper subgroup, we have reduced the problem to finding a complement to $N_H(P) = H \cap N_G(P)$ in $N_G(P)$, so we may assume $P \lhd G$. But H is a minimal normal subgroup, so $P = H$. We conclude that H is elementary abelian.

In the abelian case one directly computes the cohomology $H^2(G/H; H)$ and sees that it is trivial. □

Bibliography

[1] D. L. Johnson. Minimal permutation representations of finite groups. *Amer. J. Math.*, 93:857–866, 1971.