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

- **Introduction**
  - 0.1. Administrivia 4
  - 0.2. Motivation 4
  - 0.3. Course plan (subject to revision) (Lecture 1, 10/9/2015) 5

- **Chapter 1. Some explicit groups**
  - 1.1. $\mathbb{Z}$ 6
  - 1.2. $S_n$ (Lecture 4, 22/9/2015) 10
  - 1.3. $GL_n(\mathbb{R})$ 12
  - 1.4. The dihedral group 13

- **Chapter 2. Groups and homomorphisms**
  - 2.1. Groups, subgroups, homomorphisms (Lecture 6, 29/9/2015) 14
  - 2.2. Examples (Lecture 7, 1/10/2015) 16
  - 2.3. Subgroups and coset spaces (Lecture 8, 6/10/2015) 18
  - 2.4. Normal subgroups and quotients (Lectures 9–10) 19

- **Chapter 3. Group Actions**
  - 3.1. Group actions (Lecture 11, 15/10/2015) 23
  - 3.2. Conjugation (Lecture 12, 22/10/2015) 24
  - 3.3. Orbits, stabilizers and counting (Lecture 13, 27/10/2015) 26
  - 3.4. Actions, orbits and point stabilizers (handout) 27

- **Chapter 4. $p$-Groups and Sylow’s Theorems**
  - 4.1. $p$ groups (Lecture 14, 29/10/2015) 31
  - 4.2. Example: groups of order $pq$ (Lecture 15, 3/11/2015) 33
  - 4.3. Sylow’s Theorems (Lectures 16–18) 35

- **Chapter 5. Finitely Generated Abelian Groups**
  - 5.1. Statements: Lecture 20, 19/11/2015 38
  - 5.2. Proofs 38

- **Chapter 6. Solvable and Nilpotent groups**
  - 6.1. Nilpotence: Lecture 21 42
  - 6.2. Solvable groups: Lecture 22 43

- **Chapter 7. Topics**
  - 7.1. Minimal normal subgroups 44

- **Bibliography** 45
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 $c^{610} = 1$.


• 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: $\mathbb{Z}, S_n, \text{GL}_n(\mathbb{R})$.
- 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 \( 0 \leq r < a \) 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, \( b – (–(|b| + 1))a \geq a + |b|(a – 1) \geq 0 \), and hence has a least element \( r \), say \( r = b – qa \). If \( r \geq a \) then \( 0 \leq r – a < r \) 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

\[ r – r' = a(q' – q). \]
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 \( r - r' \leq r \leq a - 1 \). \( \square \)

**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 \( b = qa \). \( \square \)

**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 contradiction.
2. To check if \( a \mid b \) 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 \( a \mid b \) if there is \( c \) such that \( b = ac \). Write \( a \nmid b \) otherwise.

**Example 10.** \( \pm 1 \) divide every integer. Only \( \pm 1 \) divide \( \pm 1 \). Every integer divides \( 0 \), but only \( 0 \) divides \( 0 \). \( 2 \mid 14 \) 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 \( d \mid a, d \mid b \) so \( d \) is a common divisor. Conversely, let \( x, y \) be such that \( d = ax + by \) and let \( e \) be another common divisor. then \( e \mid a, e \mid b \) so \( e \mid ax, e \mid by \) so \( e \mid ax + by = d \). In particular, \( e \leq d \) so \( d \) is the greatest common divisor. \( \square \)

**Algorithm 12 (Euclid).** Given \( a, b \) set \( a_0, a_1 \) be \( |a|, |b| \) 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:

\[
a_{n-1} = q_na_n + r_n.
\]

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

**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 \(b\) modulo \(n\), and write \(a \equiv b \pmod{n}\) 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. \((a' + b') - (a + b) = (a' - a) + (b' - b); \, \, a'b' - ab = (a' - a)b' + a(b' - b)\). \(\Box\)

- 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

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

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. \(\Box\)

REMARK 22. Why exclude the ones not relatively prime? These can’t have inverses.

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 \((\mathbb{Z}/8\mathbb{Z})^\times\).
Remainder 24. In general, \((\mathbb{Z}/p\mathbb{Z})^\times \simeq (\mathbb{Z}/(p-1)\mathbb{Z}, +)\) but the isomorphism is \textit{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 \(A_d = \{0 \leq a < n \mid \gcd(a, n) = d\}\). Then \(\{\frac{a}{d} \mid a \in A_d\} = \{0 \leq b < \frac{n}{d} \mid \gcd(b, \frac{n}{d}) = 1\}\) 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 \((\mathbb{Z}/p\mathbb{Z})^\times = \{\bar{1}, \ldots, \bar{p-1}\}\).

**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 \((ab)(a'b') \equiv (ad')(bb') \equiv 1 \cdot 1 \equiv 1 (p)\) 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 \(\varepsilon \prod_{p \text{prime}} p^{e_p}\) 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

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

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

\(f : \mathbb{Z}/N\mathbb{Z} \rightarrow (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z})\)

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:

\[f([b_1]_N) = ([1]_{n_1}, [0]_{n_2})\]

\[f([b_2]_N) = ([0]_{n_1}, [1]_{n_2}).\]
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
\[
f([a_1b_1 + a_2b_2]_N) = ([a_1]_{n_1} \cdot [b_1]_{n_1}, [a_2]_{n_2} \cdot [b_2]_{n_2}) + ([a_2]_{n_1} \cdot [0]_{n_2}, [a_1]_{n_2} \cdot [1]_{n_2})
\]
\[
= ([a_1]_{n_1}, [0]_{n_2}) + ([0]_{n_1}, [a_2]_{n_2}) = ([a_1]_{n_1}, [a_2]_{n_2}).
\]
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: concrete and abstract.

**Definition 33.** Let \( X \) be a set. A permutation on \( X \) is a bijection \( \sigma: X \to X \) (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 \( f: Y \to Z \) and \( g: X \to Y \) is the function \( f \circ g: X \to Z \) given by \( (f \circ g)(x) = f(g(x)) \).

**Lemma 34.** Composition of functions is associative. The identity function \( \text{id}_X: X \to X \) belongs to the symmetric group and is an identity for composition.

**Example 35.** \( \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 4 & 2 & 1 \end{pmatrix} \). The identity map. Non-example \( \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \).

**Lemma 36.** Let \( \sigma: X \to X \) be a function.

1. \( \sigma: X \to X \) is a bijection iff there is a “compositional inverse” \( \bar{\sigma}: X \to X \) such that \( \sigma \circ \bar{\sigma} = \bar{\sigma} \circ \sigma = \text{id} \).
2. \( S_X \) is closed under composition and compositional inverse.
3. Suppose \( \sigma \in S_X \) and that \( \sigma \tau = \text{id} \) or that \( \tau \sigma = \text{id} \). Then \( \tau = \bar{\sigma} \). In particular, the compositional inverse is unique and will be denoted \( \sigma^{-1} \).
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 \( \sigma \) satisfies \( \sigma \circ \bar{\sigma} = \bar{\sigma} \circ \sigma = \text{id} \) so \( \bar{\sigma} \in S_X \). Also, \( (\bar{\tau} \bar{\sigma}) (\sigma \tau) = (\bar{\tau} (\sigma \bar{\sigma})) \tau = (\bar{\tau} \text{id}) \tau = \text{id} \) and similarly in the other order, so \( \sigma \tau \in S_X \).

(3) Suppose \( \sigma \tau = \text{id} \). Compose with \( \bar{\sigma} \) on the left. Then \( \bar{\sigma} = \bar{\sigma} (\sigma \tau) = (\sigma \bar{\sigma}) \tau = \text{id} \tau = \tau \).

**Remark 37.** Note that \( S_X \) is not commutative! \( \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \) but \( \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \).

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 \( 1 \leq j \leq r-1 \), such that \( \sigma(i_r) = i_1 \), and that \( \sigma(i) = i \) if \( i \neq i_j \) for all \( j \).

**Example 40.** \( \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \).

**Definition 41.** Let \( \sigma \in S_X \). Set \( \text{supp}(\sigma) = \{ i \in X \mid \sigma(i) \neq i \} \).

**Lemma 42.** \( \sigma, \sigma^{-1} \) have the same support. Suppose \( \sigma, \tau \) have disjoint supports. Then \( \sigma \tau = \tau \sigma \).

**Proof.** \( \sigma(i) = i \) iff \( \sigma^{-1}(i) = i \). If \( i \in \text{supp}(\sigma) \) then \( j = \sigma(i) \in \text{supp}(\sigma) \) (else \( i = \sigma^{-1}(j) = j \) a contradiction). Thus \( \sigma(i) \in \text{Fix}(\tau) \) so \( \tau \sigma(i) = \sigma(i) \). Also, \( i \in \text{Fix}(\tau) \) so \( \sigma \tau(i) = \sigma(i) \). Similarly if \( i \in \text{supp}(\tau) \). If \( i \) is fixed by both \( \sigma, \tau \) 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 \( \sigma \) be a counterexample with minimal support. Then \( \sigma \neq \text{id} \), 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 \( \kappa \) be the resulting cycle. Then \( \kappa^{-1} \sigma \) agrees with \( \sigma \) off \( \{ i_j \} \) and fixes each \( i_j \). Factor this and multiply by \( \kappa \).

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 \( i \)

**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 \( \text{sgn} (\alpha) = (-1)^{n-t} \) is called the sign of \( \sigma \).

LEMMA 51. Let \( \tau \) be a transposition. Then \( \text{sgn}(\tau \sigma) = -\text{sgn}(\sigma) \).

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. \( \square \)

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

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

By Lemma 45 we see that \( H = S_n \) and the claim follows. \( \square \)

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

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

PROOF. Let \( \tau \) 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. \( \square \)

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

1.3. \( \text{GL}_n(\mathbb{R}) \)

Let \( \text{GL}_n(\mathbb{R}) = \{ g \in M_n(\mathbb{R}) \mid \det(g) \neq 0 \} \). 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 \( g \in \text{GL}_n(\mathbb{R}) \) has an inverse.

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

Next, recall that the map \( \det : \text{GL}_n(\mathbb{R}) \to \mathbb{R}^\times \) 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 \( \{ g \in \text{GL}_n(\mathbb{R}) \mid g(\mathbb{R}e_i) = (\mathbb{R}e_i) \} \) is closed under multiplication and taking inverses.

2. Show that if \( \tau i = j \) then \( \tau \text{Stab}(i) \tau^{-1} = \text{Stab}(j) \)

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 \( D_{2n} = \text{Aut}(P_n) \) be the set of maps of the plan that map \( P_n \) to itself.

- Label vertices 0, 1, \ldots, \( n-1 \) (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 \( r^2 = \text{id} \) and that \( rcr = c^{-1} \).

**Lemma 59.** Suppose \( g \in D_{2n} \) fixes \([0]\). Then \( g \) is either \( \text{id} \) 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 \( c^{-j} g = \text{id} \) 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 \( j \equiv k \mod{n} \). 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
\[
c^j r c^k r r r = c^j (rcr)^k r^1 + \delta = c^{j-k} r^{1+\delta}.
\]

**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 \( G \) is a pair \( (G, \cdot) \) where \( G \) is a set and \( \cdot : G \times G \to G \) 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. \( \bar{\bar{x}} = \bar{x} \).

PROOF. (1) For any \( x \in G \) we have \( \bar{x} = e\bar{x} = (\bar{x}x)\bar{x} = (\bar{x}(x\bar{x})) = e(x\bar{x}) = x\bar{x} \).

(2) For any \( x \in G \) we have \( xe = x(\bar{x}x) = (\bar{x}x)x = ex = x \).

(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 \( \bar{x}\bar{x} = e \). Now multiply on the right by \( x \).

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

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) \( \mathbb{Z}, S_n, \text{GL}_n(\mathbb{R}) \).
(2) \( \mathbb{R}^+, \) additive group of vector space.
(3) \( \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^* \).
(4) \( C_n \cong (\mathbb{Z}/n\mathbb{Z}, +), (\mathbb{Z}/n\mathbb{Z})^* \).
(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) \( (\mathbb{Z}_\geq 1, \text{gcd}), (\mathbb{Z}_\geq 1, \text{lcm}) \).

### 2.1.2. Homomorphisms.

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

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

**Example 73.** Trivial homomorphism, \( \text{sgn}: S_n \to \{\pm 1\}, \text{det}: \text{GL}_n(\mathbb{R}) \to \text{GL}_1(\mathbb{R}) \), the quotient map \( \mathbb{Z} \to \mathbb{Z}/N\mathbb{Z} \).

**Lemma 74.** Let \( f: G \to H \) 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 \( f(g)f(g^{-1}) = f(gg^{-1}) = f(e_G) = e_H \) so \( f(g), f(g^{-1}) \) are inverses. □

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

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

**Proof.** PS4 □

**Lemma 77.** Let \( g: G \to H, f: H \to K \) be group homomorphisms. Then \( f \circ g: G \to K \) is a group homomorphism.

**Proof.** PS4. □

**Example 78.** \( (\mathbb{Z}/5\mathbb{Z})^* \) and \( (\mathbb{Z}/8\mathbb{Z})^* \) 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 \((H, \cdot|_H \times H)\) 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 \( |H \times H| = H \)-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 \( f \in \text{Hom}(G,H) \). Its kernel is the set \( \text{Ker}(f) = \{ g \in G \mid f(g) = e_H \} \). Its image is the set \( \text{Im}(f) = \{ h \in H \mid \exists g \in G : f(g) = h \} \).

**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 \( e_G \in \text{Ker}(f) \) and \( e_H \in \text{Im}(f) \) so both are non-empty. Let \( g, g' \in \text{Ker}(f) \). Then \( f(g^{-1}) = f(gg')^{-1} = e_H = e_H \) and \( f(gg') = f(g)f(g') = e_H e_H = e_H \).

Similarly let \( h, h' \in \text{Im}(f) \). Choose preimages \( g \in f^{-1}(h) \) and \( g' \in f^{-1}(h') \). Then \( h^{-1} = f(g)^{-1} = f(g^{-1}) \in \text{Im}(f) \) and \( hh' = f(g)f(g') = f(gg') \in \text{Im}(f) \).

**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 \( \text{Ker} f = \{ e \} \).

**Proof.** (not given in class) Suppose \( f \) is injective. Then for \( g \neq e \), \( f(g) \neq f(e) \) so \( \text{Ker}(f) = e \).

Conversely, suppose \( \text{Ker}(f) = e \) and that \( f(g) = f(g') \). Then \( f(g^{-1}g') = f(g)^{-1}f(g') = f(g)^{-1}f(g) = e \) so \( g^{-1}g' \in \text{Ker}(f) \). 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 \( g^n = (g^{-1})^{-n} \).

**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.

**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. $\text{Ker } f = \{0\}$ and $f : \mathbb{Z} \to G$ is an isomorphism.
2. $\text{Ker } f = n\mathbb{Z}$ 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. $\langle g \rangle = \langle g^{-1} \rangle$).

**Proof.** $f$ is surjective by definition. If $\text{Ker } f = \{0\}$ then $f$ is injective, hence an isomorphism. Otherwise, by Proposition 7 we have $\text{Ker } f = n\mathbb{Z}$ for some $n$. We now define $\tilde{f} : \mathbb{Z}/n\mathbb{Z} \to G$ by $\tilde{f}(\overline{a}) = g^a$.

- This is well-defined: if $\overline{a} = \overline{b}$ 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 $cn \in \text{Ker } f$.
- This is a homomorphism: $\tilde{f}(\overline{a} + \overline{b}) = \tilde{f}(\overline{a} + \overline{b}) = f(a + b) = f(a)f(b) = \tilde{f}(\overline{a})\tilde{f}(\overline{b})$.
- This is injective: $\overline{a} \in \text{Ker } \tilde{f} \iff \tilde{f}(\overline{a}) = e \iff a \in n\mathbb{Z} \iff \overline{a} = [0]_n$.

**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 $\text{GL}_2(\mathbb{R})$, $egin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ has infinite order while $egin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ 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 $\text{Aut}(X) = \{ g : X \to X \mid g, g^{-1} 	ext{ "preserves the structure" } \}$ 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. $\text{Aut}(G) = \text{Hom}(G, G) \cap S_G$.

**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 $(x,y) \in E \iff (y,x) \in E$.

Example: $K_n$, cycle ...
Definition 102. An automorphism of $\Gamma$ is a map $f \in S_V(\Gamma)$ such that $(x, y) \in E \iff (f(x), f(y)) \in E$.

Lemma 103. $\text{Aut}(\Gamma) < S_\Gamma$ is a subgroup.

Example 104. $\Gamma = K_n$, $\text{Aut}(\Gamma) = S_n$.

We concentrate on the cycle.

Definition 105. $D_{2n} = \text{Aut}(n$-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. □

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 $W \subset \langle S \rangle$. □

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 $g' \equiv_R g(H) \iff g'g^{-1} \in H$.

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

**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, \(g^{\#G} = (g^m)^{\#G/m} = e\).

**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 \(H \setminus G\) 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 \(\langle g \rangle = G\).

**Example 122** (Fermat’s Little Theorem; Euler’s Theorem). Let \(a \in \mathbb{Z}\). Then:

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

**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 \(\phi(n)\).

### 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 \(f \in \text{Hom}(G, H)\) and let \(g \in G\). Then \(g\ ker(f)g^{-1} = \ker(f)\).

**Proof.** Let \(g \in G\), \(n \in \ker(f)\). Then \(f(gng^{-1}) = f(g)f(n)f(g^{-1}) = f(g)f(g)^{-1} = e\) so \(gng^{-1} \in \ker(f)\) as well.

**Definition 124.** Call \(N \triangleleft G\) normal if \(g\ N = N\ g\) for all \(g \in G\), equivalently if \(g\ N\ g^{-1} = N\) for all \(g \in G\). In that case we write \(N \triangleleft G\).

**Lemma 125.** Enough to check \(g\ N g^{-1} \subseteq N\).

**Proof.** PS5 Practice problem P4.

**Example 126.** \(\{e\}, G\) always normal; Any subgroup of an abelian group. 

\(\text{SL}_n(\mathbb{R}) \triangleleft \text{GL}_n(\mathbb{R})\) (kernel of determinant), \(A_n \triangleleft S_n\) (kernel of sign). Translations in \(\text{Isom}(\mathbb{R}^n)\).

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

**Definition 128.** The normal closure of \(S < G\) is the normal subgroup \(\langle S \rangle^N = \bigcap \{N \triangleleft G \mid S \subseteq N\\}.\)
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

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

Also, $g \equiv_L g'(N)$ iff $g^{-1} \equiv_R (g')^{-1} (N)$ 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 $f \in \text{Hom}(G,H)$ and let $K = \text{Ker}(f)$. Then $f$ induces an isomorphism $G/K \to \text{Im}(f)$.

**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 definition 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 $gK = K = e_{G/K}$. \qed

**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

$$H / (H \cap N) \simeq HN / N.$$  

**Proof.** Composing the inclusion $i : H \to HN$ and the quotient map $\pi : HN \to HN/N$. $f$ 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 $i$. We now compute its kernel. Let $h \in H$. Then $h \in \text{Ker} f$ iff $f(h) = e_{HN/N}$ iff $\pi(h) = N$ iff $hN = N$ iff $h \in N \cap H$. Thus $\text{Ker} f = H \cap N$ and the claim follows from the previous Theorem. \qed

**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 $(gK)(nK)(gK)^{-1} \overset{\text{def}}{=} gng^{-1}K \in N/K$ so $N/K \triangleleft G/K$. 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 $g \in \text{Ker} f$ iff $gK \in N/K$ iff $g \in N$. \qed
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 $N \triangleleft A_n$ 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 $\sigma$ a transposition.
- **Case 3.** $k = 3$ makes $\sigma$ a 3-cycle. By Lemma 139(1), $N$ contains all 3-cycles and thus equals $A_n$.
- **Case 4.** $k = 4$ makes $\sigma$ of the form $(12)(34)$ since 4-cycles are odd. We are then done by Lemma 139(2).
- **Case 5.** $k \geq 5$ and $\sigma$ 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 $\gamma$ fixes every point that $\sigma$ does, and also $\gamma(2) = 2$, but $\gamma(3) = 4$, so $\gamma \neq \text{id}$ – a contradiction.
- **Case 6.** $k \geq 5$ and $\sigma$ is a product of disjoint transpositions (necessarily at least 4), say $\sigma = (12)(34)(56)(78) \cdots$. Then the same $\gamma$ again fixes every point that $\sigma$ 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 $\text{id}, (12345)(13542)$ have sizes 1, 12, 12 which do not add up to a divisor of 60.
3. $A_6$ is simple:
   a. Let $N \triangleleft A_6$ 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 \( N \trianglelefteq A_n \) be normal. Let \( \sigma \in N \) be non-identity with, say, \( \sigma(1) = 2 \). Then \( \kappa = (234) \) does not commute with \( \sigma \) (\( \kappa \sigma(1) = 3 \) but \( \sigma \kappa(1) = 2 \)).

(5) The element \( \gamma = [\sigma, \kappa] = \sigma \kappa \sigma^{-1} \kappa^{-1} = \sigma (\kappa \sigma^{-1} \kappa^{-1}) \in N \) is also non-identity. But writing this element as \( (\sigma \kappa \sigma^{-1}) \kappa^{-1} \) 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 \( N \trianglelefteq A_{n+1} \) 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 $\cdot : G \times X \to X$ 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 discuss 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”, $\text{Aut}(X) = \{ \sigma \in S_X \mid \sigma, \sigma^{-1} \text{ "preserve the structure"} \}$ acts on $X$.
   • Can always restrict actions: if $\cdot : G \times X \to X$ is an action then $\cdot \mid_{H \times X}$ is an action of $H$.
      (a) $D_{2n}$ acting on cycle, inside of there’s $C_n$ acting on te cycle; $\text{Aut}(\Gamma)$ acting on $\Gamma$.
      (b) $\text{GL}_n(\mathbb{R})$ acting on $\mathbb{R}^n$, $\text{GL}(V)$ acting on $V$.
      (c) $G$ group; $\text{Aut}(G)$ acting on $G$.
(4) Induced actions (see Problem Set): suppose $G$ acts on $X, Y$.
   (a) $G$ acts on $Y^X$ by $(g \cdot f)(x) \overset{\text{def}}{=} g \cdot (f(g^{-1} \cdot x))$ (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 $\sigma_g : X \to X$ given by

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

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 $\text{Hom}(G, S_X)$ is a bijection

$$\{ \text{actions of } G \text{ on } X \} \leftrightarrow \text{Hom}(G, S_X).$$
We first show $\sigma_g \circ \sigma_h = \sigma_{gh}$. Indeed for any $x \in X$:

\[
(\sigma_g \circ \sigma_h)(x) = \sigma_g(\sigma_h(x)) \quad \text{def of } \circ \\
= g \cdot (h \cdot x) \quad \text{def of } \sigma_g, \sigma_h \\
= (gh) \cdot x \quad \text{def of gp action} \\
= \sigma_{gh}(x) \quad \text{def of } \sigma_{gh}.
\]

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

\[
\sigma_g \circ \sigma_{g^{-1}} = \text{id} = \sigma_{g^{-1}} \circ \sigma_g
\]

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

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

**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 $L_G: G \to S_G$. We show that $\text{Ker}(L_G) = \{e\}$, so that $L_G$ will be an isomorphism onto its image. For that let $g \in \text{Ker}(L_G)$. Then $L_G(g) = \text{id}_G$, and in particular this means that $g$ fixes $e$: $g \cdot e = e$. But this means $g = e$ and we are done. \hfill $\square$

**Remark 145.** Can make this quantitative: \[\text{1}\] 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 \[\text{117}\] 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 $p \leq k \leq n$. \hfill $\square$

**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 $gx = g \cdot x \cdot g^{-1}$. Set $\gamma_g(x) = g \cdot x \cdot g^{-1}$.

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

**Proof.** Check. \hfill $\square$
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). \hfill $\square$

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 $G \to \text{Aut}(G)$ (this is Lemma 142(2)).

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

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

Definition 157. Call $\text{Out}(G) \overset{\text{def}}{=} \text{Aut}(G) / \text{Inn}(G)$ the outer automorphism group of $G$.

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

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

Fact 159. $\text{Out}(S_n) = \{ e \}$ except that $\text{Out}(S_6) \cong C_2$.

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 well-defined: if $g' = gz$ with $z \in Z$ then $^g' x = ^g z \cdot x = ^g x$. It is surjective: the conjugate $^g x$ is the image of $gZ_G(x)$, and finally if $^g x = ^{g'} x$ then $x = ^{g^{-1}} x = ^{g^{-1}} g^{-1} x$ so $g^{-1} g' \in Z_G(x)$ and $g'Z_G(x) = g'Z(x)$. \hfill $\square$

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. \hfill $\square$

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, $^g (^h H) = ^{gh} H$. \hfill $\square$
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. □

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

PROOF. Same. □

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. □

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 $O(x)$ for the orbit of $x \in X$. Write $G \setminus X$ for the set of orbits. For $x \in X$ set $\text{Stab}_G(x) = \{ g \in G \mid g \cdot x = x \}$.

LEMMA 172. $\text{Stab}_G(x)$ 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 $(hg)x = h(gx) = hx = x$. □

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

PROOF. Same. □

COROLLARY 174 (General class equation). We have

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

PROOF. $X$ is the disjoint union of the orbits. □

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

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

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 $p$. □

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,


- 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 $g = yg^{-1}$. Then $g(xH) = y^{-1}xH = yH$ so there is only one orbit.

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

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

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

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

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

\begin{align*}
\text{Claim 179. Let } V \text{ be a vector space, } u, v \in V \text{ be two non-zero vectors. Then there is a linear map } g \in \text{GL}(V) \text{ such that } gu = v.
\end{align*}

We need a fact from linear algebra

\begin{align*}
\text{Fact 180. Let } V, W \text{ be vector spaces and let } \{u_i\}_{i \in I} \text{ be a basis of } V. \text{ Let } \{w_i\}_{i \in I} \text{ be any vectors in } W. \text{ Then there is a unique linear map } f : V \to W \text{ such that } f(u_i) = w_i.
\end{align*}

\begin{align*}
\text{Proof of Claim. Complete } u, v \text{ to a bases } \{u_i\}_{i \in I}, \{v_i\}_{i \in I} (u_1 = u, v_1 = v). \text{ There is a unique linear map } g : V \to V \text{ such that } gu_i = v_i \text{ (because } \{u_i\} \text{ is a basis) and similarly a unique map } h : V \to V \text{ such that } hv_i = u_i. \text{ But then for all } i \text{ we have } (gh)v_i = v_i = Idv_i \text{ and } (hg)u_i = u_i = Idu_i, \text{ so by the uniqueness prong of the fact we have } gh = Id = hg \text{ and } g \in \text{GL}(V). \quad \square
\end{align*}

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

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

3.4.3. \( \text{GL}_n(\mathbb{R}) \) 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 \( G = \text{GL}_n(\mathbb{R}) \) and \( X = Y = \mathbb{R}^n \).

(1) Orbits:
   - Clearly \((0,0)\) is a fixed point of the action.
   - If \( u \neq 0, v \neq 0 \), the previous discussion constructed \( g \) such that \( gu = v \) and hence \( g \cdot (u,0) = (v,0) \) and \( g \cdot (0,u) = (0,v) \). Since \( G \cdot (u,0) \subset \mathbb{R}^n \times \{0\} \), we therefore get two more orbits: \( \{(u,0) \mid u \neq 0\} \) and \( \{(0,u) \mid u \neq 0\} \).
   - We now need to understand when there is \( g \) such that \( g \cdot (u_1,u_2) = (v_1,v_2) \). In the previous discussion we saw that if \( \{u_1,u_2\} \) are linearly independent then completing to a basis will provide such \( g \). Conversely, if \( \{u_1,u_2\} \) are independent then so are \( \{gu_1,gu_2\} \) for any invertible \( g \) (preserves the vector space structure hence linear algebra properties like linear independence). We therefore have an orbit \( \{(u_1,u_2) \mid \text{the vectors are linearly independent}\} \).
   - The case of linear dependence remains, so we need to consider the orbit of \( (u_1,u_2) \) where both are non-zero and \( u_2 = au_1 \) for some scalar \( a \), necessarily non-zero. But in that case \( g \cdot (u_1,u_2) = (gu_1,g(au_1)) = (gu_1,a(gu_1)) \) so we conclude that the orbit is contained in \( \{(u_1,au_1) \mid u_1 \neq 0\} \).
   - Conversely, this is an orbit because if \( u_1,u_2 \) are both non-zero then if \( gu_1 = u_2 \) then \( g \cdot (u_1,au_1) = (v_1,a(v_1)) \).

Summary: the orbits are \( \{(0,0)\}, \{(u,0) \mid u \neq 0\}, \{(0,u) \mid u \neq 0\}, \{(u_1,u_2) \mid \dim \text{Span}_F \{u_1,u_2\} = 2 \} \) and for each \( a \in F^\times \) the set \( \{(u_1,au_1) \mid u_1 \neq 0\} \).

(2) Point stabilizers:
   - \((0,0)\) is fixed by the whole group.
   - \( g \cdot (u,0) = (u,0) \) iff \( gu = u \), so this is the case solved before. Similarly for \( g \cdot (u,au) = (u,au) \) which holds iff \( gu = u \).
   - \( g (e_{n-1},e_n) = (e_{n-1},e_n) \) holds iff the last two columns of \( g \) are \( e_{n-1},e_n \) so

\[
\text{Stab}_{\text{GL}_n(\mathbb{R})}(e_{n-1},e_n) = \left\{ g = \begin{pmatrix} h & 0 \\ y & I_2 \end{pmatrix} \mid h \in \text{GL}_{n-2}(\mathbb{R}), y \in M_{2,n-2}(\mathbb{R}) \right\}.
\]

EXERCISE 183. Show that the block-diagonal matrices \( M = \left\{ \begin{pmatrix} h & 0 \\ 0 & I_2 \end{pmatrix} \mid h \in \text{GL}_{n-2}(\mathbb{R}) \right\} \) are a subgroup of \( \text{GL}_n(\mathbb{R}) \) isomorphic to \( \text{GL}_{n-2}(\mathbb{R}) \). Show that the matrices \( N = \left\{ \begin{pmatrix} I_{n-2} & 0 \\ y & 1 \end{pmatrix} \mid y \in M_{2,n-2}(\mathbb{R}) \right\} \approx \).
are a subgroup isomorphic to \( \mathbb{R}^{2(n-2)} \). Show that \( \text{Stab}_{\text{GL}_n(\mathbb{R})}(\mathbb{E}_{n-1}, \mathbb{E}_n) \) is the semidirect product \( M \ltimes N \).

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

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

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

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

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

This can be generalized. Write

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

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

#### 3.4.5. \( \text{O}(n) \) acting on \( \mathbb{R}^n \).

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

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

1. Orbits: we know that if \( g \in \text{O}(n) \) and \( v \in \mathbb{R}^n \) then \( \|gv\| = \|v\| \). Conversely, for each \( a \geq 0 \) \( \{v \in \mathbb{R}^n \mid \|v\| = a\} \) is an orbit. When \( a = 0 \) this is clear (just the zero vector) and otherwise let \( u, v \) both have norm \( a \). Let \( u_1 = \frac{1}{a} v u, v_1 = \frac{1}{a} v \) and complete \( u_1, v_1 \) to orthonormal bases \( \{u_i\}, \{v_j\} \) respectively. Then the unique invertible linear map \( g \in \text{GL}_n(\mathbb{R}) \) such that \( gu_1 = v_1 \) is orthogonal (linear algebra exercise) and in particular we have \( g \in \text{O}(n) \) such that \( gu_1 = v_1 \) and then \( gu = g(a u_1) = a u_1 = a v_1 = vv \).

#### 3.4.6. \( \text{Isom}(\mathbb{R}^n) \) acting on \( \mathbb{R}^n \).

Let \( \text{Isom}(\mathbb{R}^n) \) be the Euclidean group: the group of all rigid motions of \( \mathbb{R}^n \) (maps \( f : \mathbb{R}^n \to \mathbb{R}^n \) which preserve distance, in that \( \| f(u) - f(v) \| = \| u - v \| \)).

1. The action is transitive: for any fixed \( a \in \mathbb{R}^n \) the translation \( T_a x = x + a \) preserves distances, and for any \( u, v \) we have \( T_{v-u}(u) = v \).
2. The point stabilizer of zero is exactly the orthogonal group!
PROOF. Let $f \in \text{Isom}(\mathbb{R}^n)$ satisfy $f(0) = 0$. We show that $f$ preserves inner products. For this first note that for any $x$,

$$
\|f(x)\| = \|f(x) - 0\| = \|f(x) - f(0)\| = \|x - 0\| = \|x\|.
$$

Second since $\|x - y\|^2 = \|x\|^2 + \|y\|^2 - 2 \langle x, y \rangle$ we have the polarization identity

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

so that

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

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

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

$$
\langle f(x), u_i \rangle = \langle f(x), f(e_i) \rangle = \langle x, e_i \rangle = a_i
$$

that also

$$
f(x) = \sum_i a_i u_i = \sum_i a_i ge_i = g \left( \sum_i a_i e_i \right) = gx
$$

so that $f$ agrees with $g$. □

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

Exercise 186. The orbits of $\text{Isom}(\mathbb{R}^n)$ on the space of pairs $\mathbb{R}^n \times \mathbb{R}^n$ are exactly the sets

$$
D_a = \{ (x, y) \mid \|x - y\| = a \} \ (a \geq 0).
$$
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 \( p \mid \#G \). 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 \( p \mid \#Z(G) \) 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. \( \square \)

Here’s another proof:

PROOF. Let \( X = \{ g \in G^p \mid \prod_{i=1}^{p} g_i = e \} \). 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 \( p \mid \#Y \). But \( Y \) is in bijection with the set of elements of order divisible by \( p \), which is non-empty since \( e \) is there. \( \square \)

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:

\[
|X| \equiv |\{x \in X \mid \text{Stab}_G(x) = G\}| \quad \text{mod } p .
\]

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 \( p \). \( \square \)

31
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
\[
xy = g^kg^lw = g^{k+l}zw
\]
\[
yx = g^lw^kz = g^lw^kwz = g^{k+l}zw.
\]
\( \square \)

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 \( \langle \mathbb{Z}/p\mathbb{Z} \rangle^2 \to G \) given by \( f(a,b) = xa^yb \). 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 identification with \( (\mathbb{F}_p^2, +) \simeq C_{p^2} \).

(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 denoted \( G^p \). This subgroup is non-trivial because the \( p \)th 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 \( y \in C_p^p \) 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-trivial, hence of the form \( x^{kp} \) for some \( k \) prime to \( p \). Let \( k \) be inverse to \( k \) mod \( p \). Then \( z = y^k \) has \( \langle z \rangle = \langle y \rangle \), so
it still has order \( p^2 \) and still lies outside \( \langle x \rangle \). Finally, by contradiction \( z^p = x^p \) so \( x^{-1} \not\in \langle x \rangle \) has order \( p \) and we are done.

\( \square \)

### 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). \( S_3 \cong D_6 \). 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] 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 \( x^{-1} \langle y \rangle^{-1} y = P \cap Q = \{ e \} \) so \( x = x' \) and \( y = y' \). \( \square \)

**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 \( C = \{ gQg^{-1} \mid g \in G \} \) be the congruacy class of \( Q \). Since \( G = PQ \) we have

\[
\begin{align*}
C &= \{ xyQy^{-1}x^{-1} \mid x \in P, y \in Q \} \\
&= \{ xQx^{-1} \mid x \in P \} \\
&= \{ Q, aQa^{-1} \}
\end{align*}
\]

if we parametrize \( P = \{ 1, a \} \). Suppose that \( Q' = aQa^{-1} \not= Q \). Now \( Q \cong Q' \cong C_3 \), 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 contradiction. \( \square \)

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

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

In particular, to the product structure on \( P \times Q \) 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 \( Q = \{ 1, b, b^2 \} \) 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 $G \cong P \times Q$ (internal direct product). But this means $G \cong C_2 \times C_3 \cong C_6$ by the Chinese Remainder Theorem. 

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 $C = \{gQg^{-1} \mid g \in G\}$ be the conjugacy class of $Q$. Since $G = PQ$ we have
\[
C = \{xyQy^{-1}x^{-1} \mid x \in P, y \in Q\} = \{xQx^{-1} \mid x \in P\}.
\]

In other words, $C$ 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 $C$ 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 $Q' \in C$ 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 $G = P \times Q$. Again the product structure on $P \times Q$ 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 $ab^j a^{-1} = (b^j)^k$ so $aya^{-1} = y^k$ for all $y \in Q$. Second, by induction on $i$, $a^iy^{-1} = y^{(k)}$ (composition of homomorphisms). We see that it remains to choose $k$.

Note that $a^p = e$ and that $b = a^p ba^{-p} = b^{kp}$ so we must have $kp \equiv 1 (q)$, 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 $G \cong C_p \times C_q \cong C_{pq}$ by the Chinese Remainder Theorem.

Case 2. If $aba^{-1} = b^k$ for $k \neq 1 (q)$. 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 subgroup, 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:
\[
\langle a, b \mid a^p = b^q = e, aba^{-1} = q^k \rangle
\]

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

\[34\]
4.2.3. More detail, and examples (Lecture 16, 5/11/2015).

- Explicitly parametrize $G$ as $\{a^i b^j \mid i \mod p, j \mod q\}$.
  - 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, $\text{Aut}(C_n) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.
  - For any $k \mod q$ can try to define the product
    $$\left(a^i b^j \right) \left(a^k b^j \right) = a^{i+k} b^j k^{-i} + j$$
    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 $k'$ we can replace $a$ with $a'$ (with $a^r$) 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 $C_3 \rtimes C_7$.

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 $p^i \mid n$ 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, $\#\text{Fix}(H) \equiv \#(G/H) (p)$, so $p | \#\text{Fix}(H)$. Now $gH \in \text{Fix}(H)$ iff for all $h \in H$ we have

$$hgH = gH \iff hgHg^{-1} = gHg^{-1} \iff h \in gHg^{-1}$$

so $gH \in \text{Fix}(H)$ iff $H \subset gHg^{-1}$. Since these groups have the same order, we see that $gH \in \text{Fix}(H)$ iff $g \in N_G(H)$, so $\text{Fix}(H) = N_G(H)/H$. 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 $p \cdot p^i = p^{i+1}$. \hfill $\square$

**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 $\text{Syl}_p(G)$ for the set of such subgroup and $n_p(G) = \#\text{Syl}_p(G)$ 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 $P' < P$. □

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

**Proof.** Let $P$ be a $p$-Sylow subgroup, and consider the action of $P$ on $\text{Syl}_p(G)$ by conjugation. Then $P$ fixes $P' \in \text{Syl}_p(G)$ 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 $\{P^g\}_{g \in G} \subset \text{Syl}_p(G)$ be the set of $p$-Sylow subgroups conjugate to $P$. The size of this set is $|G : N_G(P)| \cdot |G : P|$ and is therefore prime to $p$ (in fact, it is $\equiv 1 \pmod{p}$ 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 $\text{Syl}_p(G)$ is $P'$ itself, so $P'$ is conjugate to $P$. It follows that $n_p(G) = |G : N_G(P)|$, which divides $n$. □

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

**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 $C_4 \times C_3$.

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

**Case 1.** $n_3(G) = 4$. Then the action of $G$ by conjugation on $\text{Syl}_3(G)$ 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 $2^4 / 3! = 8$ 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 $G \cong A_4$.

**Case 2.** $n_3(G) = 1$. Then $G \cong P_2 \times P_3$, 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 ($G \cong P_2 \times P_3$). Then either $G \cong C_4 \times C_3 \cong C_{12}$ or $G \cong C_2 \times C_2 \times C_3$. Here $n_2(G) = 1$.

**Case ii.** The action is non-trivial and $P_2 \cong V$. Since $\text{Aut}(C_3) \cong C_2$, we can write $V \cong K \times C_2$ where $K$ is the kernel of the action. Then $G \cong K \times (C_2 \times C_3) \cong C_2 \times S_3$. Here $n_2(G) = 3$ since $P_2$ does not commute with $P_3$.

**Case iii.** The action is non-trivial and $P_2 \cong C_4$. Since there is a unique non-trivial homomorphism $C_4 \to C_2$ (reduction mod 2), there is a unique semidirect product $C_4 \rtimes C_3$. Here also $n_2(G) = 3$. □

**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. □

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

**Example 207.** Let $G$ be a simple group of order 60. Then $G \cong A_5$. 36
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

\[
\begin{align*}
n_2 & \in \{5, 15\} , n_3 = 10, n_5 = 6 .
\end{align*}
\]

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 \( \text{Syl}_3(G) \) 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

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

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

\[
A \cong \prod_p A_p,
\]

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 elements of order 4 mod elements 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 \( C^3_2 \).

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 \( A \cong \mathbb{Z}^r \times A_{\text{tors}} \) 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 $\prod_{i=1}^{r} C_{p^{r_i}} \cong \prod_{j=1}^{s} C_{p^{f_j}}$. Then $r = s$ and $f_j = e_{\sigma(j)}$ for some $\sigma \in S_r$.

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

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

and for the same reason

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

By induction on the order of $A$, both products have the same number of factors, so in particular $r' = \# \{i \mid e_i > 1\} = \# \{i \mid f_j > 1\}$ 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. □

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

**Claim 214.** The map $h_e : (\mathbb{Z}/p^e \mathbb{Z})^{l_e} \to A$ given by

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

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 $\bar{x} = p^k \bar{x}' \in \text{Ker}(h_e)$. For such $k$ and $x'_i$ we have

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

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

$$\sum_i x'_i \cdot c_{e,i} = 0$$

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

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 $a - b \in \text{Ker}(f_e) = A[p^{e-1}]$ 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 $f_{e-1} : A[p^{e-1}] \to A[p]$ 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 $f_{e-1}(A[p^{e-1}]) \supset f_e(A)$.
- Let $\{c_{e-1,i}\}_{i=1}^{l_{e-1}} \subset f_{e-1}(A[p^{e-1}])$ extend $\{c_{e,i}\}_{i=1}^{l_e}$ to a basis of $f_{e-1}(A[p^{e-1}])$.
- Let $\{b_{e-1,i}\}_{i=1}^{l_{e-1}} \subset A[p^{e-1}]$ 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 $\{b_{e-1,i}\}_{i=1}^{l_{e-1}}$.

CLAIM 216. The map $h_{e-1} : (\mathbb{Z}/p^{e} \mathbb{Z})^{l_e} \times (\mathbb{Z}/p^{e-1} \mathbb{Z})^{l_{e-1}} \to A$ given by 

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

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

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 $\{b_{e,i}\} \cup \{b_{e-1,i}\}$. To compute the kernel suppose 

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

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 $x^e_i$ are all divisible by $p$. Now let $k \leq e-1$ be maximal such that there is $(x^e_i, x^{e-1}_i) \in \text{Ker}h_{e-1}$ with $x^{e-1}_i$ divisible by $p^k$, $x^e_i$ divisible by $p^{k+1}$. Multiply by $p^{e-1-k}$ we get $\bar{x}^e_i, x^{e-1}_i$, not all zero mod $p$, such that 

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

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

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. \( \square \)

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

**Proof.** Let \( A_{\text{tors}} \) be the torsion subgroup. Then \( A/A_{\text{tors}} \) is finitely generated and torsion-free, hence isomorphic to \( \mathbb{Z}^r \) for some \( r \). Let \( s : \mathbb{Z}^r \rightarrow A \) 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 \( A \simeq \mathbb{Z}^r \times A_{\text{tors}} \). This shows \( A_{\text{tors}} \simeq A/\mathbb{Z}^r \) so \( A_{\text{tors}} \) is also finitely generated, hence finite. \( \square \)
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 $Z(G/Z^i(G))$. For example $Z^1(G) = Z(G)$.

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

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

DEFINITION 227. This is called the ascending central series.

EXAMPLE 228. Let $U_n = \left\{ \begin{pmatrix} 1 & * & * \\ & \ddots & * \\ & & 1 \end{pmatrix} \right\} \subset \text{GL}_n(F)$ 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.


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 $N \triangleleft G$. 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 $p^aq^b$ is solvable.

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

**Lemma 238.** $G/N$ is abelian iff $G' \subseteq N$.

Now let $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_k = \{e\}$ with $G_i/G_{i+1}$ abelian. Then $G' \subseteq G_1$. Replace $G_1$ with $G'$. Then $G_2 \cap G' \triangleleft G'$ 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.** $K \text{ char } N \Rightarrow K \text{ char } G$. 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 $G = Q \rtimes H$ 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