Math 322: Introduction to Group Theory
Lecture Notes

Lior Silberman

These are rough notes for the Fall 2014 course. Solutions to problem sets were posted on an internal website.

Contents

Introduction

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

0.1. Administrivia

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

0.2. Motivation

> Coxeter came to Cambridge and he gave a lecture, then he had this problem ... I left the lecture room thinking. As I was walking through Cambridge, suddenly the idea hit me, but it hit me while I was in the middle of the road. When the idea hit me I stopped and a large truck ran into me ... So I pretended that Coxeter had calculated the difficulty of this problem so precisely that he knew that I would get the solution just in the middle of the road ... One consequence of it is that in a group if $a^2 = b^3 = c^5 = (abc)^{-1}$, then $c^{610} = 1$.
>
> *J.H. Conway, Math. Intelligencer v. 23 no. 2 (2001)*

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

0.3. Course plan (subject to revision) (Lecture 1, 6/1/13)

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

Math 322 Fall 2014: Problem Set 1, due 11/9/2014

Practice and supplementary problems, and any problems specifically marked "OPT" (optional), "SUPP" (supplemenetary) or "PRAC" (practice) are *not for submission*. It is possible that the grader will not mark all problems.

Practice problems

P1 Find all solutions to the congruence $5x \equiv 1\,(7)$.

The following problem is a review of the axioms for a vector space.

P2 Let X be a set. Carefully show that pointwise addition and scalar multiplication endow the set $\mathbb{R}^X$ of functions from X to $\mathbb{R}$ with the structure of an $\mathbb{R}$-vectorspace. Meditate on the case $X = [n] = \{0, 1, \ldots, n-1\}$.

P3 (Euclid's Lemma) Let a, b, q, r be four integers with $b = aq + r$. Show that the pairs $\{a, b\}$ and $\{a, r\}$ have the same sets of common divisors, hence the same greatest common divisor.

The integers

1. Show that for any integer k, one of the integers $k, k+2, k+4$ is divisible by 3.

2. Consider the equation $13x + 5y = 1$ for unknowns $x, y \in \mathbb{Z}$.
   PRAC Exhibit a solution.
   (a) Exhibit infinitely many solutions.
   (*b) Show that you found *all* the solutions.

3. Let a, n be positive integers and let $d = \gcd(a, n)$. Show that the equation $ax \equiv 1\,(n)$ has a solution iff $d = 1$.

4. Let $f\colon \mathbb{Z} \to \mathbb{Z}$ be *additive*, in that for all $x, y \in \mathbb{Z}$ we have $f(x+y) = f(x) + f(y)$.
   PRAC Check that for any $a \in Z$, $f_a(x) = ax$ is additive.
   (a) Show that $f(0) = 0$ (hint: $0 + 0 = 0$).
   (b) Show that $f(-x) = -f(x)$ for all $x \in \mathbb{Z}$.
   (c) Show by induction on n that for all $n \geq 1$, $f(n) = f(1) \cdot n$.
   (d) Show that every additive map is of the form f_a for some $a \in \mathbb{Z}$.
   RMK Let H be the set of additive maps $\mathbb{Z} \to \mathbb{Z}$. We showed that the function $\varphi\colon H \to \mathbb{Z}$ given by $\varphi(f) = f(1)$ is a bijection (with inverse $\psi(a) = f_a$).
   SUPP Show that the bijections φ, ψ are themselves additive maps (addition in H is defined pointwise).

Supplementary problems I: Functions, sets and relations

The following problem will be used in the upcoming discussion of permutations.

A. Let X, Y, Z, W be sets and let $f\colon X \to Y$, $g\colon Y \to Z$ and $h\colon Z \to W$ be functions. Recall that the *composition* $g \circ f$ is the function $g \circ f\colon X \to Z$ such that $(g \circ f)(x) = g(f(x))$ for all $x \in X$.
   (a) Show that composition is *associative*: that $h \circ (g \circ f) = (h \circ g) \circ f$ (recall that functions are equal if they have the same value at every x).
   (b) f is called *injective* or *one-to-one* (1:1) if $x \neq x'$ implies $f(x) \neq f(x')$. Show that if $g \circ f$ is injective then so is f.
   (c) g is called *surjective* or *onto* if for every $z \in Z$ there is $y \in Y$ such that $g(y) = z$. Show that if $g \circ f$ is surjective then so is g.
   (d) Suppose that f, g are both surjective or both injective. In either case show that the same holds for $g \circ f$.
   (e) Give an example of a set X and $f, g\colon X \to X$ such that $f \circ g \neq g \circ f$.

The following problem is intended to help clarify the construction of $\mathbb{Z}/n\mathbb{Z}$. See also section 0.1 of Dummit and Foote.

B. A relation R between elements of a set X is (1) *reflexive* if xRx for every $x \in X$; (2) *symmetric* if for any x, y, xRy implies yRx (3) *transitive* if for any x, y, z, if xRy and yRz then xRz. Example: $<$ on $\mathbb{R}$ isn't reflexive ($3 < 3$ doesn't hold), isn't symmetric ($3 < 5$ holds but $5 < 3$ doesn't) by is transitive (if $x < y$ and $y < z$ then $x < z$).
   (a) Decide which of the properties holds for the relations $=, \leq$ on $\mathbb{R}$.
   (b) Ditto where R is the relation on $\mathbb{R}$ given by $xRy \leftrightarrow |x - y| \leq 1$ (so $\frac{1}{2} R \frac{3}{4}$ holds but $0R2$ doesn't).
   (c) Ditto where $aRb \leftrightarrow ab > 0$ on $\mathbb{Z}$ and where $aRb \leftrightarrow ab \geq 0$ on $\mathbb{Z}$.

   DEF An *equivalence relation* is one satisfying all of (1),(2),(3).

   (d) On the set of integers $\mathbb{Z}$ show that the relation "a, b are both even or both odd" is an equivalence relation (in detail: you need to show that for any a "a, a are both even or both odd" that "if a, b are both even or both odd then also b, a are both even or both odd" and that "if a, b are both even or both odd, and if b, c are both even or both odd" then "a, c are both even or both odd"

Supplementary Problems II: Subsemigroups of $(\mathbb{Z}_{\geq 0}, +)$

C. The Kingdom of Ruritania mints coins in the denominations $d_1, \ldots, d_r$ Marks (d_i are positive integers, of course). Let $d = \gcd(d_1, \ldots, d_r)$.
   (a) Show that every payable sum (total value of a combination of coins) is a multiple of d Marks.
   (b) Show that there exists $N \geq 1$ such that any multiple of d Marks exceeding N can be expressed using the given coins.
   (c) Let $H \subset \mathbb{Z}_{\geq 0}$ be the set of sums that can be paid using the coins. Show that H is closed under addition.

   DEF H is called the *subsemigroup of* $\mathbb{Z}_{\geq 0}$ *generated* by $\{d_1, \ldots, d_r\}$.

D. (partial classification of subsemigroups of $\mathbb{Z}_{\geq 0}$) Let $H \subset \mathbb{Z}_{\geq 0}$ be closed under addition.
   (a) Show that either $H = \{0\}$or there are $N, d \geq 1$ such that d divides every element of h, and such that H contains all multiples of d exceeding N.
   Hint: Enumerate the elements of H in increasing order as $\{h_i\}_{i=1}^{\infty}$ and consider the sequence $\{\gcd(h_1, \ldots, h_m)\}_{m=1}^{\infty}$.
   (b) Conclude that H is *finitely generated*: there are $\{d_1, \ldots, d_r\} \subset H$ such that H is obtained as in problem C.

Supplementary Problems III: Additive groups in $\mathbb{R}$.

E. (just linear algebra)
   (a) Show that the usual addition and multiplication by rational numbers endow $\mathbb{R}$ with the structure of a vector space over the field $\mathbb{Q}$.
   (b) Let $f: \mathbb{R} \to \mathbb{R}$ be additive ($f(x+y) = f(x) + f(y)$). Show that f is $\mathbb{Z}$-linear: that $f(nx) = nf(x)$ for all $x \in \mathbb{R}, n \in \mathbb{Z}$.
   (c) Show that f is $\mathbb{Q}$-linear: $f(rx) = rf(x)$ for all $r \in \mathbb{Q}$.
   (d) Let $B \subset \mathbb{R}$ be a basis for $\mathbb{R}$ as a $\mathbb{Q}$-vector space (this is called a *Hamel basis*). Use B to construct a $\mathbb{Q}$-linear map $\mathbb{R} \to \mathbb{R}$ which is not of the form $x \mapsto ax$.

F. (add topology ...) Let $f: \mathbb{R} \to \mathbb{R}$ be additive.
   (a) Suppose that f is *continuous*. Show that $f(x) = ax$ where $a = f(1)$.
   (b) (If you have taken Math 422) Suppose that f is *Lebesgue* (*or Borel*) *measurable*. Show that there is $a \in \mathbb{R}$such that $f(x) = ax$ a.e.
   (c) ("$\mathbb{R}$ has no field automorphisms") Let $f: \mathbb{R} \to \mathbb{R}$satisfy $f(x+y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$. Show that either $f(x) = 0$ for all x or $f(x) = x$ for all x.

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.

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

EXAMPLE 4. $\{0\}$, all even integers. What else?

LEMMA 5 (Division with remainder). *Let $a,b \in \mathbb{Z}$with $a > 0$. Then there are unique q,r with $0 \le r < a$ such that*

$$b = qa + r\,.$$

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

(Uniqueness) Suppose that there are two solutions so that

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

We then have

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

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

PROPOSITION 6. *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 $b = qa$. □

1.1.2. Multiplicative structure (Lecture 2, 9/9/2014).

DEFINITION 7. Let $a, b \in \mathbb{Z}$. Say "*a divides b*" and write $a|b$ if there is c such that $b = ac$. Write $a \nmid b$ otherwise.

EXAMPLE 8. ± 1 divide every integer. Only ± 1 divide ± 1. Every integer divides 0, but only 0 divides 0. $2|14$ but $3 \nmid 14$. $|a|$ divides a.

THEOREM 9 (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 6 there is $d \in \mathbb{Z}_{>0}$ such that $H = \mathbb{Z}d$. Since $a, b \in H$ it follows that $d|a$, $d|b$ so d is a common divisor. Conversely, let x, y be such that $d = ax + by$ and let e be another common divisor. then $e|a, e|b$ so $e|ax, e|by$ so $e|ax + by = d$. In particular, $e \leq d$ so d is the *greatest* common divisor. □

ALGORITHM 10 (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:*

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

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

CLAIM 11. When $a_{n+1} = 0$ we have $a_n = \gcd(a, b)$.

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

REMARK 12. 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 13. $(69, 51) = (51, 18) = (18, 15) = (15, 3) = (3, 0) = (3)$. 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 14. Let $a, b, n \in \mathbb{Z}$ with $n \geq 1$. Say *a is congruent to b modulu n*, and wite $a \equiv b \ (n)$ if $n|b - a$.

LEMMA 15. *This is an equivalence relation.*

- Aside: Equivalence relations

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

LEMMA 16. *Suppose $a \equiv a'$, $b \equiv b'$. Then $a+b \equiv a'+b'$, $ab \equiv a'b'$.*

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

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

DEFINITION 17. Let $\mathbb{Z}/n\mathbb{Z}$ denote the quotient of $\mathbb{Z}$ by the equivalence relation $\equiv (n)$. Define on it arithmetic operations by

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

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

OBSERVATION 18. *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, 11/9/2014). Let $(\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \mathbb{Z}/n\mathbb{Z} \mid (a,n) = 1\}$.

LEMMA 19. *$(\mathbb{Z}/n\mathbb{Z})^\times$ is closed under multiplication and inverses.*

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

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

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

REMARK 20. Why exclude the ones not relatively prime? These can't have *inverse*s.

DEFINITION 21. 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 $(\mathbb{Z}/8\mathbb{Z})^\times$.

DEFINITION 22. *Euler's totient function* is the function $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$.

LEMMA 23. *$\sum_{d|n} \phi(n) = n$.*

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

1.1.5. Primes and unique factorization.

DEFINITION 24. Call *p prime* if it has no divisors except 1 and itself.

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

COROLLARY 25. *$p|ab$ iff $p|a$ or $p|b$.*

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

THEOREM 26 (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

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

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

DEFINITION 27. Call *n, m relatively prime* if $\gcd(n,m) = 1$.

Next comes our first non-trivial isomorphism.

THEOREM 28 (Chinese Remainder Theorem). *Let $N = n_1 n_2$ with n_1, n_2 relatively prime. Then the map*

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

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

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

$$n_1 x_1 + n_2 y = 1\,.$$

Let $b_1 = n_2 y$ and let $b_2 = n_1 x$. Then:

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

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

$$\begin{aligned} f([a_1 b_1 + a_2 b_2]_N) &= ([a_1]_{n_1} \cdot [1]_{n_1}, [a_1]_{n_2} \cdot [0]_{n_2}) + ([a_2]_{n_1} \cdot [0]_{n_1}, [a_2]_{n_2} \cdot [1]_{n_2}) \\ &= ([a_1]_{n_1}, [0]_{n_2}) + ([0]_{n_1}, [a_2]_{n_2}) = ([a_1]_{n_1}, [a_2]_{n_2})\,. \end{aligned}$$

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

REMARK 29. Meditate on this. Probably first example of a non-obvious isomorphism, and a non-obvious "basis".

Math 322 Fall 2014: Problem Set 2, due 18/9/2014

Practice and supplementary problems, and any problems specifically marked "OPT" (optional), "SUPP" (supplemenetary) or "PRAC" (practice) are *not for submission*. It is possible that the grader will not mark all problems.

Practice: modular arithmetic

P1. Evaluate:
   (a) $[3]_6+[5]_6+[9]_6$, $[3]_7+[5]_7+[9]_7$, $[2]_{13}\cdot[5]_{13}\cdot[7]_{13}$.
   (b) $([3]_8)^n$ (hint: start by finding $([3]_8)^2$).

P2. Linear equations.
   (a) Use Euclid's algorithm to solve $[5]_7x=[1]_7$.
   (b) Solve $[5]_7y=[2]_7$ by multiplying both sides by the element from (a).
   (c) Solve $\begin{cases} 2x+3y+4z &= 1 \\ x+y &= 3 \\ x+2z &= 6 \end{cases}$ in $\mathbb{Z}/7\mathbb{Z}$ (imagine all numbers are surrounded by brackets).

Number Theory

1. (Modular arithmetic)
   (a) Evaluate $([3]_{13})^n$, $n\in\mathbb{Z}_{\geq 0}$.
   – Check that $2^{12}\equiv 1\,(13)$.
   (b) Let k be the smallest positive integer such that $2^k\equiv 1\,(13)$. Show that $k|12$ (hint: division with remainder).
   – Check that $2^6\equiv -1\,(13)$, $2^4\equiv 3\,(13)$.
   (c) Use the last check to show that $k=12$.
   (d) Show that $2^i\equiv 2^j\,(13)$ iff $i\equiv j\,(12)$.

2. (The Chinese Remainder Theorem)
   (a) Let p be an odd prime. Show that the equation $x^2=[1]_p$ has exactly two solutions in $\mathbb{Z}/p\mathbb{Z}$ (hint: what does it mean that $x^2\equiv 1\,(p)$ for $x\in\mathbb{Z}$?) (aside: what about $p=2$?)
   (b) We will find all solutions to the congruence $x^2\equiv 1\,(91)$.
      (i) Find a "basis" a,b such that $a\equiv 1\,(7)$, $a\equiv 0\,(13)$ and $b\equiv 0\,(7)$, $b\equiv 1\,(13)$.
      (ii) Solve the congruence mod 7 and mod 13.
      (iii) Find all solutions mod 91.

Permutation Groups

3. On the set $\mathbb{Z}/12\mathbb{Z}$ consider the maps $\sigma(a)=a+[4]$ and $\tau(a)=[5]a$ (so $\sigma([2])=[6]$ and $\tau([2])=[10]$)
   DEF $(f\circ g)(x)=f(g(x))$ is composition of functions.
   (a) Find maps σ^{-1},τ^{-1} such that $\sigma\circ\sigma^{-1}=\sigma^{-1}\circ\sigma=\tau\circ\tau^{-1}=\tau^{-1}\circ\tau=\mathrm{id}$.
   (b) Compute $\sigma\tau,\tau\sigma,\sigma^{-1}\tau$.
   (c) For each $a\in\mathbb{Z}/12\mathbb{Z}$ compute $a,\sigma(a),\sigma(\sigma(a))$ and so on until you obtain a again. How many distinct cycles arise? List them.
   RMK The relation "a,b are in the same cycle" is an equivalence relation.

SUPP [R1.29] On $\mathbb{Z}/11\mathbb{Z}$ let $f(x)=4x^2-3x^7$. Show that f is a permutation and find its cycle structure and its inverse.

4. Let X be a set, $i \in X$. Say $\sigma \in S_X$ *fixes* i if $\sigma(i) = i$, and let $P_i = \mathrm{Stab}_{S_X}(i) = \{\sigma \in S_X \mid \sigma(i) = i\}$ be the set of such permutations.
   (a) Show that P_i is closed under composition and under inverses (if $\sigma, \tau \in P_i$ then $\sigma \circ \tau$ and $\sigma^{-1} \in P_i$). (hint: given $\sigma(i) = i$ and $\tau(i) = i$, check that $(\sigma \circ \tau)(i) = i$)
   — Suppose that $\rho(i) = j$ for some $\rho \in S_X$. Define $f\colon S_X \to S_X$ by $f(\sigma) = \rho \circ \sigma \circ \rho^{-1}$.
   (b) Show that $f(\sigma \circ \tau) = f(\sigma) \circ f(\tau)$ for all $\sigma, \tau \in S_X$ (hint: what is the definition of f?). Show that $f(\sigma^{-1}) = (f(\sigma))^{-1}$ (hint: PS1 problem 4(b))
   (c) Show that if $\sigma \in P_i$ then $f(\sigma) \in P_j$ (hint: what's $\rho^{-1}(j)$?)
   (d) Show that f is a bijection ("isomorphism") between P_i and P_j (hint: find its inverse)

Operations in a set of sets

Let X be a set, $P(X)$ (the "powerset") the set of its subsets (so $P(\{0,1\}) = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$.
The *difference* of $A, B \in P(X)$ is the set $A - B \stackrel{\text{def}}{=} \{x \in A \mid x \notin B\}$ (so $[0,2] - [-1,1] = (1,2]$).
The *symmetric difference* is $A \Delta B \stackrel{\text{def}}{=} (A - B) \cup (B - A)$ (so $[0,2] \Delta [-1,1] = [-1,0) \cup (1,2]$).

5. (Checking that $(P(X), E, \Delta)$ is a commutative group).
   PRAC Show that $A \Delta B$ is the set of $x \in X$ which belong to *exactly one* of A, B. Note that this shows the *commutative law* $A \Delta B = B \Delta A$.
   (a) (associative law) Show that for all $A, B, C \in X$ we have $(A \Delta B) \Delta C = A \Delta (B \Delta C)$.
   (b) (neutral element) Find $E \in P(X)$ such that $A \Delta E = A$ for all $A \in P(X)$.
   (c) (negatives) For all $A \in P(X)$ find a set $\bar{A} \in P(X)$ such that $A \Delta \bar{A} = E$.

6. (A quotient construction) Fix $N \in P(X)$ and say that $A, B \in P(X)$ *agree away from* N if $A - N = B - N$. Denote this relation $\sim$ during this problem. For example, as subsets of $\mathbb{R}$, the intervals $[-1,1]$ and $[0,1]$ agree "away from the negative reals".
   PRAC Show that $A \sim B$ iff for all $x \in X - N$ either x belong to both A, B or to neither.
   (a) Show that $\sim$ is an equivalence relation. We will use $[A]$ to denote the equivalence class of $A \subset X$ under $\sim$.
   (b) Show that if $A \sim A'$, $B \sim B'$ then $(A \Delta B) \sim (A' \Delta B')$.
   RMK This means the operation $[A] \tilde{\Delta} [B] \stackrel{\text{def}}{=} [A \Delta B]$ is well-defined: it does not depend on the choice of representatives.
   (c) Show that every equivalence class has a *unique* element which also belongs to $P(X - N)$ (that is, exactly one element of the class is a subset of $X - N$).
   (d) Show that $P(X - N) \subset P(X)$ is non-empty and closed under Δ (it is automatically closed under the "bar" operation of 5(c))
   RMK It follows that $\left(P(X)/\sim, [\emptyset], \tilde{\Delta}\right)$ and $(P(X - N), \emptyset, \Delta)$ are essentially the same algebraic structure (there is an operation-preserving bijection between them). We say "they are *isomorphic*".

Supplementary Problems I: The Fundamental Theorem of Arithmetic

If you haven't seen this before, you *must* work through problem A.

A. By definition the empty product (the one with no factors) is equal to 1, and a product with one factor is equal to that factor.
   (a) Let n be the smallest positive integer which is not a product of primes. Considering the possilibities that $n = 1$, n is prime, or that n is neither, show that n does not exist. Conclude that every positive integer is a product of primes.
   (b) Let $\{p_i\}_{i=1}^r$, $\{q_j\}_{j=1}^s$ be sequences of primes, and suppose that $\prod_{i=1}^r p_i = \prod_{j=1}^s q_j$. Show that p_r occurs among the $\{q_j\}$ (hint: p_r divides a product ...)
   (c) Call two representations $n = \prod_{i=1}^r p_i = \prod_{j=1}^s q_j$ of $n \geq 1$ as a product of primes *essentially the same* if $r = s$ and the sequences only differ in the order of the terms. Let n be the smallest integer with two essentially different representations as a product of primes. Show that n does not exist.

The following problem is for your amusement only; it is not relevant to Math 322 in any way.

B. (The p-adic absolute value)
   (a) Show that every non-zero rational number can be written in the form $x = \frac{a}{b}p^k$ for some non-zero integers a, b both prime to p and some $k \in \mathbb{Z}$. Show that k is *unique* (only depends on x). By convention we set $k = \infty$ if $x = 0$ ("0 is divisible by every power of p").

   DEF The *p-adic absolute value* of $x \in \mathbb{Q}$ is $|x|_p = p^{-k}$ (by convention $p^{-\infty} = 0$).

   (b) Show that for any $x, y \in \mathbb{Q}$, $|x+y|_p \leq \max\left\{|x|_p, |y|_p\right\} \leq |x|_p + |y|_p$ and $|xy|_p = |x|_p\,|y|_p$ (this is why we call $|\cdot|_p$ an "absolute value").
   (c) Fix $R \in \mathbb{R}_{\geq 0}$. Show that the relation $x \sim y \iff |x-y|_p \leq R$ is an equivalence relation on $\mathbb{Q}$. The equivalence classes are called "balls of radius R" and are usually denoted $B(x,R)$ (compare with the usual absolute value).
   (d) Show that $B(0,R) = \left\{x \,\middle|\, |x|_p \leq R\right\}$ is non-empty and closed under addition and subtraction. Show that $B(0,1) = \left\{x \,\middle|\, |x|_p \leq 1\right\}$ is also closed under multiplication.

Supplementary Problem II: Permutations and the pigeon-hole principle

C. (a) Prove by induction on $n \geq 0$: Let X be any finite set with n elements, and let $f\colon X \to X$ be either surjective or injective. Then f is bijective.
   (b) conclude that if X, Y are sets of the same size n and $f\colon X \to Y$ and $g\colon Y \to X$ satisfy $f \circ g = \mathrm{id}_Y$ then $g \circ f = \mathrm{id}_X$ and the functions are inverse.

Supplementary Problem II: Cartesian products and the CRT

NOTATION. For sets X, Y we write X^Y for the set of functions from Y to X.

D. Let I be an index set, A_i a family of sets indexed by I (in other words, a set-valued function with domain I). The *Cartesian product* of the family is the set of all touples such that the ith element is chosen from A_i, in other words:

$$\prod_{i\in I} A_i = \left\{ a \in \left(\bigcup_{i\in I} A_i \right)^I \;\middle|\; \forall i \in I : a(i) \in A_i \right\}$$

(we usually write a_i rather than $a(i)$ for the ith member of the touple).

(a) Verify that for $i = \{1,2\}$, $A_1 \times A_2$ is the set of pairs.

(b) Give a natural bijection

$$\left(\prod_{i\in I} A_i \right)^B \leftrightarrow \prod_{i\in I} \left(A_i^B \right) .$$

(you have shown: a vector-valued function is the same thing as a vector of functions).

(b) Let $\{V_i\}_{i\in I}$ be a family of vector spaces over a fixed field F (say $F = \mathbb{R}$). Show that pointwise addition and multiplication endow $\prod_i V_i$ with the structure of a vector space.

DEF This vector space is called the *direct product* of the vector spaces $\{V_i\}$.

RMK Recall that, if W is another vector space, then the set $\mathrm{Hom}_F(W,V)$ of linear maps from W to V is itself a vector space.

(*c) Let W be another vector space. Show that the bijection of (a) restricts to an isomorphism of vector spaces

$$\mathrm{Hom}_F \left(W, \prod_{i\in I} V_i \right) \to \prod_{i\in I} \mathrm{Hom}_F \left(W, V_i \right) .$$

E. (General CRT) Let $\{n_i\}_{i=1}^r$ be divisors of $n \geq 1$.

(a) Construct a map

$$f \colon \mathbb{Z}/n\mathbb{Z} \to \prod_{i=1}^{r} \left(\mathbb{Z}/n_i\mathbb{Z} \right) ,$$

generalizing the case $r = 2$ discussed in class.

(b) Show that f respects modular addition and multiplication.

(*c) Suppose that $n = \prod_{i=1}^r n_i$ and that the n_i are pairwise relatively prime (for each $i \neq j$, $\gcd\left(n_i, n_j\right) = 1$. Show that f is an isomorphism.

1.2. S_n

1.2.1. Permutations: concerete and abstract.

DEFINITION 30. Let X be a set. A *permutation* on X is a bijection $\sigma\colon X \to X$ (a function which is $1:1$ and onto). The set of all permutations will be denoted S_X and called the *symmetric group*.

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

LEMMA 31. *Composition of functions is associative. The identity function* $\mathrm{id}_X : X \to X$ *belongs to the symmetric group and is an identity for composition.*

EXAMPLE 32. $\begin{pmatrix}1\\1\end{pmatrix}$, $\begin{pmatrix}1&2\\2&1\end{pmatrix}$, $\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}$. The identity map. Non-example $\begin{pmatrix}1&2\\1&1\end{pmatrix}$.

LEMMA 33. *Let $\sigma\colon X \to X$ be a function.*

(1) $\sigma\colon X \to X$ is a bijection iff there is a "compositional inverse" $\bar{\sigma}\colon X \to X$ such that $\sigma \circ \bar{\sigma} = \bar{\sigma} \circ \sigma = \mathrm{id}$.

(2) S_X is closed under composition and compositional inverse.

(3) Suppose $\sigma \in S_X$ and that $\sigma\tau = \mathrm{id}$ or that $\tau\sigma = \mathrm{id}$. Then $\tau = \bar{\sigma}$. In particular, the compositional inverse is unique *and will be denoted σ^{-1}.*

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

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

REMARK 34. Note that S_X is not commutative! $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ but $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$.
Also, note that $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ – can have $\sigma^{-1} = \sigma$ ("involution").

LEMMA 35. $\#S_n = n!$.

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

1.2.2. Cycle structure.

DEFINITION 36. For $r \geq 2$ call $\sigma \in S_X$ an *r-cycle* if there are distinct $i_1, \ldots, i_r \in X$ such that $\sigma(i_j) = i_{j+1}$ for $1 \leq j \leq r-1$, suich that $\sigma(i_r) = i_1$, and that $\sigma(i) = i$ if $i \neq i_j$ for all j.

EXAMPLE 37. $\begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix}$, $\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}$, $\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$.

DEFINITION 38. Let $\sigma \in S_X$. Set $\mathrm{supp}(\sigma) = \{i \in X \mid \sigma(i) \neq i\}$.

LEMMA 39. *σ, σ^{-1} have the same support. Suppose σ, τ have disjoint supports. Then $\sigma\tau = \tau\sigma$.*

PROOF. $\sigma(i) = i$ iff $\sigma^{-1}(i) = i$. If $i \in \text{supp}(\sigma)$ 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 σ, τ there's nothing to prove. □

THEOREM 40 ("Prime factorization"). *Every permutation on a finite set is a product of disjoint cycles. Furthermore, the representation is essentially unique: if we add a "1-cycle"(i) for each fixed point, the factorization is unique up to order of the cycles.*

PROOF. Let σ be a counterexample with mininal support. Then $\sigma \neq \text{id}$, 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 κ be the resulting cycle. Then $\kappa^{-1}\sigma$ agrees with σ off $\{i_j\}$ and fixes each i_j. Factor this and multiply by κ.

For uniqueness note that the cycles can be intrinsically defined. □

EXAMPLE 41. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 2 & 1 & 5 & 7 & 4 \end{pmatrix} = (1674)(23)(5)$.

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

LEMMA 42. *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 43. 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 44. A_n is closed under multiplication and inverses, so it is a subgroup of S_n.

LEMMA 45. *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. □

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

EXAMPLE 46. $(17)(1674)(23)(5) = (16)(74)(23)(5)$ while $(12)(1674)(23)(5) = (167423)(5)$.

DEFINITION 47. 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 σ.

LEMMA 48. *Let τ 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. □

THEOREM 49. *For all $\tau, \sigma \in S_n$ we have* $\text{sgn}(\tau\sigma) = \text{sgn}(\tau)\,\text{sgn}(\sigma)$.

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

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

By Lemma 42 we see that $H = S_n$ and the claim follows. □

COROLLARY 50. *If $\sigma = \prod_{i=1}^{r} \tau_i$ with each τ_i are transposition then $\operatorname{sgn}(\tau) = (-1)^r$, and in particular the parity of r depends on σ but not on the representation.*

COROLLARY 51. *For $n \geq 2$, $\#A_n = \frac{1}{2}\#S_n$.*

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

EXERCISE 52. A_n is generated by the cycles of length 3.

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

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

LEMMA 53. *Every $g \in \mathrm{GL}_n(\mathbb{R})$ has an inverse.*

SUMMARY 54. $(\mathrm{GL}_n(\mathbb{R}), \cdot)$ is a group.

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

EXERCISE 55. (Some subgroups)

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

Math 322: Problem Set 3 (due 25/9/2014)

Practice problems

P1 Which of the following are groups? If yes, prove the group axioms. If not, show that an axiom fails.

(a) The "half integers" $\frac{1}{2}\mathbb{Z} = \left\{\frac{a}{2} \mid a \in \mathbb{Z}\right\} \subset \mathbb{Q}$, under addition.

(b) The "dyadic integers" $\mathbb{Z}[\frac{1}{2}] = \left\{\frac{a}{2^k} \mid a \in \mathbb{Z}, k \geq 0\right\} \subset \mathbb{Q}$, under addition.

(c) The non-zero dyadic integers, under multiplication.

P2. [DF1.1.7] Let $G = [0,1)$ be the half-open interval, and for $x, y \in G$ define $x * y = \begin{cases} x+y & \text{if } x+y < 1 \\ x+y-1 & \text{if } x+y \geq 1 \end{cases}$.

(a) Show that $(G, *)$ is a commutative group. It is called "$\mathbb{R}$ mod $\mathbb{Z}$".

(b) Give an alternative construction of G using the equivalence relation $x \equiv y\,(\mathbb{Z})$ if $x - y \in \mathbb{Z}$

P3. [DF1.1.9] Let $F = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\} \subset \mathbb{R}$.

(a) Show that $(F, +)$ is a group.

(*b) Show that $(F \setminus \{0\} \cdot)$ is a group.

RMK Together with the distributive law, (a),(b) make F a *field*.

P4*. Show that S_n contains $(n-1)!$ n-cycles.

Symmetric Groups

1. (Generation of the alternating group)

(a) Let β be an r-cycle. Show that $\beta \in A_n$ iff r is odd.

(b) Show that every element of A_n is a product of 3-cycles (hint: start with $(12)(13) \in A_3$ and $(12)(34) \in A_4$).

RMK You have shown "the subgroup of S_n generated by the 3-cycles is A_n".

2. Call $\sigma, \tau \in S_X$ *conjugate* if there is $\rho \in S_X$ such that $\tau = \rho\sigma\rho^{-1}$.

(a) Show that "σ is conjugate to τ" is an equivalence relation.

(*b) Let β be an r-cycle. Show that $\rho\beta\rho^{-1}$ is also an r-cycle.

(c) Show that if $\sigma = \prod_{i=1}^{t} \beta_i$ is the cycle decomposition of σ, then $\rho\sigma\rho^{-1} = \prod_{i=1}^{t} \left(\rho\beta_i\rho^{-1}\right)$ is the cycle decomposition of $\rho\sigma\rho^{-1}$.

RMK We have shown: if σ is conjugate to τ then they have the same *cycle structure*: for each r they have the same number of r-cycles.

(*d) Suppose σ, τ have the same cycle structure. Show that they are conjugate.

3. A *permutation matrix* is an $n \times n$ matrix which is zero except for exactly one 1 in each row and column (example: the identity matrix). The *Kroncker delta* is defined by $\delta_{a,b} = \begin{cases} 1 & a = b \\ 0 & a \neq b \end{cases}$.

(a) Given $\sigma \in S_n$ let $P(\sigma)$ be the matrix with $(P(\sigma))_{ij} = \delta_{i,\sigma(j)}$. Show that P is a bijection between S_n and the set of permutation matrices of size n.

(b) Show that $P\colon S_n \to M_n(R)$ has $P(\sigma\tau) = P(\sigma)P(\tau)$.

(c) Show that the image of P consists of invertible matrices.

RMK $\det(P(\sigma)) = \operatorname{sgn}(\sigma)$.

Groups and homomorphisms

4. Which of the following are groups? If yes, prove the group axioms. If not, show that an axiom fails.
   (a) The non-negative real numbers with the operation $x * y = \max\{x, y\}$.
   (b) $\mathbb{R} \setminus \{-1\}$ with the operation $x * y = x + y + xy$.

5. Let $*$ be an associative operation on a set G (that means $(x*y)*z = x*(y*z)$), and let $a \in G$. We make the rescursive definition $a^1 = a$, $a^{n+1} = a^n * a$ for $n \geq 1$.
   (a) Show by induction on m that if $n, m \geq 1$ then $a^n * a^m = a^{n+m}$ and $(a^n)^m = a^{nm}$.
   SUPP If G is a group, set $a^0 = e$ and $a^{-n} = \left(a^{-1}\right)^n$ and show that for all $n, m \in \mathbb{Z}$ we have $a^n * a^m = a^{n+m}$ and $(a^n)^m = a^{nm}$.
   — From now on suppose G is a group.
   (c) Let $\beta \in S_X$ be an r-cycle. Show that $\beta^r = \mathrm{id}$, while $\beta^k \neq \mathrm{id}$ if $1 < k < r$.
   (d) [R1.31] Let m, n be relatively prime integers and suppose that $a^m = e$. Show that there is $b \in G$ such that $b^n = a$ (hint: Bezout's Theorem).
   (e) Let $a \in G$ satisfy $a^n = e$ for some $n \neq 0$ and let $k \in \mathbb{Z}_{\geq 1}$ be minimal such that $a^k = e$. Show that $k | n$.
   DEF We call k the *order* of a. We have shown that $a^n = e$ iff n is divisible by the order of a.

6. Let G be a group, and suppose that $f(x) = x^{-1}$ is a group homomorphism $G \to G$. Show that $xy = yx$ for all $x, y \in G$ (we call such G *abelian*).

Supplementary Problems I: Permutations

A. In this problem we will give an alternative proof of the cycle decomposition of permutations. Fix a set X (which may be infinite) and a permutation $\sigma \in S_X$.
   (a) Define a relation $\sim$ on X by $i \sim j \leftrightarrow \exists n \in \mathbb{Z} : \sigma^n(i) = j$. Show that this is an equivalence relation.
   DEF We'll call the equivalence classes the *orbits* of σ on X.
   (b) Let O be an orbit, and let $\kappa_O = \sigma \restriction_O$ be the *restriction* of σ to O: the function $O \to X$ defined by $\kappa_O(i) = \sigma(i)$ if $i \in O$. Show that $\kappa_O \in S_O$ (note that you need to show that the range of κ_O is in O!)
   (c) Choose $i \in O$ and suppose O is finite, of size r. Show that κ_O is an r-cycle: that mapping $[j]_r \mapsto \kappa_O^j(i)$ gives a well-defined bijection $\mathbb{Z}/r\mathbb{Z} \to O$ (equivalently, that if we set $i_0 = i$, $i_1 = \sigma(i)$, $i_{j+1} = \sigma(i_j)$ and so on we get $i_r = i_0$).
   RMK Note that $r = 1$ is possible now – every fixed point is its own 1-cycle.
   (d) Choose $i \in O$ and suppose O is infinite. Show that κ_O is an infinite cycle: that mapping $j \mapsto \kappa_O^j(i)$ gives bijection $\mathbb{Z} \to O$.
   RMK We'd like to say

$$\sigma = \prod_{O \in X/\sim} \kappa_O$$

   but there very well may be infinitely many cycles if X is infinite. We can instead interpret this as σ being the union of the κ_O: for every $i \in X$ let O be the orbit of i, and then $\sigma(i) = \kappa_O(i)$.

B. In this problem we give an alternative approach to the sign character.

(a) For $\sigma \in S_n$ set $t(\sigma) = \#\{1 \le i < j \le n \mid \sigma(i) > \sigma(j)\}$ and let $s(\sigma) = (-1)^{t(\sigma)} = \begin{cases} 1 & t(\sigma) \text{ even} \\ 0 & t(\sigma) \text{ odd} \end{cases}$.
Show that for an r-cycle κ we have $s(\kappa) = (-1)^{r-1}$.

(b) Let $\tau \in S_n$ be a transposition. Show that $t(\tau\sigma) - t(\sigma)$ is odd, and conclude that $s(\tau\sigma) = s(\tau)s(\sigma)$.

(c) Show that $s\colon S_n \to \{\pm 1\}$ is a group homomorphism.

(d) Show that $s(\sigma) = \operatorname{sgn}(\sigma)$ for all $\sigma \in S_n$.

Supplementary Problems II: Automorphisms

C. (The automorphism group) Let G be a group.

(a) An isomorphism $f\colon G \to G$ is called an *automorphism* of A. Show that the set $\operatorname{Aut}(G)$ of all automorphisms of G is a group under composition.

DEF Fix $a \in G$. For $g \in G$ set $\gamma_a(g) = aga^{-1}$. This is called "*conjugation by a*".

(b) Show that $\gamma_a \in \operatorname{Hom}(G,G)$.

(*c) Show that $\gamma_a \in \operatorname{Aut}(G)$ and that the map $a \mapsto \gamma_a$ is a group homomorphism $G \to \operatorname{Aut}(G)$.

DEF The image of this map is called the group of *inner* automorphisms and is denoted $\operatorname{Inn}(G)$.

D. Let F be a field. A map $f\colon F \to F$ is an *automorphism* if it is a bijection and it respects addition and multiplication.

(a) Show that $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is an automorphism of the field from problem P3.

(b) Show that complex conjugation is an automorphism of the field of complex numbers.

RMK $\mathbb{C}$ has many other automorphisms.

(c) Supplementary Problem F to PS1 shows that $\operatorname{Aut}(\mathbb{R}) = \{\mathrm{id}\}$.

CHAPTER 2

Groups and homomorphisms

2.1. Groups, subgroups, homomorphisms (Lecture 6, 23/9/2014)

2.1.1. Groups.

DEFINITION 56 (Group). A *group* is a pair $(G,\cdot)$ where G is a set and $\cdot\colon G\times G\to G$ is a binary operation satisfying:

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

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

Fix a group G.

LEMMA 57 (Unit and inverse). *(1) $\bar{x}$ is a two-sided inverse: $x\bar{x}=e$ as well.*
(2) e is a two-sided identity: $\forall x:xe=x$.
(3) The identity and inverse are unique.
(4) $\bar{\bar{x}}=x$.

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

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

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

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

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

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

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

NOTATION 58. We write x^{-1} for the unique inverse to x. Then $\left(x^{-1}\right)^{-1}=x$.

REMARK 59. Because of this Lemma, quite often the axioms call for a two-sided identity and a two-sided inverse.

COROLLARY 60 (Cancellation laws). *Suppose $xy=xz$ or $yx=zx$ holds. Then $x=y$.*

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

COROLLARY 61. *e is the unique element of G satisfying $xx=x$.*

PROOF. Multiply by x^{-1}. □

EXAMPLE 62 (Examples of groups). (0) The trivial group.

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

EXAMPLE 63 (Non-groups). (1) $(\mathbb{Z}_{\geq 0},+)$.
(2) $(\mathbb{Z},\times)$, $(M_n(\mathbb{R}),+)$.
(3) $(\mathbb{Z}_{\geq 1},\mathrm{gcd})$. $(\mathbb{Z}_{\geq 1},\mathrm{lcm})$.

2.1.2. Homomorphisms.

PROBLEM 64. Are $(\mathbb{Z}/2\mathbb{Z},+)$ and $(\{\pm 1\},\times)$ the same group? Are $\mathbb{R}^+$and $\mathbb{R}^\times_{>0}$ the same group?

DEFINITION 65. Let $(G,\cdot),(H,*)$ be a groups. A *(group) homomorphism* from G to H is function $f\colon G \to H$ such that $f(x\cdot y) = f(x) * f(y)$ for all $x,y \in G$. Write $\mathrm{Hom}(G,H)$ for the set of homomorphisms.

EXAMPLE 66. Trivial homomorphism, $\mathrm{sgn}\colon S_n \to \{\pm 1\}$, $\det\colon \mathrm{GL}_n \to \mathrm{GL}_1$, the quotient map $\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$.

LEMMA 67. *Let $f\colon G \to H$ be a homomorphism. Then*
(1) $f(e_G) = e_H$.
(2) $f(g^{-1}) = (f(g))^{-1}$.

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

DEFINITION 68. $f \in \mathrm{Hom}\,(G,H)$ is called an *isomorphism* if it is a bijection.

PROPOSITION 69. *f is an isomorphism iff there exists $f^{-1} \in \mathrm{Hom}(H,G)$ such that $f \circ f^{-1} = \mathrm{id}_H$ and $f^{-1} \circ f = \mathrm{id}_G$.*

PROOF. PS4 □

LEMMA 70. *Let $g\colon G \to H$, $f\colon H \to K$ be group homomorphisms. Then $f \circ g\colon G \to K$ is a group homomorphism.*

PROOF. PS4. □

2.1.3. Subgroups.

LEMMA 71. *Let $(G,\cdot)$be a group, and let $H \subset G$ be non-empty and closed under $\cdot$ and under inverses, or under $(x,y) \mapsto xy^{-1}$. Then $e \in H$ and $(H, \cdot\restriction_{H\times H})$ is a group.*

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

DEFINITION 72. Such H is called a *subgroup* of G.

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

DEFINITION 73 (Kernel and image). Let $f \in \mathrm{Hom}(G,H)$. Its *kernel* is the set $\mathrm{Ker}(f) = \{g \in G \mid f(g) = e_H\}$. Its *image* is the set $\mathrm{Im}(f) = \{h \in H \mid \exists g \in G : f(g) = h\}$.

PROPOSITION 74. *The kernel and image of a homomorphism are subgroups of the respective groups.*

PROOF. The natural one. □

LEMMA 75. *f in injective iff* $\mathrm{Ker}\, f = \{e\}$.

2.2. Examples (Lecture 7, 25/9/2014)

2.2.1. Cyclic groups.

DEFINITION 76. Let G be a group, $g \in G$. We set $g^0 = e$, for $n \geq 0$ define by recursion $g^{n+1} = g^n g$, and for $n < 0$ set $g^n = \left(g^{-1}\right)^{-n}$.

PROPOSITION 77 (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. Exercise. □

LEMMA 78. *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. □

DEFINITION 79. A group G is *cyclic* if $G = \langle g \rangle$for some $g \in G$.

PROPOSITION 80. *Let G be cyclic, generated by g, and let $f(n) = g^n$ be the standard homomorphism. Then either:*

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

NOTATION 81. 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 82. The generator isn't unique (e.g. $\langle g \rangle = \langle g^- \rangle$).

PROOF. f is surjective by definition. If $\mathrm{Ker}\, f = \{0\}$ then f is injective, hence an isomorphism. Otherwise, by Proposition 6 we have $\mathrm{Ker}\, f = n\mathbb{Z}$ for some n. We now define $\bar{f}\colon \mathbb{Z}/n\mathbb{Z} \to G$ by $\bar{f}([a]_n) = g^a$.

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

□

DEFINITION 83. The *order* of $g \in G$ is the size of $\langle g \rangle$.

COROLLARY 84. *The order of g is the least positive m such that $g^m = e$ (infinity if there is no such m).*

OBSERVATION 85. *If G is finite, then every $g \in G$ has finite order.*

LEMMA 86. *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. □

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

EXAMPLE 87. 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. $\mathrm{Aut}(G) = \mathrm{Hom}(G,G) \cap S_G$.

2.2.3. Dihedral groups.

DEFINITION 88. A *(simple) graph* is an ordered pair $\Gamma = (V,E)$ where V is a set ("vertices") and $E \subset V \times V$ is a set ("edges") such that $(x,x) \notin E$ and $(x,y) \in E \leftrightarrow (y,x) \in E$.

Example: K_n, cycle ...

DEFINITION 89. An *automorphism* of Γ is a map $f \in S_{V(\Gamma)}$ such that $(x,y) \in E \leftrightarrow (f(x), f(y)) \in E$.

LEMMA 90. $\mathrm{Aut}(\Gamma) < S_\Gamma$ *is a subgroup.*

EXAMPLE 91. $\Gamma = K_n$, $\mathrm{Aut}(\Gamma) = S_n$.

We concentrate on the cycle.

DEFINITION 92. $D_{2n} = \mathrm{Aut}(n\text{-cycle})$.

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

LEMMA 93. $|D_{2n}| = 2n$.

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

Math 322: Problem Set 4 (due 2/10/2014)

Practice Problems

P1 Let G be a group with $|G| = 2$. Show that $G = \{e, g\}$ with $g \cdot g = e$. Show that $G \simeq C_2$ (that is, find an isomorphism $C_2 \to G$).

P2 Let G be a group. Give a bijection between $\{H < G \mid \#H = 2\}$ and $\{g \in G \mid g^2 = e, g \neq e\}$.

P3 (Basics of groups and homomorphisms) Fix groups G, H, K and let $f \in \mathrm{Hom}(G,H)$.
(a) Given also $g \in \mathrm{Hom}(H,K)$, show that $g \circ f \in \mathrm{Hom}(G,K)$.
(b) Suppose f is bijective. Then $f^{-1}\colon H \to G$ is a homomorphism.

Groups and Homomorphisms

1. Let G be a group, and let $(A,+)$ be an abelian group. For $f, g \in \mathrm{Hom}(G,A)$ and $x \in G$ define $(f+g)(x) = f(x) + g(x)$ (on the right this is addition in A).
   (a) Show that $f + g \in \mathrm{Hom}(G,A)$.
   (b) Show that $(\mathrm{Hom}(G,A), +)$ is an abelian group.
   (*c) Let G be a group, and let $\mathrm{id}\colon G \to G$ be the identity homomorphism. Define $f\colon G \to G$ by $f(x) = (\mathrm{id}(x))(\mathrm{id}(x)) = x \cdot x = x^2$. Suppose that $f \in \mathrm{Hom}(G,G)$. Show that G is commutative.

2. (External Direct products) Let G, H be groups.
   (a) On the product set $G \times H$ define an operation by $(g,h) \cdot (g',h') = (gg', hh')$. Show that $(G \times H, \cdot)$ is a group.
   DEF this is called the (external) *direct product* of G, H.
   (b) Let $\tilde{G} = \{(g, e_H) \mid g \in G\}$ and $\tilde{H} = \{(e_G, h) \mid h \in H\}$. Show that $\tilde{G}, \tilde{H}$ are subgroups of $G \times H$ and that $\tilde{G} \cap \tilde{H} = \{e_{G \times H}\}$.
   SUPP Show that $\tilde{G}$, $\tilde{H}$ are isomorphic to G, H respectively.
   (c) Show that for any $x = (g,h) \in G \times H$ we have $x\tilde{G}x^{-1} = \tilde{G}$ and $x\tilde{H}x^{-1} = \tilde{H}$.
   EXAMPLE The Chinese remainder theorem shows that $C_n \times C_m \simeq C_{nm}$ if $\gcd(n,m) = 1$.

3. Products with more than two factors can be defined recursively, or as sets of k-tuples.
   SUPP Show that the obvious maps give "natural" isomorphisms $G \times H \simeq H \times G$ and $(G \times H) \times K \simeq G \times (H \times K)$. We therefore write products without regard to the order of the factors.
   DEF Write G^k for the k-fold product of groups isomorphic to G.
   (a) Show that every non-identity element of C_2^k has order 2.
   (b) Show that $C_3 \times C_3 \not\simeq C_9$.

4. The *Klein group* or the *four-group* is the group $V \simeq C_2 \times C_2$.
   PRAC Check that $(\mathbb{Z}/12\mathbb{Z})^\times \simeq V$ and that $(\mathbb{Z}/8\mathbb{Z})^\times \simeq V$.
   (a) Write a multiplication table for V, and show that V is not isomorphic to C_4.
   (b) Show that $V = H_1 \cup H_2 \cup H_3$ where $H_i \subset V$ are subgroups isomorphic to C_2.
   (c) Let G be a group of order 4. Show that G is isomorphic to either C_4 or to $C_2 \times C_2$.

5. Let G be a group, and let $H, K < G$ be subgroups and suppose that $H \cup K$ is a subgroup as well. Show that $H \subset K$ or $K \subset H$.

6. Let $H < G$ have index 2 and let $g \in G$. Show that $gHg^{-1} = \{ghg^{-1} \mid h \in H\} = H$ (hint: show that if $g \notin H$ then $gH = G - H$).

Supplementary Problems

A. Let G be the *isometry group* of the Euclidean plane: $G = \{f : \mathbb{R}^n \to \mathbb{R}^n \mid \|f(\underline{x}) - f(\underline{y})\| = \|\underline{x} - \underline{y}\|\}$.
   (a) Show that that every $f \in G$ is surjective and injective and that G is closed under composition and inverse.
   (b) For $\underline{a} \in \mathbb{R}^n$ set $t_{\underline{a}}(\underline{x}) = \underline{x} + \underline{a}$. Show that $t_{\underline{a}} \in G$, and that $\underline{a} \to t_{\underline{a}}$ is an injective group homomorphism $(\mathbb{R}^n, +) \to G$.

   DEF Call the image the subgroup of *translations* and denote it by T.
   (c) Let $K = \{g \in G \mid g(\underline{0}) = \underline{0}\}$. Show that $K < G$ is a subgroup (we usually denote it $\mathrm{O}(n)$ and called it the *orthogonal group*).

   DEF This is called the *orthogonal group* and consists of rotations and reflections.

   FACT K acts on $\mathbb{R}^n$ by linear maps.
   (d) Show $\forall g \in G \exists t \in T : g\underline{0} = t\underline{0}$, and hence that $t^{-1}g \in K$. Conclude that $G = TK$.
   (e) Show that every $g \in G$ has a *unique* representation in the form $g = tk$, $t \in T$, $k \in K$ (hint: what is $T \cap K$?)
   (f) Show that K *normalizes* T: if $k \in K$, $t \in T$ we have $ktk^{-1} \in T$ (hint: use the linearity of k).
   (g) Show that $T \lhd G$: that for every $g \in G$ we have $gTg^{-1} = T$.

   RMK We have shows that G is the *semidirect product* $G = K \ltimes T$.

B. Let X be a set of size at least 2, and fix $e \in X$. Define $*: X \times X \to X$ by $x * y = y$.
   (a) Show that $*$ is an associative operation and that e is a left identity.
   (b) Show that every $x \in X$ has a right inverse: an element $\bar{x}$ such that $x * \bar{x} = e$.
   (c) Show that $(X, *)$ is not a group.

C. Let $\{G_i\}_{i \in I}$ be groups. On the cartesian product $\prod_i G_i$ define an operation by

$$\left(\underline{g} \cdot \underline{h}\right)_i = g_i h_i$$

   (that is, by co-ordinatewise multiplication).
   (a) Show that $(\prod_i G_i, \cdot)$ is a group.

   DEF This is called the (external) *direct product* of the G_i.
   (b) Let $\pi_j : \prod_i G_i \to G_j$ be projection on the jth coordinate. Show that $\pi_j \in \mathrm{Hom}\left(\prod_i G_i, G_j\right)$.
   (c) (Universal property) Let H be any group, and suppose given for each i a homomorphism $f_i \in \mathrm{Hom}(H, G_i)$. Show that there is a unique homomorphism $\underline{f} : H \to \prod_i G_i$ such that for all i, $\pi_i \circ \underline{f} = f_i$.
   (**d) An *abstract direct product* of the groups G_i is a pair $\left(\mathbf{G}, \{q_i\}_{i \in I}\right)$ where $\mathbf{G}$ is a group, $q_i : \mathbf{G} \to G_i$ are homomorphisms, and the property of (c) holds. Suppose that $\mathbf{G}, \mathbf{G}'$ are both abstract direct products of the same family $\{G_i\}_{i \in I}$. Show that $\mathbf{G}, \mathbf{G}'$ are isomorphic (hint: the system $\{q_i\}$ and the universal property of $\mathbf{G}'$ give a map $\varphi : \mathbf{G} \to \mathbf{G}'$, and the same idea gives a map $\psi : \mathbf{G}' \to \mathbf{G}$. To see that the composition is the identity compare for example $q_i \circ \psi \circ \varphi$, $q_i \circ \mathrm{id}_{\mathbf{G}}$ and use the uniqueness of (c).

D. Let V, W be two vector spaces over a field F. On the set of pairs $V \times W = \{(\underline{v}, \underline{w}) \mid \underline{v} \in V, \underline{w} \in W\}$ define $(\underline{v}_1, \underline{w}_1) + (\underline{v}_2, \underline{w}_2) = (\underline{v}_1 +_V \underline{v}_2, \underline{w}_1 +_W \underline{w}_2)$ and $a \cdot (\underline{v}_1, \underline{w}_1) = (a \cdot_V \underline{v}_1, a \cdot_W \underline{w}_1)$.
   (a) Show that this endows $V \times W$ with the structure of a vector space. This is called the *external direct sum* of V, W and denote it $V \oplus W$.
   (b) Generalize the construction to an infinite family of vector spaces as in problem C(a).
   (*c) State a universal property analogous to that of C(c),C(d) and prove the analogous results.

E. (Supplement to P3) Let $S^1 \subset \mathbb{R}^2$ be the unit circle. Then $f\colon [0, 2\pi) \to S^1$ given by $f(\theta) = (\cos\theta, \sin\theta)$ is continuous, 1-1 and onto but its inverse is not continuous.

2.3. Subgroups and coset spaces (Lecture 8, 2/10/2014)

2.3.1. The lattice of subgroups; generation.

LEMMA 95. *The intersection of any family of subgroups is a subgroup.*

DEFINITION 96. 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 97. 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 98. *$\langle S \rangle$ 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 99. *This is an equivalence relation. The equivalence class of g is the set gH.*

DEFINITION 100. The equivalence classes are called *left cosets*.

REMARK 101. Equivalently, we can define left cosets Hg which are the equivalence classes for the relation $g' \equiv_R g\,(H) \leftrightarrow g'g^{-1} \in H$.

DEFINITION 102. 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 103. *The map $gH \mapsto Hg^{-1}$ is a bijection between $H\backslash G$ and G/H. In particular, the index does not depend on the choice of left and right cosets.*

THEOREM 104 ("Lagrange's Theorem"). *$|G| = [G:H] \times |H|$. In particular, if G is finite then $|H|$ divides $|G|$.*

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

COROLLARY 105. *Let G be a finite group. Then the order of every $g \in G$ divides the order of G.*

PROOF. $o(g) = |\langle g \rangle|$. □

REMARK 106. 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 107. *It is a Theorem of Philip Hall that if G is finite, then $H\backslash G$ and G/H always have a* common *system of representatives.*

EXAMPLE 108. 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 109 (Fermat's Little Theorem; Euler's Theorem). Let $a \in \mathbb{Z}$. Then:

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

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

Math 322: Problem Set 5 (due 9/10/2014)

Practice problems

P1. $H = \{\mathrm{id}, (12)\}$ and $K = \{\mathrm{id}, (123), (132)\}$ are two subgroups of S_3. Compute the coset spaces S_3/H, $H\backslash S_3$, S_3/K, $K\backslash S_3$.

P2. Let $H < G$. Then for any non-empty $X \subset H$ we have $XH = H$. In particular, $hH = H$ for any $h \in H$.

P3. Let $K < H < G$ be groups with G finite. Use Lagrange's Theorem to show $[G:K] = [G:H]\,[H:K]$.

P4. Let $N < G$ satisfy for all $g \in G$ that $gNg^{-1} \subset N$. Show that for all $g \in G$, $gNg^{-1} = N$.

P5. Let $N < G$ satisfy for all $g_1, g_2 \in G$ that if $g_1 \equiv_L g_1'\,(N)$ and $g_2 \equiv_L g_2'\,(N)$ then $g_1 g_2 \equiv_L g_1' g_2'\,(N)$.

(a) Show that for any $g \in G$, $n \in N$ we have $gng^{-1} \equiv_L e\,(N)$, and conclude that $gNg^{-1} = N$.

(b) Give $G/\equiv_L\,(N)$ a group structure, and construct a homomorphism $q\colon G \to G/N$ such that $N = \mathrm{Ker}(q)$. Conclude that N is normal.

Cosets, normal subgroups and quotients

1. (Normalizers and centralizers) Let G be a group, $X \subset G$ a subset. The *centralizer* of X (in G) is $Z_G(X) = \{g \in G \mid \forall x \in X : gx = xg\}$ (in particular $Z(G) = Z_G(G)$ is called the *centre* of G). The *normalizer* of X (in G) is $N_G(X) = \left\{g \in G \mid gXg^{-1} = X\right\}$. Fix $H < G$.

   (a) Show that $N_G(X) < G$.

   PRAC Show that $Z_G(X) < N_G(X)$.

   (b) Show $H < N_G(H)$.

   PRAC Let $H < K < G$. Show that $H \lhd K$ iff $K \subset N_G(H)$. In particular, $H \lhd G$ iff $N_G(H) = G$.

   (c) Show that $Z(G)$ is a normal, abelian subgroup of G.

   PRAC Show that $H \cap Z_G(H) = Z(H)$, in particular that $H \subset Z_G(H)$ iff H is abelian.

2. (Semidirect products) Let $H, K < G$ and consider the map $f\colon H \times K \to G$ given by $f(h,k) = hk$. Recall that the image of this map is denoted HK.

   (a) Show that f is injective iff $H \cap K = \{e\}$.

   SUPP For $x \in HK$ give a bijection $f^{-1}(x) \leftrightarrow H \cap K$, hence a bijection $H \times K \leftrightarrow HK \times H \cap K$.

   PRAC Show $H < N_G(K) \iff \forall h \in H : hKh^{-1} = K$. In this case we say "$H$ normalizes K".

   (b) Suppose H normalizes K. Show that HK is a subgroup of G and that $\langle H \cup K\rangle = HK$. Show that $K \lhd HK$ (hint: you need to show that $HK < N_G(K)$ and already know that H, K separately are contained there).

   DEF If $H < N_G(K)$ and $H \cap K = \{e\}$ we call HK the (*internal*) *semidirect product* of H and K. We write $HK = H \ltimes K$ (combining the symbols for product and normal subgroup).

   (c) Let HK be the semidirect product of H, K and let $q\colon HK \to (HK)/K$ be the quotient map. Directly show that the restriction $q\restriction_H\colon H \to (HK)/K$ is an isomorphism. (Hint: what is the kernel? what is the image?)

   PRAC Let $g, h \in G$. Show that $gh = hg$ iff the *commutator* $[g,h] = ghg^{-1}h^{-1}$ has $[g,h] = e$.

   — For parts (d),(e) suppose that H, K normalize each other and that $H \cap K = \{e\}$

   (d) Show that H, K *commute*: $hk = kh$ whenever $h \in H$, $k \in K$.

   (e) Show that the map f is an isomorphism onto its image (it's a bijection by part (a); you need to show it is a group homomorphism).

   DEF In that case we say HK is the (*internal*) *direct product* of H and K.

PRAC Let $G = \mathrm{GL}_2(\mathbb{R})$ be the group of 2×2 invertible matrices. We will consider the subgroups $B = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G \middle| ad \neq 0 \right\}$, $A = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in G \middle| ad \neq 0 \right\}$ and $N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{R} \right\}$.

(a) Show that these really are subgroups. Evidently $N, A \subset B \subset G$.

(b) Show that $A \simeq (\mathbb{R}^\times)^2 = \mathbb{R}^\times \times \mathbb{R}^\times$. Show that $N \simeq \mathbb{R}^+$.

(b) Show that $B = N \rtimes A$(you need to show that $B = NA$, that $A \cap N = \{I\}$, and that $N \lhd B$).

(c) Directly show that for any fixed a, d with $ad \neq 0$ we have $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} N = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid b \in \mathbb{R} \right\}$, demonstrating part of 2(c).

3. Let $K < H < G$ be a chain of subgroups. Let $R \subset G$ be a system of representatives for G/H and let $S \subset H$ be a system of representatives for H/K.

(a) Show that the map $R \times S \to RS$ given by $(r,s) \mapsto rs$ is a bijection.

(b) Show that $RS = \{rs \mid r \in R, s \in S\}$ is a system of representatives for G/K, and conclude that $[G:K] = [G:H]\,[H:K]$.

RMK See P1 for a numerical proof in the finite case.

4. In a previous problem set we defined the subgroup $P_n = \{\sigma \in S_n \mid \sigma(n) = n\}$ of S_n. We now give an explicit description of S_n/P_n and use that to inductively determine the order of S_n.

(a) Show that for $\tau, \tau' \in S_n$ we have $\tau P_n = \tau' P_n$ iff $\tau(n) = \tau'(n)$, and conclude that $[S_n : P_n] = n$.

(b) Show that $P_n \simeq S_{n-1}$.

(c) Combine (a),(b) into a proof by induction that $|S_n| = n!$.

Challenge problems

5. Let G be a group

(a) Suppose that $x^2 = e$ for all $x \in G$. Show that G is abelian.

(**b) Suppose that G has n elements, at least $\frac{3}{4}n$ of which have order 2. Then G is abelian.

6**. Let G be group of order n. Show that there is $X \subset G$ of size at most $1 + \log_2 n$ such that $G = \langle X \rangle$.

Supplementary Problems: Quotients and the abelianization

A. (The universal property of G/N) Let $N \lhd G$. An "abstract quotient" of a group G is a group $\bar{G}$, together with a homomorphism $\bar{q}\colon G \to \bar{G}$ such that the property for any $f\colon G \to H$ with kernel containing N there is a unique $\bar{f}\colon \bar{G} \to H$ with $f = \bar{f} \circ \bar{q}$ (in class we saw that the quotient group G/N has this property). Suppose that $\left(\bar{G}', \bar{q}'\right)$ is another abstract quotient. Show that there is a uinque isomorphism $\varphi\colon \bar{G} \to \bar{G}'$ such that $\bar{q}' = \varphi \circ \bar{q}$.

B. (The derived subgroup and abelian quotients) Fix a group G and recall that notation $[g,h] = ghg^{-1}h^{-1}$.

(a) Let $f \in \mathrm{Hom}(G,H)$ be a homomorphism. Show that $f([g,h]) = [f(g), f(h)]$ for all $g,h \in G$.

(b) Deduce from (a) that the set of commutators is invariant under conjugation.

DEF For $H,K < G$ set $[H,K] = \langle \{[h,k] \mid h,k \in G\} \rangle$ – note that this is the *subgroup* generated by those commutators, not just the set of commutators. In particular, we write $G' = [G,G]$ for the *derived subgroup* (or *commutator subgroup*) of G, the subgroup generated by all the commutators.

(c) Show that G' is normal in G.

(d) Show that $G^{\mathrm{ab}} \stackrel{\mathrm{def}}{=} G/G'$ is abelian (hint: apply (a) to the quotient map).

DEF we call G^{ab} the *abelianization* of G.

(e) Let $N \lhd G$. Show that G/N is abelian iff $G' \subset N$.

(f) Let A be an abelian group and let $q\colon G \to G^{\mathrm{ab}}$ be the quotient map. Show that the map $\Phi\colon \mathrm{Hom}(G^{\mathrm{ab}}, A) \to \mathrm{Hom}(G,A)$ given by $\Phi(f) = f \circ q$ is a bijection.

C. Compute the derived subgroup and the abelianization of the groups: $C_n, D_{2n}, S_n, \mathrm{GL}_n(\mathbb{R})$.

2.4. Normal subgroups and quotients

2.4.1. Normal subgroups. HW: Every subgroup is normal in its normalizer.

DEFINITION 110. Call $N < G$ *normal* if $gN = Ng$ for all $g \in G$, equivalently if $gNg^{-1} = N$ for all $g \in G$. In that case we write $N \lhd G$.

EXAMPLE 111. $\{e\}, G$ always normal; Any subgroup of an abelian group.

LEMMA 112. *Let $f \in \mathrm{Hom}(G,H)$. Then $\mathrm{Ker}(f)$ is normal.*

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

EXAMPLE 113. $\mathrm{SL}_n(\mathbb{R}) \lhd \mathrm{GL}_n(\mathbb{R})$ (kernel of determinant), $A_n \lhd S_n$ (kernel of sign). Translations in $\mathrm{Isom}(\mathbb{E}^n)$.

LEMMA 114. *The intersection of any family of normal subgroups is normal.*

DEFINITION 115. The *normal closure* of $S < G$ is the normal subgroup $\langle S \rangle^{\mathrm{N}} = \bigcap \{N \lhd G \mid S \subset N\}$.

2.4.2. Quotients.

LEMMA 116. *The subgroup $N < G$ is normal iff the relation $\equiv (N)$ respects products and inverses.*

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

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

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

COROLLARY 117. *Defining group operations via representatives endows G/N with the structure of a group.*

DEFINITION 118. This is called the quotient *of G by N*.

LEMMA 119. *The quotient map $g \mapsto gN$* is a surjective group homomorphism with kernel N.

EXAMPLE 120. $\mathbb{Z}$ 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.

THEOREM 121 (First isomorphism theorem). *Let $f \in \mathrm{Hom}(G,H)$ and let $K = \mathrm{Ker}(f)$. Then f induces an isomorphism $G/K \to \mathrm{Im}(f)$.*

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

THEOREM 122 (Second isomorphism theorem). *Let $N, H < G$ with N normal. Then $N \cap H$ is normal in H, and the natural map $H \to HN$ induces an isomorphism*

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

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

THEOREM 123 (Third isomorphism theorem). *Let $K < N < G$ be subgroups with K, N normal in G. Then N/K is normal in G/K and there is a natural isomorphism $G/N \to (G/K)/(N/K)$.*

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

2.4.4. Simplicity of A_n.

DEFINITION 124. G is *simple* if it has no normal subgroups except for $\{e\}, G$ ("prime")

LEMMA 125 (Generation and conjugacy in A_n). *The pair $(123), (145)$ and $(12)(34), (12)(35)$ are conjugate in A_5. The*

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

LEMMA 126 (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 127. *A_n is simple if $n \geq 5$.*

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

Case 1. $k = 1$ would make $\sigma = \mathrm{id}$.
Case 2. $k = 2$ would make σ a transposition.
Case 3. $k = 3$ makes σ a 3-cycle. By Lemma 126(1), N contains all 3-cycles and thus equals A_n.
Case 4. $k = 4$ makes σ of the form $(12)(34)$ since 4-cycles are odd. We are then done by Lemma 126(2).
Case 5. $k \geq 5$ and σ has a cycle of length at least 3. We may then assume $\sigma(1) = 2$, $\sigma(2) = 3$ and let $\gamma = (345)\sigma(345)^{-1}\sigma^{-1} \in N$. Then γ fixes every point that σ does, and also $\gamma(2) = 2$, but $\gamma(3) = 4$, so $\gamma \neq \mathrm{id}$ – a contradiction.
Case 6. $k \geq 5$ and σ is a product of at least 4 disjoint transposition, say $\sigma = (12)(34)(56)(78)\cdots$. Then the same γ again fixes every point that σ fixes, and also $1, 2$ – but it still exchanges $7, 8$ – another contradiction.

□

2.4.5. Alternative proofs.

2.4.5.1. *Rotman.*

(1) $A_n$is generated by 3-cycles if $n \geq 5$.
(2) A_5 is simple:
   (a) The conjugacy classes of (123) and $(12)(34)$ generate A_5.
   (b) The other conjugacy classes id, (12345) (13542) have sizes $1, 12, 12$ which do not add up to a divisor of 60.
(3) A_6 is simple:
   (a) Let $N \lhd A_6$ be normal and non-trivial. For $i \in [6]$, let $P_i = \mathrm{Stab}_{A_6}(i) \simeq A_5$. 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 $N \lhd A_n$ be normal. Let $\sigma \in N$ be non-identity with, say, $\sigma(1) = 2$. Then κ=(234) does not commute with σ ($\kappa\sigma(1) = 3$ but $\sigma\kappa(1) = 2$).
(5) The element $\gamma = [\sigma, \kappa] = \sigma\kappa\sigma^{-1}\kappa^{-1} = \sigma\left(\kappa\sigma^{-1}\kappa^{-1}\right) \in N$ is also non-identity. But writing this element as $\left(\sigma\kappa\sigma^{-1}\right)\kappa^{-1}$we see that it is a product of two 3-cycles and hence has support of size at most 6. This therefore belongs to a copy A^* of A_6 inside A_n. But $N \cap A^*$ is normal, and $A_6$is simple. Thus N contains A^* and in particular a 3-cycle.

2.4.5.2. *Induction.*

(1) A_5 is simple: see above.
(2) Suppose A_n simple, and let $N \lhd A_{n+1}$ 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, 9/10/2014)

DEFINITION 128 (Group action). An *action* of the group G on the set X is a binary operation $\cdot\colon G\times X\to X$ such that $e_G\cdot x=x$ for all $x\in X$ and such that $g\cdot(h\cdot x)=(gh)\cdot x$ for all $g,h\in G$, $x\in X$. A *G-set* is a pair $(X,\cdot)$ where X is a set and $\cdot$ is an action of G on X. We sometimes write $G\curvearrowright X$.

We discus Examples of group actions

(0) For any X,G we have the *trivial action* $g\cdot x=x$ for all x.
(1) S_X acting on X. Key example.
(2) F field, V F-vector space. Then scalar multiplication is an action $F^\times\curvearrowright V$.
    - Orbit of non-zero vector is (roughly) the 1d subspace it spans.
(3) X set with "structure", $\mathrm{Aut}(X)=\left\{\sigma\in S_X\mid \sigma,\sigma^{-1}\text{ "preserve the structure"}\right\}$ acts on X.
    - Can always restrict actions: if $\cdot\colon G\times X\to X$ is an action then $\cdot\restriction_{H\times X}$ is an action of H.
    (a) D_{2n} acting on cycle, inside of there's C_n acting on te cycle; $\mathrm{Aut}(\Gamma)$ acting on Γ.
    (b) $\mathrm{GL}_n(\mathbb{R})$ acting on $\mathbb{R}^n$, $\mathrm{GL}(V)$ acting on V.
    (c) G group; $\mathrm{Aut}(G)$ acting on G.
(4) Induced actions (see Problem Set): suppose G acts on X,Y.
    (a) G acts on Y^X by $(g\cdot f)(x)\overset{\text{def}}{=}g\cdot\left(f\left(g^{-1}\cdot x\right)\right)$ (in particular, action of G on the vector space F^X where X is a G-set).
    (b) G acts on $P(X)$ by $g\cdot A=\{g\cdot a\mid a\in A\}$.
    (c) etc.

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

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

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

LEMMA 129 (Actions vs homomorphisms). *In increasing level of abstraction:*

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

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

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

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

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

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

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

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

REMARK 130. 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 131 (Cayley 1878). *Every group G is isomorphic to a subgroup of S_G. In particular, every group of order n is isomorphic to a subgroup of S_n.*

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

REMARK 132. Can make this quantitative: [**1**] asks for the minimal m such that G is isomorphic to a subgroup of S_m.

LEMMA 133. *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 104, if S_n has a subgroup isomorphic to C_p then $p | n!$. Since p is prime this means $p | k$ for some $k \leq n$ so that $p \leq k \leq n$. □

REMARK 134. 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.

Math 322: Problem Set 6 (due 23/10/2014)

Practice problems

P1. Let G be a group and let X be a set of size at least 2. Fix $x_0 \in X$ and for $g \in G, x \in X$ set $g \cdot x = x_0$.
   (a) Show that this operation satisfies $(gh) \cdot x = g \cdot (h \cdot x)$ for all $g, h \in G, x \in X$.
   (b) This is not a group action. Why?

P2. Label the elements of the four-group V by $1,2,3,4$ in some fashion, and explicitely give the permutation corresponding to each element by the regular action.

P3. Repeat with S_3 acting on itself by conjugation (you will now have six permutations in S_6).

P4. Let G act on X. Say that $A \subset X$ is *G-invariant* if for every $g \in G$, $a \in A$ we have $g \cdot a \in A$.
   (a) Show that A is G-invariant iff $g \cdot A = A$ ($g \cdot A$ in the sense of problem 4(a)).
   (b) Suppose A is G-invariant. Show that the restriction of the action to A (formally, the binary operation $\cdot\restriction_{G \times A}$) is an action of G on A.

Simplicity of A_n

1. Let $V = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$. Show that $V \lhd S_4$, so that S_4 is not simple.

2. (The normal subgroups of S_n) Let $N \lhd S_n$ with $n \geq 5$.
   (a) Let G be a group and let $H \lhd G$ be a normal subgroup isomorphic to C_2. Show that $H < Z(G)$ (hint: let $H = \{1, h\}$, let $g \in G$, and consider the element ghg^{-1}).
   (b) Suppose that $N \cap A_n \neq \{\mathrm{id}\}$. Show that $N \supset A_n$ and conclude that $N = A_n$ or $N = S_n$ (hint: what is the index of N?)
   (c) Suppose that $N \cap A_n = \{\mathrm{id}\}$. Show that N is isomorphic to a subgroup of C_2 (hint: restrict $\mathrm{sgn}\colon S_n \to C_2$ to N).
   (d) Show that if $n \geq 3$ then $Z(S_n) = \{\mathrm{id}\}$, and conclude that in case (c) we must have $N = \mathrm{id}$.

3. Let X be an infinite set.
   (a) Show that $S_X^{\mathrm{fin}} = \{\sigma \in S_X \mid \mathrm{supp}(\sigma) \text{ is finite}\}$ is a subgroup of S_X.

   PRAC For finite $F \subset X$ there is a natural inclusion $S_F \hookrightarrow S_X$, which is a group homomorphism, an isomorphism onto its image. Let $\mathrm{sgn}_F\colon S_F \to \{\pm 1\}$ be the sign character.

   DEF For $\sigma \in S_X^{\mathrm{fin}}$ define $\mathrm{sgn}(\sigma) = \mathrm{sgn}_F(\sigma)$ for any finite F such that $\sigma \in S_F$.
   (c) Show that $\mathrm{sgn}(\sigma)$ is well-defined (independent of F) and a group hom $S_X^{\mathrm{fin}} \to \{\pm 1\}$.
   (d) The *infinite alternating group* A_X is kernel of this homomorphism. Show that A_X is simple.

Group actions

4. Let the group G act on the set X.
   (a) For $g \in G$ and $A \in P(X)$ set $g \cdot A = \{g \cdot a \mid a \in A\} = \{x \in X \mid \exists a \in A : x = g \cdot a\}$. Show that this defines an action of G on $P(X)$.
   (b) In PS2 we endowed $P(X)$ with a group structure. Show that the action of (a) is by *automorphisms*: that the map $A \mapsto g \cdot A$ is a group homomorphism $(P(X), \Delta) \to (P(X), \Delta)$.
   (c) Let Y be another set. For $f\colon X \to Y$ set $(g \cdot f)(x) = f(g^{-1} \cdot x)$. Show that this defines an action of G on Y^X, the set of functions from X to Y.
   (*d) Suppose that $Y = \mathbb{R}$ (or any field), so that $\mathbb{R}^X$ has the structure of a vector space over $\mathbb{R}$. Show that the action of (c) is by *linear maps.*

5. (Some stabilizers) The action of S_X on X induces an action on $P(X)$ as in problem 4(a). Suppose that X is finite, $\#X = n$.
   (a) Show that the orbits of S_X on $P(X)$ are the sets $\binom{X}{k} = \{A \subset X \mid \#A = k\}$ for $0 \leq k \leq n$.
   SUPP When X is infinite, $\binom{X}{\kappa}$ are orbits if $\kappa < |X|$, but there are multiple orbits on $\binom{X}{|X|}$, parametrized by the cardinality of the complement.
   (b) Let $A \subset X$. Show that $\mathrm{Stab}_{S_X}(A) \simeq S_A \times S_{X-A}$.
   (c) Use (a),(b) to show that $\#\binom{X}{k} = \frac{n!}{k!(n-k)!}$.

Conjugation

6. Let G be a finite group, H a proper subgroup. Show that the conjugates of H do not cover G (that is, there is some $g \in G$ which is not conjugate to an element of H).
   RMK There exists an infinite group in which all non-identity elements are conjugate.

3.2. Conjugation (Lecture 12, 16/10/2014)

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

3.2.1. Conjugacy of elements.

DEFINITION 135. For $g \in G$, $x \in G$ set ${}^g x = gxg^{-1}$. Set $\gamma_g(x) = gxg^{-1}$.

LEMMA 136. *This is a group action of G on itself, and it is an action by* automorphisms*:* $\gamma_g \in \mathrm{Aut}(G)$.

PROOF. Check. □

DEFINITION 137. Say "x is conjugate to y" if there is $g \in G$ such that ${}^g x = y$.

LEMMA 138. *This is an equivalence relation.*

PROOF. See PS3, problem 2(a). □

DEFINITION 139. The equivalence classes are called *conjugacy classes. Write $G\backslash X$ for the set of equivalence classes.*

EXAMPLE 140. The class of e is $\{e\}$. More generally, the class of x is $\{x\}$ iff $x \in Z(G)$ (proof).

REMARK 141. Why is conjugacy important? Because

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

In fact, the map $g \mapsto \gamma_g$ is a group homomorphism $G \to \mathrm{Aut}(G)$ (this is Lemma 129(2)).

DEFINITION 142. The image of this homomorphism is denoted $\mathrm{Inn}(G)$ and called the group of *inner automorphisms*.

EXERCISE 143. The kernel is exactly $Z(G)$, so by Theorem 121, $\mathrm{Inn}(G) \simeq G/Z(G)$. Also, if $f \in \mathrm{Aut}(G)$ then $f \circ \gamma_g \circ f^{-1} = \gamma_{f(g)}$ so $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$.

DEFINITION 144. Call $\mathrm{Out}(G) \stackrel{def}{=} \mathrm{Aut}(G)/\mathrm{Inn}(G)$ the *outer automorphism group* of G.

EXAMPLE 145. $\mathrm{Aut}(\mathbb{Z}^d) \simeq \mathrm{GL}_d(\mathbb{Z})$ but all inner automorphisms are trivial (the group is commutative).

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

FACT 146. $\mathrm{Out}(S_n) = \{e\}$ *except that* $\mathrm{Out}(S_6) \simeq C_2$.

LEMMA 147. *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 ${}^{g'}x = {}^{gz}x = {}^g({}^z x) = {}^g x$. It is surjective: the conjugat${}^g x$ is the image of $gZ_G(x)$, and finally if ${}^g x = {}^{g'} x$ then $x = {}^{g^{-1}g} x = {}^{g^{-1}g'} x$ so $g^{-1}g' \in Z_G(x)$ and $g'Z_G(x) = g'Z(x)$. □

THEOREM 148 (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. □

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

DEFINITION 149. For $g \in G$, $H < G$ set ${}^gH = gHg^{-1} = \gamma_g(H)$.

LEMMA 150. *This is a group action of G on its set of subgroups.*

PROOF. Same: ${}^eH = eHe^{-1} = H$. Given ${}^gH$ we have ${}^{g^{-1}}{}^gH = H$. Finally, ${}^g\left({}^hH\right) = {}^{gh}H$. □

EXAMPLE 151. The class of H is $\{H\}$ iff H is normal in G.

LEMMA 152. *Conjugacy of subgroups is an equivalence relation.*

PROOF. Same. □

LEMMA 153. *There is a bijection between the conjugates of H and $G/N_G(H)$.*

PROOF. Same. □

3.3. Orbits, stabilizers and counting

Fix a group G acting on a set X.

DEFINITION 154. Say $x, y \in X$ are *in the same orbit* if there is $g \in G$ such that $gx = y$.

LEMMA 155. *This is an equivalence relation.*

PROOF. Repeat. □

DEFINITION 156. The equivalence classes are called orbits.

REMARK 157. Why orbits? Consider action of $\mathbb{R}^+$ on phase space by time evolution (idea of Poincaré).

DEFINITION 158. Write $G \cdot x$ or $\mathcal{O}(x)$ for the orbit of $x \in X$. Write $G\backslash X$ for the set of orbits. For $x \in X$ set $\mathrm{Stab}_G(x) = \{g \in G \mid g \cdot x = x\}$.

LEMMA 159. $\mathrm{Stab}_G(x)$ *is a subgroup.*

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

LEMMA 160 (Orbit-Stabilizer Theorem). *There is a bijection between $\mathcal{O}(x) \subset X$ and $G/\mathrm{Stab}_G(x)$. Moreover, the stabilizers of an orbit of G is a conjugacy class in of subgroups. In particular, if X is finite,*

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

PROOF. Same. □

DEFINITION 161. $\mathrm{Fix}(G) = \{x \in X \mid \mathrm{Stab}_G(x) = G\}$.

COROLLARY 162. *Suppose G has order p^k and X is finite. Then $\#X \equiv \#\mathrm{Fix}(X)$ (p).*

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

EXAMPLE 163. Zagier's slick proof of Fermat's Theorem

3.4. Actions, orbits and point stabilizers (Lecture 13, 21/10/2014)

3.4.1. G **acting on** G/H**.**

- Transitive action
- Isomorphic to any orbit where H is the point stabilizer
- Point stabilizers are conjugate.

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

- This is an action
- Orbits and Stabilizers
- Action on pairs

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

- Transitive action
- Point stabilizers
- Action on $\mathcal{G}(n,k)$.

3.4.4. $\mathrm{O}(n)$ **acting on** $\mathbb{R}^n$**.**

- Restriction of actions
- Orbits

3.4.5. $\mathrm{Aff}(\mathbb{R}^n)$ **acting on** $\mathbb{R}^n$**.**

- Semidirect product
- Point stabilizer
- Transitive, study action on pairs

3.4.6. $\mathrm{Isom}(\mathbb{R}^n)$ **acting on** $\mathbb{R}^n$**.**

- Semidirect product
- Action on pairs

3.4.7. $\mathrm{Gal}(E/F)$ **and the Fundamental Theorem of Algebra.**

3.4.8. $\mathrm{Diff}(M)$ **acting on a connected manifold** M**.**

CHAPTER 4

p-Groups and Sylow's Theorems

4.1. p groups (Lecture 14, 23/10/2014)

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

THEOREM 164 (Cauchy 1845). *Suppose that $p|\#G$. Then G has an element of order p.*

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

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

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

Here's another proof:

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

COROLLARY 165. *The number of elements of order exactly p is congruent to -1 mod p (in particular, it is non-zero).*

COROLLARY 166. *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 167. Call G a p-group if every element of G has order a power of p.

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

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

THEOREM 168. *Let G be a finite p-group. Then $Z(G) \neq 1$.*

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

LEMMA 169. *If $G/Z(G)$ is cyclic it is trivial and G is commutative.*

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

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

which means

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

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

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

□

PROPOSITION 170 (Groups of order p^2, p^3). .

(1) Let G have order p^2. Then G is abelian, in fact isomorphic to one of C_{p^2} and $C_p \times C_p$.

(2) Let G be an abelian group of order p^3. Then G is one of C_{p^3}, $C_{p^2} \times C_p$, $C_p \times C_p \times C_p$.

(3) Let G be non-commutative, of order p^3. Then $Z(G) \simeq C_p$ and $G/Z(G) \simeq C_p \times C_p$.

PROOF.

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

(2) The map $g \mapsto g^p$ is a homomorphism $G \to G$. Its kernel is the elements of order dividing p (must be non-trivial!) so its image is a proper subgroup, to be detnoed G^p. Then G/G^p is a subgroup where every element has order dividing p. We consider its dimension.
   (a) $G/G^p \simeq C_p^3$. Then $G^p = \{e\}$, so $G/G^p \simeq G$.
   (b) $G/G^p \simeq C_p^2$. Let $x, y \in G$ be such that their images are a basis for G/G^p.

□

Math 322: Problem Set 7 (due 30/10/2014)

Practice problems

P1. Let G commutative group where every element has order dividing p.
   (a) Endow G with the structure of a vector space over $\mathbb{F}_p$.
   (b) Show that $\dim_{\mathbb{F}_p} G = k$ iff $\#G = p^k$ iff $G \simeq (C_p)^k$.
   (c) Show that for any $X \subset G$, we have $\langle X \rangle = \mathrm{Span}_{\mathbb{F}_p} X$.

P2. For a field F let $H = \left\{ \begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix} \mid x,y,z \in F \right\}$ is called the *Heisenberg group* over F.
   (a) Show that H is a subgroup of $\mathrm{GL}_3(F)$ (you also need to show containment, that is that each element is an invertible matrix).
   (b) Show that $Z(H) = \left\{ \begin{pmatrix} 1 & 0 & z \\ & 1 & 0 \\ & & 1 \end{pmatrix} \mid z \in F \right\} \simeq F^+$.
   (c) Show that $H/Z(H) \simeq F^+ \times F^+$ via the map $\begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix} \mapsto (x,y)$.
   (d) Show that H is non-commutative, hence is not isomorphic to the direct product $F^2 \times F$.
   (e) Suppose $F = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ with p odd. Then $\#H = p^3$ so that H is a p-group. Show that every element of $H(\mathbb{F}_p)$ has order p.

General theory

Fix a group G.

1. (Correspondence Theorem) Let $f \in \mathrm{Hom}(G,H)$, and let $K = \mathrm{Ker}(f)$.
   (a) Show that the map $M \mapsto f(M)$ gives a bijection between the set of subgroups of G containing K and the set of subgroups of $\mathrm{Im}(f) = f(G)$.
   (b) Show that the bijection respects inclusions, indices and normality (if $K < M_1, M_2 < G$ then $M_1 < M_2$ iff $f(M_1) < f(M_2)$, in which case $[M_2 : M_1] = [f(M_2) : f(M_1)]$, and $M_1 \lhd M_2$ iff $f(M_1) \lhd f(M_2)$).

2. Let $X, Y \subset G$ and suppose that $K = \langle X \rangle$ is normal in G. Let $q\colon G \to G/K$ be the quotient map. Show that $G = \langle X \cup Y \rangle$ iff $G/K = \langle q(Y) \rangle$.

p-groups

3. Recall the group $\mathbb{Z}\left[\frac{1}{p}\right] = \left\{ \frac{a}{p^k} \in \mathbb{Q} \mid a \in \mathbb{Z}, k \geq 0 \right\} < \mathbb{Q}^+$, and note that $\mathbb{Z} \lhd \mathbb{Z}\left[\frac{1}{p}\right]$ (why?).
   (a) Show that $G = \mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z}$ is a p-group.
   (b) Show that for every $x \in G$ there is $y \in G$ with $y^p = x$ (warning: what does y^p mean?)

   SUPP Show that every proper subgroup of G is finite and cyclic. Conversely, for every k there is a unique subgroup isomorphic to p^k.

**4. If $|G| = p^n$, show for each $0 \leq k \leq n$ that G contains a normal subgroup of order p^k.

*5. Let G be a finite p-group, and let $H \lhd G$. Show that if H is non-trivial then so is $H \cap Z(G)$.

Supplement: Generation of finite commutative p-groups

A. Let G be a finite commutative p-group.
   (a) Show that G^p is a proper subgroup (problem P1 is relevant here).
   (b) Show that G/G^p is a non-trivial commutative group where every element has order p.
   — Let $X \subset G$ be such that its image under the quotient map generates G/G^p.
   (c) For $k \geq 0$ let $g_k \in G^{p^k}$ ($G^1 = G$). Show that there is $w \in \langle X \rangle$ and $g_{k+1} \in G^{p^{k+1}}$ such that $g_k = w^{p^k} g_{k+1}$.
   (d) Suppose that $\#G = p^n$. Show that $G^{p^n} < \langle X \rangle$, and then by backward induction eventually show that $G = G^1 < \langle X \rangle$.
   RMK You have proved: X generates G iff $q(X)$ generates G/G^p. In particular, the minimal number of generators is exactly $\dim_{\mathbb{F}_p} G/G^p = \log_p [G : G^p]$.

RMK In fact, for any p-group, G, X generates G iff its image generates $G/G'G^p$ where G' is the derived (commutator) subgroup.

4.2. Example: groups of order pq (Lecture 15, 28/10/14)

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

REMARK 171. 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 164, is it has a subgroup P of order 2, a subgroup Q of order 3. Note that the subgroup $P \cap Q$ must have order dividing both $2,3$ so it is trivial.

LEMMA 172. *Let $P,Q < G$ satisfy $P \cap Q = \{e\}$. Then the (set) map $P \times Q \to PQ$ given by $(x,y) \mapsto xy$ is a bijection.*

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

REMARK 173. In general there is a bijection between $PQ \times P \cap Q \leftrightarrow P \times Q$.

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

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

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

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

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

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

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

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

REMARK 174. Having constructed two non-isomorphic groups, we are done, but we'd like to discover them anew.

Case 1. If $aba^{-1} = b$ then a,b commute, so P,Q commute, so $G \simeq P \times Q$ (internal direct product). But this means $G \simeq C_2 \times C_3 \simeq C_6$ by the Chinese Remainder Theorem 28.

Case 2. If $aba^{-1} = b^2 = b^{-1}$ then also $ab^2a = (b^2)^{-1}$ and we have D_6: $\left\{1,b,b^2\right\}$ 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 164, 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 172 we have $\#PQ = pq = \#G$ so $G = PQ$.

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

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

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

In other words, $\mathcal{C}$ is a single orbit for the action of P by conjugation. By the orbit-stabilizer theorem (Lemma 172), this must have size dividing $\#P = p$ so either 1 or p. Assume Q not normal, so the size is p. Now consider the action of Q on $\mathcal{C}$ by conjugation. Each Q-orbit can have size q or 1, but since $q > p$ there is no room for an orbit of size 1. We conclude that every $Q' \in \mathcal{C}$ is normalized by Q.

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

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

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

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

Case 1. If $aba^{-1} = b$ then a, b commute, so P, Q commute and $G \simeq C_p \times C_q \simeq C_{pq}$ by the Chinese Remainder Theorem 28.

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

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

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

4.2.3. More detail, and examples (Lecture 16).

- Explicitely parametrize G as $\left\{a^i b^j \mid i \mod p, j \mod q\right\}$.
  - Every hom $C_n \to C_n$ must be of the form $x \mapsto x^k$. Composing two such gives the hom $x \mapsto x^{kl}$, so have an *automorphism* if k is invertible mod q. In other words, $\mathrm{Aut}\,(C_n) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

- For any k mod q can try to define the product
$$\left(a^{i'}b^{j'}\right)\left(a^{i}b^{j}\right) = a^{i'+i}b^{j'k^{-i}+j}$$
where k^{-r} is the power in $\mathbb{Z}/q\mathbb{Z}$.
- Makes sense only if $k^p \equiv 1\,(q)$ so that a^p acts correctly. This can happen only if $q \equiv 1\,(p)$.
- If $q \equiv 1\,(p)$ then by Cauchy there are elements of order p and we can make the definition.
- If we replace k by k^r we can replace a with a^r (with $a^{\bar{r}}$) to get isomorphism of the semidirect products, so only one semidrect product

- Understand in detail how a group of order 3 cannot act on a group of order 5.
- Understand in details that the two actions of C_3 on C_7 give isomorphic groups $C_3 \ltimes C_7$.

Math 322: Problem Set 8 (due 6/11/2014)

P1. Let G be a commutative group and let $k \in \mathbb{Z}$.
(a) Show that the map $x \mapsto x^k$ is a group homomorphism $G \to G$.
(b) Show that the subsets $G[k] = \{g \in G \mid g^k = e\}$ and $\{g^k \mid g \in G\}$ are subgroups.
RMK For a general group G we let $G^k = \langle \{g^k \mid g \in G\} \rangle$ be the subgroup generated by the kth powers. You have shown that, for a commutative group, $G^k = \{g^k \mid g \in G\}$.

On group actions and homomorphisms

1. Let the group G act on the set X.
DEF The *kernel* of the action is the normal subgroup $K = \{g \in G \mid \forall x \in X : g \cdot x = x\}$.
PRAC K is the kernel of the associated homomorphism $G \to S_X$, hence $K \lhd G$ indeed.
(a) Construct an action of G/K on X "induced" from the action of G.
DEF An action is called *faithful* its the kernel is trivial.
(b) Show that the action of G/K on X is faithful.
SUPP Show that this realizes G/K as a subgroup of S_X.
(c) Suppose G acts non-trivially on a set of size n. Show that G has a proper normal subgroup of index at most $n!$.
(*d) Show that an infinite simple group has no proper subgroups of finite index.

*2. Let G be a group of finite order n, and let p be the smallest prime divisor of n. Let $M < G$ be a subgroup of index p. Show that M is normal.
RMK In particular, this applies when G is a finite p-group.

Cyclic groups and their automorphisms

3. (Structure of cyclic groups)
(a) Let G be a group, $g \in G$ an element of order n, and let $a \in \mathbb{Z}$ Show that g^a has order $\frac{n}{\gcd(n,a)}$.
(b) Show that C_n has $\phi(n)$ generators, where $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$ is the Euler totient function.
(c) Let $A = \mathbb{Z}/n\mathbb{Z}$. Show that if $d|n$ then $A[d] = \{a \in A \mid d \cdot a = [0]\}$ (see problem P1) is the subgroup generated by the residue class of $\frac{n}{d}$.
(d) Show that C_n has a unique subgroup of order d for each $d|n$.

4. We show "If G has order n, and for every $d|n$ there is at most one subgroup of order d then G is cyclic". For this let G be a minimal counterexample.
(a) Show that every proper subgroup of G is cyclic.
(b) Show that, for each proper divisor $d|n$, G has at most $\phi(d)$ elements of order exactly d (hint: let $g \in G$ have order d; what can you say about $\langle g \rangle$?)
(c) Use the formula $\sum_{d|n} \phi(d) = n$ show that G is cyclic.

PRAC Let F be a field, and let $H \subset F^\times$ be a finite group.
(a) Show that for each positive integer d, H has at most d elements of order dividing d (hint: express the statement "x has order dividing d" by a polynomial equation, and use the fact that a polynomial of order d over a field has at most d roots).

(b) Show that H is cyclic.

Automorphisms of groups and semidirect products

5. Let H, N be groups, and let $\varphi \in \mathrm{Hom}(H, \mathrm{Aut}(N))$ be an action of H on N by automorphisms.
DEF The (external) *semidirect product* of H and N *along* φ is the operation

$$(h_1, n_1) \cdot (h_2, n_2) = \left(h_1 h_2, \left(\varphi(h_2^{-1}) n_1\right) n_2\right)$$

on the set $H \times N$. We denote this group $H \ltimes_\varphi N$.
PRAC Verify that when φ is the trivial homomorphism ($\varphi(h) = \mathrm{id}$ for all $h \in H$), this is the ordinary direct product.
(a) Show that the semidirect product is, indeed, a group.
(b) Show that $f_H \colon H \to H \ltimes_\varphi N$ given by $f(h) = (h, e)$, $f_N \colon N \to H \ltimes_\varphi N$ given by $f(n) = (e, n)$ and $\pi \colon H \ltimes_\varphi N \to H$ given by $\pi(h, n) = h$ are group homomorphisms.
(c) Show that $\tilde{H} = f_H(H)$ and $\tilde{N} = f_N(N)$ are subgroups with $\tilde{N}$ normal. Show that for $\tilde{h} = (h, e)$ and $\tilde{n} = (e, n)$ we have $\tilde{h}\tilde{n}\tilde{h}^{-1} = \widetilde{(\varphi(h))}(n)$.
(d) Show that $H \ltimes_\varphi N$ is the internal semidirect product of its subroups $\tilde{H}$, $\tilde{N}$.

Supplementary problems

A. Let D_{2n} be the dihedral group, acting on the graph with vertices $\{1, 2, \cdots, n\}$ and edges $\{\{1,2\}, \{2,3\}, \ldots, \{n,1\}\}$.
PRAC Let $c = (123\cdots n) \in D_{2n}$ be the "rotation" and let $r(i) = n + 1 - i$ be the "reflection". Show that $r, c \in D_{2n}$.
(a) Show that $C = \langle c \rangle \simeq C_n$ and that $R = \langle r \rangle \simeq C_2$. Show that R normalizes C.
(b) Show that $D_{2n} = R \ltimes C$, and in particular that every element of D_{2n} is either of the form c^j or rc^j.
(c) Give the multiplication rule in those coordinates. In particular, show that all the elements of the form rc^j are of order 2.
(d) Find all the conjugacy classes in D_{2n}.

Solving the following problem involves many parts of the course.

B. Let G be a group of order 8.
(a) Suppose G is commutative. Show that G is isomorphic to one of C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$.
(b) Suppose G is non-commutative. Show that there is $a \in G$ of order 4 and let $H = \langle a \rangle$.
(c) Show that $a \notin Z(G)$ but $a^2 \in Z(G)$.
(d) Suppose there is $b \in G - H$ of order 2. Show that $G \simeq D_8$ (hint: $bab^{-1} \in \{a, a^3\}$ but can't be a).
(e) Let $b \in G - H$ have order 4. Show that $bab^{-1} = a^3$and that $a^2 = b^2 = (ab)^2$.
(f) Setting $c = ab$, $-1 = a^2$ and $-g = (-1)g$ show that $G = \{\pm 1, \pm a, \pm b, \pm c\}$with the multiplication rule $ab = c$, $ba = -c$, $bc = a$, $cb = -a$, $ca = b$, $ac = -b$.
(g) Show that the set in (f) with the indicated operation is indeed a group.
DEF The group of (f),(g) is called the *quaternions* and indicated by Q.

Supplement: p-Sylow subgroups

C. Let G be a group (especially infinite).

DEF Let X be a set. A *chain* $\mathcal{C} \subset P(X)$ is a set of subsets of X such that if $A, B \in \mathcal{C}$ then either $A \subset B$ or $B \subset A$.

(a) Show that if $\mathcal{C}$ is a chain then for every finite subset $\{A_i\}_{i=1}^n \subset \mathcal{C}$ there is $B \in \mathcal{C}$ such that $A_i \subset B$ for all i.

(b) Suppose $\mathcal{C}$ is a non-empty chain of subgroups of a group G. Show that the union $\bigcup \mathcal{C}$ is a subgroup of G containing all $A \in cC$.

(c) Suppose $\mathcal{C}$ is a chain of p-subgroups of G. Show that $\bigcup \mathcal{C}$ is a p-group as well.

(*d) Use Zorn's Lemma to show that every group has maximal p-subgroups (p-subgroups which are not properly contained in other p-subgroups), in fact that every p-subgroup is contained in a maximal one.

RMK When G is infinite, it does not follow that these maximal subgroups are all conjugate.

4.3. Sylow's Theorems (Lecture 17, 4/11/2014)

We substantially strengthen Cauchy's Theorem.

4.3.1. The Sylow Theorems. Fix a group G of order n, and let $n = p^r m$ where $p \nmid m$.

THEOREM 175 (Sylow I). *If $p^i | n$ then G contains a subgroup of order p^i.*

PROOF. By induction on i, the case $i = 0$ being trivial. Accordingly let p^{i+1} divide the order of G, and let $H < G$ be a subgroup of order p^i. Let H act from the left on G/H. Since H is a p-group, $\#\mathrm{Fix}(H) \equiv \#(G/H)\ (p)$, so $p | \#\mathrm{Fix}(H)$. Now $gH \in \mathrm{Fix}(H)$iff for all $h \in H$ we have

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

so $gH \in \mathrm{Fix}(H)$ iff $H \subset gHg^{-1}$. Since these groups have the same order, we see that $gH \in \mathrm{Fix}(H)$ iff $g \in N_G(H)$, so $\mathrm{Fix}(H) = N_G(H)/H$. It follows that the group $N_G(H)/H$ has order divisible by p. By Cauchy's Theorem (Theorem 164), it has a subgroup C of order p, whose inverse image in $N_G(H)$ has order $p \cdot p^i = p^{i+1}$. □

REMARK 176. 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 177. *Then every maximal (by inclusion) p-subgroup of G has order p^r.*

DEFINITION 178. A maximal p-subgroup of G is called a *p-Sylow subgroup* of G. We write $\mathrm{Syl}_p(G)$ for the set of such subgroup and $n_p(G) = \#\mathrm{Syl}_p(G)$ for their number.

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

LEMMA 179. *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 180 (Sylow II,III). *The p-Sylow subgroups of G are all conjugate (in particular, $n_p(G) | n$). Furthermore, $n_p(G) \equiv 1\ (p)$ (so actually $n_p(G) | m$).*

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

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

REMARK 181. If $n = p^k m$ with $p \nmid m$, then we actually saw $n_p(G) | [G : P] = m$.

4.3.2. Applications.

EXAMPLE 182. The only groups of order 12 are C_{12}, $C_2 \times C_6$, A_4, $C_2 \times S_3$ and $C_4 \ltimes C_3$.

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

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

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

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

□

EXAMPLE 183. 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. □

EXAMPLE 184. Let G be a simple group of order 60. Then $G \simeq A_5$

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

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

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

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

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

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

□

EXAMPLE 185. No group of order p^2q is simple.

PROOF. Suppose Sylow subgroup not normal. Then $n_p(G) = q$, so $q \equiv 1\,(p)$ and neccessarily $q > p$. Also, $n_q(G) \in \{p, p^2\}$ and in either case we get $p^2 \equiv 1\,(q)$ so $p \equiv \pm 1\,(q)$. But $p < q$ so this forces $p = q-1$ and $n_q(G) = p^2$ (in fact we must have $p = 2$, $q = 3$). We thus have $p^2(q-1)$ elements of order q, hence at most p^2 elements of order dividing p, so $n_p(G) = 1$. $\square$

Math 322: Problem Set 9 (due 13/11/2014)

P1. In class we classified the groups of order 12, finding the isomorphism types A_{12}, C_{12}, $C_4 \ltimes C_3$, $C_2 \times C_6$, $C_2 \ltimes S_6$. The dihedral group D_{12} is a group of order 12 – where does it fall in this classification?

Sylow's Theorems

1. Show that there is no simple group of order 36 (hint: construct a non-trivial action on a set of size 4).

2. Let G be a group of order $255 = 3 \cdot 5 \cdot 17$.
   (a) Show that $n_{17}(G) = 1$.
   (*b) Show that P_{17} is central in G (hint: conjugation gives a homomorphism $G \to \mathrm{Aut}(P_{17})$).
   (*c) Show that $n_5(G) = 1$
   (d) Show that P_5 is also central in G.
   (e) Show that $G \simeq C_3 \times C_5 \times C_{17} \simeq C_{255}$.

3. Let G be a group of order 140
   (a) Show that $G \simeq H \ltimes C_{35}$ where H is a group of order 4.
   (*b) Classify actions of C_4 on C_{35} and determine the isomorphism classes of groups of order 140 with $P_2 \simeq C_4$.
   (**c) Classify actions of V on C_{35} and determine the isomorphism classes of groups of order 140 with $P_2 \simeq V$.
4. Let G be a finite group, $P < G$ a Sylow subgroup. Show that $N_G(N_G(P)) = N_G(P)$ (hint: let $g \in N_G(N_G(P))$ and consider the subgroup gPg^{-1}).

*5. Let G be a finite group of order n, and for each $p|n$ let P_p be a p-Sylow subgroup of G.
   (a) Show that $G = \left\langle \bigcup_{p|n} P_p \right\rangle$.
   (b) Suppose that G_p has a unique p-Sylow subgroup for each p. Show that $G = \prod_p P_p$ (internal direct product).

CHAPTER 5

Solvability

Math 322: Problem Set 10 (due 20/11/2014)

P1. Find a group G and three pairwise disjoint subgroups A, B, C such that the multiplication map $A \times B \times C \to G$ is not injective.

DEFINITION. Let G be a group. Call $g \in G$ a *torsion element* if g has finite order ($g^k = e$ for some $k \neq 0$), and write G_{tors} for the set of torsion elements. Say that g is *p-power torsion* if its order is a power of p. For an abelian group write $A[p^\infty]$ for the set of its p-power torsion elements.

P2. (Torsion) Let G, H be groups, A an abelian group.
(a) If G is finite then $G = G_{\text{tors}}$. Give an example of an infinite consisting entirely of torsion elements.
(b) Show that $f(G_{\text{tors}}) \subset H_{\text{tors}}$ for any $f \in \text{Hom}(G, H)$.
(c) $A_{\text{tors}} = \bigcup_{n \geq 1} A[n]$, $A[p^\infty] = \bigcup_{r=0}^{\infty} A[p^r]$.
(d) Let $X \in \text{GL}_n(\mathbb{R})$ be a torsion element. Show that the eigenvalues of X are (possibly complex) roots of unity.
(e) Find $X, Y \in \text{GL}_n(\mathbb{R})_{\text{tors}}$ such that XY has infinite order.

Abelian groups

1. (First do problem P2) Fix an abelian group A.
(a) Show that A_{tors} and $A[p^\infty]$ are subgroups of A.
(b) Show that $A[p^\infty]$ is the p-Sylow subgroup of A.
— It follows that, if A is finite, $A = \prod_p A[p^\infty]$ as an internal direct product.
(c) Show that A/A_{tors} is *torsion-free*: $(A/A_{\text{tors}})_{\text{tors}} = \{e\}$.

2. Find the Sylow subgroups of $C_{360} \times C_{300} \times C_{200} \times C_{150}$.

Nilpotent groups and torsion

3. Let G be *two-step nilpotent*, in that $G/Z(G)$ is abelian.
PRAC Verify that the Heisenberg group (PS7 problem P2) is two-step nilpotent.
(a) For $x, y \in G$ let $[x, y] = xyx^{-1}y^{-1}$ be their commutator. Show that $[x, y] \in Z(G)$ for all G (hint: this is purely formal).
(b) Let $x, y \in G$ and $z, z' \in Z(G)$. Show that $[x, y] = [xz, yz']$ and conclude that the commutator induces a map $G/Z \times G/Z \to Z$.
(c) Show that this map is *anti-symmetric*: $[\bar{y}, \bar{x}] = [\bar{x}, \bar{y}]^{-1}$ and *biadditive:* $[\bar{x}\bar{x}', \bar{y}] = [\bar{x}, \bar{y}]\,[\bar{x}', \bar{y}]$, $[\bar{x}, \bar{y}\bar{y}'] = [\bar{x}, \bar{y}]\,[\bar{x}, \bar{y}']$.
RMK In fact, a two-step nilpotent group is more-or-less determined by the abelian groups $A = G/Z(G)$, $Z = Z(G)$ and the anti-symmetric biadditive form $[\cdot, \cdot] : A \times A \to Z$.

4. (Torsion in nilpotent groups) Continue with the hypotheses of problem 3.
(a) Let $x, y \in G$ and suppose that $x \in G_{\text{tors}}$. Show that $[x, y] \in Z(G)_{\text{tors}}$.
(*b) (The hard part). Show that G_{tors} is a subgroup of G.

RMK In general, a group is 0-step nilpotent if it is trivial, $(k+1)$-step nilpotent if $G/Z(G)$ is k-step nilpotent, and *nilpotent* if it is k-step nilpotent for some k. A variant on the argument above shows that the set of torsion elements of any nilpotent group is a subgroup.

5.1. Finite abelian groups

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

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

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

$$A \simeq \prod_p A_p,$$

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

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

5.1.3. Statement.

THEOREM 186 (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.*

By the reduction before, enough to consider abelian p-groups.

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

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

By induction the e_i with $e_i > 1$ as uniquely defined; say there are r' of them. Then there were $r - r'$ i with $e_i = 1$.

5.1.5. Existence. Let e be maximal such that A has elements of order p^e, and consider the map $a \mapsto a^{p^{e-1}}$. This maps $A \to A[p]$; pull back a basis for the image to get $\{b_{e,i}\}_{i=1}^{I_e}$.

LEMMA 187. *They generate a subgroup A_{p^e} isomorphic to $(C_{p^e})^{I_e}$.*

PROOF. Raise any relation to the power p^{e-1}. □

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

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

LEMMA 188. *They generate a subgroup $A_{p^{e-1}}$ isomorphic to $\left(C_{p^{e-1}}\right)^{I_{e-1}}$, disjoint from A_{p^e}.*

Now continue by induction.

5.1.6. On rank. sdf

5.2. Finitely generated abelian groups

PROPOSITION 189. *$\mathbb{Z}^d$ is free.*

LEMMA 190. *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 191. *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. □

EXAMPLE 192. Elliptic curves and Mordell–Weil.

5.3. Normal series and solvability

5.3.1. Motivation: Galois theory.

PROPOSITION 193. *Let p be prime. Then S_p is generated by any p-cycle and involution.*

5.3.2. Solvable groups.

DEFINITION 194 (Normal series).

DEFINITION 195. G is solvable if it has a normal series with each quotient abelian.

EXAMPLE 196. Abelian groups. Upper-triangular group. Non-example: S_n, $n \geq 5$.

LEMMA 197. *Any subgroup of a solvable group is solvable.*

THEOREM 198. *Let $N \lhd G$. Then G is solvable iff $N, G/N$ are.*

DEFINITION 199 (Derived subgroup).

LEMMA 200. *G/N is abelian iff $G' \subset N$.*

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

THEOREM 201. *The derived series is the fastest descending series with abelian quotients.*

COROLLARY 202. *G is solvable iff $G^{(k)} = \{e\}$ for some k.*

PROPOSITION 203. *$K \operatorname{char} N \operatorname{char} G \Rightarrow K \operatorname{char} G$. In particular, $G^{(i)}$ are all normal in G.*