Math 110AH Notes

Charlie Cronenwett

September 2023

Intro

My notes for Math 110AH, taught by Alexander Merkurjev (merkurev@math.ucla.edu)at UCLA in Fall 2023.

Lecture 1

- Course sequence is essentially Math 210 but slower.
- Ch. 1 - Integers
- Ch. 2 - Groups

0 Notation

0.1 Sets

$x \in X$ means x is an element of X, $X \bigcup Y$ is union of sets X and Y, $X \bigcap Y = \{x \in X | x \in Y\}$, $X \times Y = \{(x, y) | x \in X, y \in Y\}$

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are all just like normal.

0.2 Functions

(Informal) Let X, Y be sets. A map/function $f : X \to Y$ is a rule that sends every element $x \in X$ to $f(x) \in Y$.

(Actual) A map $f : X \to Y$ is a subset $\Gamma \subset X \times Y$ such that $\forall x \in X, \exists! y \in Y$ s.t. $(x, y) \in \Gamma$, and $f(x) = y$ s.t $(x, y) \in \Gamma$.

Let $f : X \to Y, g : Y \to Z$. Then $h = g \circ f : X \to Z$ is defined as $\{(x, g(f(x))) | x \in X\}$.

The set $Id_X := \{(x, x) | x \in X\}$ is the identity function $X \to X$.

A function $f : X \to Y$ is injective $\iff (\forall x_1 \neq x_2 \in X, f(x_1) \neq f(x_2))$.

A function $f : X \to Y$ is surjective $\iff (\forall y \in Y \exists x \in X : y = f(x)$.

A function is bijective if it's injective and surjective.

Let $f : X \to Y$, then $g : Y \to X$ is the inverse of f, or f^{-1}, if $g \circ f = Id_X$ and $f \circ g = Id_Y$.

Proposition 1. *A map $f : X \to Y$ has an inverse $\iff$ X is bijective.*

Proof. ($\implies$) Let $g = f^{-1}$. Suppose $f(x_1) = f(x_2)$.

Then $x_1 = Id_X(x_1) = g(f(x_1)) = g(f(x_2)) = Id_X(x_2) = x_2$, so f is injective.

Let $y \in Y$. Then $g(y) \in X$, and $f(g(y)) = Id_Y(y) = y$, so $\exists x = g(y) \in X$ s.t $f(x) = y$, so f is surjective.

f is surjective and injective, hence bijective.

($\impliedby$) Suppose f is bijective. By injectivity and surjectivity of f, for all $y \in Y$, $\exists! x \in X : y = f(x)$. Let $g(y) = x$ as we defined x. Then $g(f(x)) = x$, $f(g(y)) = y$, as desired, so g is the inverse of f. $\square$

Ch I. Integers

1 Induction

(Principle of Induction)Let $n_0 \in \mathbb{Z}, P(n)$ is a statement $\forall n \geq n_0$.

If $P(n_0)$ and $(\forall n \geq n_0 : P(n) \implies P(n+1))$ then $P(n)$ is true for all $n \in \mathbb{Z}$ s.t. $n \geq n_0$.

(Strong Induction) If $P(n_0)$ and
$(\forall n \geq n_0 : (P(k)$ is true $\forall k \in \mathbb{Z} : n_0 \leq k \leq n) \implies P(n+1))$, then $P(n)$ for all $n \in \mathbb{Z} : n \geq n_0$.

Ex. All positive integers can be written as $2^{k_1} + 2^{k_2} + \cdots + 2^{k_m}$, where $k \in \mathbb{Z}$, and all of the k_i are distinct.

Proof. Base case obvious since $1 = 2^0$.

Assume $P(k)$ is true for all $1 \leq k < n$. Find the largest s such that $2^s \leq n$. If $n = 2^s$ we're done. Otherwise, $2^s < n$, so $p := n - 2^s > 0$, so by $P(p)$ we have $p = 2^{k_1} + 2^{k_2} + \cdots + 2^{k_m}$. $p < 2^s$ because otherwise $n > 2^{s+1}$, a contradiction, so s is distinct from all the prior k_i, so $n = 2^s + 2^{k_1} + 2^{k_2} + \cdots + 2^{k_m}$, as desired. $\square$

2 Division of Integers

Definition 1. *Let $n, m \in \mathbb{Z}, m \neq 0$. Then n is divisible by m if there exists $q \in \mathbb{Z}$ such that $n = mq$.*

Here are some divisibility facts:

$1 | n \forall n \in \mathbb{Z}$

$m | 0 \forall m \in \mathbb{Z}, m \neq 0$

$m | n_1$ and $m | n_2 \implies m | (n_1 + n_2)$.

And here are there proofs:

Proof. $n = 1(n)$

$0 = 0(m)$

Let $n_1 = am, n_2 = bm$ for $a, b \in \mathbb{Z}$. Then $n_1 + n_2 = (a+b)m$, so m divides $n_1 + n_2$. $\square$

Lecture 2

Proposition 2. *If $m|n$, $m|an$ $\forall$ $a \in \mathbb{Z}$.*

Proof. $n = mq, q \in \mathbb{Z}$, so $an = m(aq)$, and $aq \in \mathbb{Z}$, so $m|an$. □

Proposition 3. *If $m|n_1$ and $m|n_2$, $m|a_1n_1 + a_2n_2 \forall a_1, a_2 \in \mathbb{Z}$*

Proof. By Proposition 2 and the third divisibility fact, $m|a_1n_1$ and $m|a_2n_2$, so $m|a_1n_1 + a_2n_2$ □

Proposition 4. *If $m|n$ and $n \neq 0, |m| \leq |n|$*

Proof. $n = mq, q \in \mathbb{Z}, q \neq 0$, so $|n| = |m||q| \geq |m|$ □

Proposition 5. *If $m|n$ and $n|m$, $n = \pm m$*

Proof. By Proposition 4, $|m| \leq |n| \leq |m|$, so $|m| = |n|$, so $m = \pm n$. □

Theorem 1 (Division Algorithm)**.** *Let $n, m \in \mathbb{Z}$, $m \neq 0$. Then there exist unique $q, r \in \mathbb{Z}$ such that $n = mq + r$ and $0 \leq r < |m|$.*

Proof. (Existence) Let $S = \{n - mx, x \in \mathbb{Z}\}$. Note that S contains at least one nonnegative integer. Recall that every nonempty subset of $\mathbb{N}$ has a least element, so consider the least element of $S \bigcap \mathbb{N}$, $n - mx$. Let $q = x$, $r = n - mx$. Then $n = mq + r$. Then $r - |m| = n - m(q \pm 1)$, and $r - |m| < r$, so $r - |m| \notin \mathbb{N}$, so $r - |m| < 0$, so $r < |m|$. $r, q \in \mathbb{Z}$, so we've proven existence.

(Uniqueness) Suppose $n = mq_1 + r_1 = mq_2 + r_2$, where $0 \leq r_1, r_2 < m$. Then $0 = m(q_1 - q_2) + (r_1 - r_2)$. So $r_1 - r_2 = m(q_2 - q_1)$. So because $|r_1 - r_2| < |m|$, $-1 < q_2 - q_1 < 1$, so $q_2 = q_1$, so it follows that $r_1 = r_2$, so our q and r are unique. □

Definition 2. *Let $n > 0$. Then $d \in Z, d \neq 0$ is a divisor of n if $d|n$.*

$d \leq |n|$, so any integer $n > 0$ has finitely many divisors.

Definition 3. *Let $n, m \in \mathbb{Z}$ such that $n, m > 0$. Then*
$d = \max(\{z \in \mathbb{Z}|z|n \text{ and } z|m\}) = \gcd(n, m) \geq 1$

The Euclidean Algorithm is as follows. For $n, m > 0$, use the Division Algorithm to get $n = mq_1 + r_1, 0 \leq r_1 < m$. Then get $m = r_1q_2 + r_2, 0 \leq r_2 < r_1$, then $r_1 = r_2q_3 + r_3, 0 \leq r_3 < r_2, \cdots, r_{k-2} = r_{k-1}q_k + r_k$. The r_i are a series of strictly decreasing non-negative integers, so eventually we get $r_{k-1} = r_kq_{k+1}$.

Theorem 2. $r_k = \gcd(n, m)$

Proof. $r_1 = n - mq_1$
$r_2 = m - r_1q_2$
$r_3 = r_1 - r_2q_3$
$\cdots$
$r_k = r_{k-2} - r_{k-1}q_k$

Because d divides n and m, $d|r_1$, so $d|r_2$, etc. Thus, $d|r_k$.

Conversely, r_k divides r_{k-1}, so r_k divides r_{k-2}, etc, up until r_k divides m and r_k divides n.

So r_k is a common divisor of n and m. Thus, $r_k \leq d$, and $d|r_k$, so $d = r_k$. $\square$

Theorem 3 (Bézout's Lemma)**.** *Let $n, m > 0$, $d = \gcd(n, m)$. Then there are $x, y \in \mathbb{Z}$ such that $d = nx + my$.*

Proof. Obviously, by the Euclidean algorithm $d = r_k$ is a linear combination of n, m, so we're done. Could do induction if unclear. $\square$

Here's an alternate proof

Proof. Let $S = \{nx + my | x, y \in \mathbb{Z}\}$. Let s be the least positive integer in S. Then we claim $s = d$.

$s = nx + my$, so by division algorithm $n = sq + r$, $0 \leq r < s$. So $r = n - sq = n - (nx + my)q = n(1 - x) - myq$. $r \geq 0$, but $r < s$, so $r = 0$, so s divides n, so s also divides m by $s = nx + my$, so $s \leq d$. But $d|nx + my = s$, so $d|s$, so $s = d$. $\square$

This also gives us that d is the smallest positive number that can be written as a linear combo of x, y.

Lecture 3

Corollary 1. *Let $n, m > 0$. Then n and m are relatively prime $\iff \exists x, y \in \mathbb{Z}$ s.t. $nx + my = 1$.*

Proof. $\implies$ is obvious by Bézout's lemma

($\impliedby$). If $nx + my = 1$, then 1 is a divisor of n, m, so $d := \gcd(m, n) \geq 1$. $d|n$ and $d|m$, so $d|1$. Thus, $1 = d$. $\square$

Definition 4. *An integer $p > 1$ is prime if the only divisors of p are ± 1 and $\pm p$*

Obviously, if $n > 0$, p prime, then $\gcd(n, p)$ is p is $p|n$, and 1 otherwise.

Proposition 6. *Every integer $n > 1$ is a product of prime integers.*

Proof. By induction, consider the statement $P(n) : n$ is a product of primes. Obviously, if, $n_0 = 2$, then $P(n_0)$ holds.

Now assume $P(k) \forall k \leq 2 < n$. If n is prime, then we're done. If n is not prime, there exist $s, t \in \mathbb{Z}$ for $n > s, t > 1$ such that $n = st$. By the induction hypothesis, s and t are products of primes. Thus, n is also a product of primes. So $P(n)$ is true, and we're done. $\square$

Lemma 1. *Let p be a prime, $n, m > 0$, and $p|nm$. Then $p|n$ or $p|m$.*

Proof. If $p|n$ we're done. Otherwise, $\gcd(p, n) = 1$, so there exist $x, y \in Z$ such that $1 = px + ny$ by Bézout's Lemma. So $m = pmx + nmy$. But $p|pmx$ and $p|nmy$, so $p|m$, and we're done. $\square$

Corollary 2. *Let $p \in Z$ be prime, and $n_1, n_2, \cdots, n_s > 0$ s.t. $p|n_1 n_2 \cdots n_2$. Then there exists $1 \leq i \leq s$ such that $p|n_i$.*

Proof. We already know it holds for $s = 1, 2$. Suppose it holds for $s = k - 1$. Then if $p|n_1 n_2 \cdots n_k = (n_1 n_2 \cdots n_{k-1})(n_k)$, by the previous lemma, either $p|n_k$, in which case we're done, or $p|(n_1 n_2 \cdots n_{k-1})$, in which case by the induction hypothesis, $p|n_i$ for some $1 \leq i \leq k - 1$, and we're done. $\square$

Definition 5. *Suppose $n = p_1 p_2 \cdots p_2 = q_1 q_2 \cdots q_t$, where p_i, q_i are prime. We say these two factorizations are the same if $s = t$ and for all $j = 1, 2, \cdots, t$, $q_j = p_{\alpha(j)}$, where α is a bijection from $\{1, 2, \cdots, s\}$ to itself.*

Theorem 4 (Fundamental Theorem of Arithmetic)**.** *Every integer $n > 1$ admits a unique factorization as a product of primes.*

Proof. We already know existence by Proposition 6. Suppose $n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$ for p_i, q_i primes. We proceed by induction on s to show the two factorizations are the same.

When $s = 1$, $n = p_1 = q_1 \cdots q_t$, p_1 has no prime factors other than itself, so $t = 1$, and $p_1 = q_1$.

Now suppose a product of $s - 1$ primes has a unique prime factorization up to permutation. Then $p_s|q_1 q_2 \cdots q_t$, so Lemma 1, and WLOG, we may assume $p_s|q_t$, so because $p_s|q_t$, $p_s = q_t$. Then because $p_s, q_t \neq 0$, $p_1 p_2 \cdots p_{s-1} = q_1 q_2 \cdots q_t$, so by the induction hypothesis, the q_j are the p_i up to permutation, so all the prime factors of n are the same up to permutation, so n admits a unique prime factorization up to permutation. $\square$

Proposition 7. *Let $n = p_1^{a_1} \cdots p_k^{a_k}, m = p_1^{b_1} \cdots p_k^{b_k}$, where $a_i, b_i \geq 0$. Then $m|n \iff b_i \leq a_i$ for all $1 \leq i \leq k$.*

Proof. ($\implies$) If $n = mq$, then because n admits a unique prime factorization, it must be such that $b_i \leq a_i$. Otherwise, the factors of q cannot make the exponent of p_i smaller.

($\impliedby$)If $b_i \leq a_i$, then $n = m(p_i^{a_i - b_i})$ $\square$

Lecture 4

Theorem 5 (Euclid)**.** *There are infinitely many primes.*

Proof. Suppose there are finitely many primes $p_1, p_2, \cdots, p_n$. Then let $N = p_1 p_2 \cdots p_n + 1$. Let p be a prime divisor of N, which we know to exist by Proposition 6. So $p|p_1 p_2 \cdots p_n$, so $p|1$, a contradiction. $\square$

3 Congruences

Definition 6. *Let $m > 0$. Then a, b are congruent* $\mod m$ *if* $a - b | m$.

Proposition 8. $a \equiv b(\mod m) \iff$ *a and b have the same remainder dividing by m.*

Proof. ($\implies$). $m|(b-a)$, so $b-a = mx$. By the division algorithm, $a = mq+r$, $0 \leq r < m$ So $b = a + mx = m(x+q)+r$, so b has remainder r.

($\impliedby$) $a = mq + r, b = ms + r$, so $b - a = m(s-q)$, so $m|b-a$, so $a \equiv b \mod m$ □

Corollary 3. *Every integer a is congruent* $\mod m$ *to exactly one integer in the set* $\{0, 1 \cdots, m-1\}$.

Proof. By the division algorithm, $a = mq+r$, and $r = 0m+r$, so $a \equiv r \mod m$. If $x \neq r, 0 \leq x < m$, then $a-x = a-r+(r-x) = qm+r-x$, but $0 < |r-x| < m$, so $m \not| a-x$. □

Trivial, but you can add and multiply congruences without problems/as expected.

If $a \equiv b$, $ax \equiv bx$ for $x \in \mathbb{Z}$ because $ax - bx = (a-b)x$, and $m|a-b$.

If $a_1 \equiv b_1, a_2 \equiv b_2$, then $a_1 + a_2 \equiv b_1 + b_2$ because $m|(b_1 - a_1) + (b_2 - a_2)$.

Furthermore, $b_1b_2 - a_1a_2 = b_1b_2 - a_1b_2 + a_1b_2 - a_1a_2 = b_2(b_1-a_1)+a_1(b_2-b_1)$, which m obviously divides and $a_1b_1 \equiv a_2b_2 \mod m$.

Then Merkurjev just started talking about equivalence relations, equivalence classes, and equivalence relations on a set being in bijection with partitions of the set. Kinda disappointing, but I guess an easy way to end the week.

Obviously, congruences are an equivalence relation though.

Lecture 5

This week's lectures are by Hannah Knight, a postdoc.

Proposition 9. $\equiv \mod m$ *is an equivalence relation.*

Proof. $m|a-a = 0$, so $a \equiv a \mod m$.

If $a \equiv b \mod m, m|b-a$, so $m|a-b = -(b-a)$, so $b \equiv a \mod m$.

If $a \equiv b \mod m, b \equiv c \mod m$, then $m|b-a, m|c-b$, so $m|(b-a)+(c-b) = c-a$, so $a \equiv c \mod m$ □

Equivalence classes work the way we expect. For $a \in \mathbb{Z}, [a]$ is the set of all integers congruent to $a \mod m$.

Proposition 10. *(a)* $[a] = [b] \iff a \equiv b \mod m$

(b) $[a] \bigcap [b] = \emptyset \iff a \not\equiv b \mod m$

This is obvious for any equivalence relation.

Proposition 11. *There are exactly m congruence classes $\mod m$. Namely, $[0], [1], \cdots [m-1]$.*

Proof. Let $0 \leq p, q < m$, $p \neq q$. WLOG, suppose $p < q$. Then $0 < q - p < m$, so $q - p$ doesn't divide m, so $q \not\equiv p \mod m$, so $[q]$ and $[p]$ are distinct for all $0 \leq q, p < m$, $q \neq p$. For any $n \in \mathbb{Z}$, by the division algorithm, we have $n = mq + r$, where $q, r \in Z, 0 \leq r < m$, so $m|mq = n - r$, so $n \equiv r \mod m$, so for all $n \in \mathbb{Z}, [n] = [r]$ for some $0 \leq r < m$. So our equivalence classes are exactly $[0], [1], \cdots [m-1]$, as desired. □

Definition 7. $\mathbb{Z}/m\mathbb{Z} = \{$*congruence classes of integers* $\mod m\}$

We define addition on $\mathbb{Z}/m\mathbb{Z}$ as $[a]+[b] = [a+b]$. This is well defined because for any $x \in [a], y \in [b]$, $[x+y] = [a - cm + b - dm] = [a + b - (c+d)m] = [a+b]$ for some $c, d \in Z$.

So it follows from commutativity and associativity of the integers that addition $\mathbb{Z}/m\mathbb{Z}$ is commutative and associative, $[0]$ is the additive identity, and $[-a]$ is the additive inverse of $[a]$.

We define multiplication on $\mathbb{Z}/m\mathbb{Z}$ as $[a] \cdot [b] = [a \cdot b]$. This is well defined by some results from the end of Lecture 4.

By associativity and commutativity of integer multiplication, we get multiplication on $\mathbb{Z}/m\mathbb{Z}$ is commutative, associative, and distributive, and has $[1]$ as multiplicative identity.

Lecture 6

Definition 8. *We say $[a]$ is invertible if there exists $[b] \in \mathbb{Z}/m\mathbb{Z}$ such that $[a][b] = [1]$.*

Theorem 6. *A congruence class $[a]$ is invertible $\iff \gcd(a, m) = 1$.*

Proof. ($\implies$) If $[a]$ is invertible, $[a][b] = [1]$, so $ab = 1 + qm$ for some $q \in \mathbb{Z}$, so $ab - qm = 1$, so by Bézout's, we have $\gcd(a, m)|1$, so $\gcd(a, m) = 1$.

($\impliedby$) If $\gcd(a, m) = 1$, then there exists $x, y \in \mathbb{Z}$ such that $ax + my = 1$ by Bézout's, so $ax = 1 - my$, so $[a][x] = [1]$, as desired. □

Definition 9. *We let $(\mathbb{Z}/m\mathbb{Z})^\times$ denote the set of all invertible congruence classes of $\mathbb{Z}/m\mathbb{Z}$*

Definition 10. *Euler's totient function $\phi : \mathbb{N} \to \mathbb{N}$ is defined by $\phi(m)$ is the number of integers $1, \cdots, m-1$ relatively prime to m.*

Obviously, $|(\mathbb{Z}/m\mathbb{Z})^\times| = \phi(m)$.

If m is prime, $\phi(m) = p - 1$.

If $m = p^k$, $\phi(m) = p^k - 1 - (p^{k-1} - 1) = p^k - p^{k-1} = p^{k-1}(p-1)$

Lemma 2. *Let $a|n, b|n$. If $\gcd(a, b) = 1$, $ab|n$.*

Proof. There exist $x, y \in \mathbb{Z}$ s.t. $ax + by = 1$. Then $nax + nby = n$. ab clearly divides each of the left hand terms, so $ab|n$. $\square$

Corollary 4. *If $m_1, \cdots, m_k|n$, $\gcd(m_i, m_j) = 1$ for $i \neq j$, then $m_1 \cdots m_k|n$.*

Proof. We proceed by induction on k. The base case of $k = 2$ is Lemma 2.

Now suppose it holds for $k = n - 1$. Then by the induction hypothesis, $m_1 \cdots m_{n-1}|n$, which is relatively prime with m_n, so by Lemma 2, $m_1 \cdots m_n|m_n$. $\square$

If $m|n$, we can map $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ by $[a]_n \mapsto [a]_m$. We will now show that this is well defined.

If $a \equiv b \mod n$, then $n|b - a$, so $m|b - a$, so $a \equiv b \mod m$, so $[a]_m = [b]_m$, so the function is well defined.

By extension, if $n = m_1 \cdots m_k$, we have a well-defined function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$, $[a]_n \mapsto ([a]_{m_1}, \cdots, [a]_{m_k})$

Theorem 7. *If $m_1, \cdots, m_k$ are pairwise relatively prime, f is a bijection.*

Proof. Since $|\mathbb{Z}/n\mathbb{Z}| = |\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}|$ is finite, it suffices to show that f is injective.

Assume $f([a]_n) = f([b]_n)$. Then $a \equiv b \mod m_i$ for all $1 \leq i \leq k$. So $m_i|b-a$, so by the corollary, $m_1 \cdots m_k = n|b - a$, so $[b]_n = [a]_n$, so f is injective, hence bijective. $\square$

Lecture 7

Corollary 5 (Chinese Remainder Theorem)**.** *If $x \equiv b_1 \mod m_1, \cdots, x \equiv b_k \mod m_k$, $m_1, \cdots, m_k$ pairwise relatively prime, then there exists such an x. Also, all solutions form an equivalence class $\mod n$.*

Proof. By Theorem 7, since f is a bijection, there exists unique $[x]_n$ such that $f([x]_n) = ([b_1]_{m_1}, \cdots, [b_k]_{m_k})$. $\square$

Ch 2. Groups

Definition 11. *A group $(G, *)$ is a set G, and a function $* : G \times G \to G$ such that*

1. $(a * b) * c = a * (b * c)$
2. *There exists $e \in G$ such that $a * e = e * a = a$ for all $a \in G$.*
3. *For any $a \in G$, there exists $b \in G$ such that $a * b = b * a = e$.*
4. *If $a * b = b * a$ for all $a, b \in G$, the group is abelian.*

Proposition 12. *The identity is unique.*

Proof. Suppose e_1, e_2 are identities. Then $e_1 = e_1 * e_2 = e_2$. $\square$

Proposition 13. *The inverse of $a \in G$ is unique.*

Proof. Suppose b, c are inverses of a. Then $b = eb = (ca)b = c(ab) = ce = c$, so $b = c$. $\square$

Proposition 14. $(a^{-1})^{-1} = a$.

Proof. $aa^{-1} = a^{-1}a = e$, so a is the unique inverse of a^{-1}. $\square$

a^n, a^{-n} are defined for $n \in \mathbb{N}$ as a^n is a times itself n times, a^{-n} is a^{-1} times itself n times.

By induction, $a^n a^m = a^{n+m}$, $a^{nm} = (a^n)^m$ are easy to show.

Lecture 8

Proposition 15. *For $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$*

Proof. $(ab)(b^{-1}a^{-1}) = aea^{-1} = aa^{-1} = e$
$(b^{-1}a^{-1})(ab) = b^{-1}eb = b^{-1}b = e$, so they're inverses. $\square$

Obviously, you can generalize this inverse to arbitrarily many a_i multiplied together by induction.

Proposition 16. $ax = bx \implies a = b$

Proof. $a = ae = a(xx^{-1}) = (ax)x^{-1} = (bx)x^{-1} = b(xx^{-1}) = be = b$ $\square$

Homomorphisms and Isomorphisms

Definition 12. *Let $G = (G, \cdot), H = (H, *)$ be groups. A homomorphism between G and H is a map $f : G \to H$ such that $f(x \cdot y) = f(x) * f(y)$ for all $x, y \in G$.*

Some examples of group homomorphisms are Id_G, $f : G \to H$ where $f(g) = e_H$ for all $g \in G$, sending $\mathbb{Z}$ to its equivalence class in $\mathbb{Z}/n\mathbb{Z}$, the projection from $G \times H$ to G by $(g, h) \mapsto g$.

For a subgroup $H \subseteq G$, $f : H \to G$, $h \mapsto h$ is a homomorphism as well.

Proposition 17. *Let $f : G \to H$ be a homomorphism. Then $f(e_G) = e_H$.*

Proof. $e_H f(e_G) = f(e_G) = f(e_G e_G) = f(e_G)f(e_G)$, so by Proposition 16, $e_H = f(e_G)$. $\square$

Proposition 18. $f(x^{-1}) = (f(x))^{-1}$

Proof. $f(x)f(x^{-1}) = f(xx^{-1}) = f(e_G) = e_H$
$f(x^{-1})f(x) = f(x^{-1}x) = f(e_G) = e_H$ $\square$

Definition 13. *A homomorphism $f : G \to H$ is an isomorphism if f is a bijection.*

Proposition 19. *If $f : G \to H$ is an isomorphism, so is $f^{-1} : H \to G$*

Proof. Obviously, f^{-1} is a bijection.

Let $a, b \in H$. Then because f is a bijection, there exist unique elements $x, y \in G$ such that $f(x) = a$, $f(y) = b$. Then $f(xy) = f(x)f(y) = ab$, so $f^{-1}(ab) = xy = f^{-1}(a)f^{-1}(b)$, so f^{-1} is an isomorphism. □

Proposition 20. *If $f : G \to H$, $g : H \to K$ are isomorphisms, so is gf.*

Proposition 21. *Obviously, gf is a bijection.*

Proof. For $a, b \in G$, $gf(ab) = g(f(a)f(b)) = gf(a)gf(b)$, as desired. □

Definition 14. *Two groups G, H are isomorphic if there exists an isomorphism $f : G \to H$*

Theorem 8. *Groups being isomorphic is an equivalence relation.*

Proof. $G \cong G$ by the identity. If $G \cong H$ by f, $H \cong G$ by f^{-1}. If $G \cong H$ by f and $H \cong K$ by g, $G \cong K$ by gf. □

Obviously, all groups of order 1 are isomorphic. You just map the identity element to the identity element.

All groups of order 2 are isomorphic. Let $G = \{e_1, g\}$, $H = \{e_2, h\}$ map e_1, e_2 to $[0]_2$, g, h to $[1]_2$. Obviously, these are both isomorphisms, by $f(xy) = f(x) + f(y)$, so by transitivity, $G \cong H$.

$\mathbb{C} \cong \mathbb{R} \times \mathbb{R}$ by $f(a, b) = a + bi$. This is clearly a bijection, and $f((a_1, b_1) + (a_2, b_2)) = f((a_1 + a_2, b_1 + b_2)) = (a_1 + a_2) + (b_1 + b_2)i = (a_1 + b_1 i) + (a_2 + b_2 i) = f(a_1, b_1) + f(a_2, b_2)$, as desired.

Lecture 9

$(\mathbb{R}, +) \cong (\mathbb{R}^{\geq 0}, \times)$ by $x \mapsto 2^x$.

For $n = m_1 \cdots m_k$, m_i relatively prime, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$ by Chinese remainder theorem.

Likewise, $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/m_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/m_k\mathbb{Z})^\times$ because x is invertible mod n is equivalent to x is invertible mod m_i for all m_i.

Cyclic Groups

Definition 15. *Let G be a group, $a \in G$. We define the order of a as the smallest positive integer n such that $a^n = e$. If such an n doesn't exist, the order of a is ∞.*

For example, the order of $(1\ 2) \in S_3$ is 2, the order of $(1\ 2\ 3) \in S_3$ is 3.
$\mathrm{ord}(a) = 1 \iff a = e$
In $(\mathbb{Z}, +)$, $\mathrm{ord}(1) = \infty$
In $(\mathbb{Z}/n\mathbb{Z}, +)$, $\mathrm{ord}(1) = n$

Definition 16. *Let G be a group, $a \in G$. We say that a generates G if for all $b \in G$, there exists $i \in \mathbb{Z}$ such that $b = a^i$. In this case, we say a is a generator of G, and G is cyclic.*

Obviously, a group H isomorphic to a cyclic group G is cyclic because for an isomorphism $f : G \to H$, we have for any $h \in H$, $h = f(a)$ for $a \in G$, but $f(a) = g^k$ for the generator g, so $h = f(g^k) = (f(g))^k$, so $f(g)$ generates H.

Proposition 22. *For cyclic G, $|G| = n \iff$ the order of a generator σ is n.*

Proof. ($\Longleftarrow$) Consider $\sigma^1, \cdots, \sigma^{n-1}$. Then $\sigma^i \neq \sigma^j$ for $1 \leq i < j \leq n-1$ because then $\sigma^{|i-j|} = 1$, contradicting n being the order of σ. So all such σ^i are distinct. Furthermore, since $\sigma^n = e$, $\sigma^p = \sigma^q$ if $p \equiv q \mod n$, so we have at most n distinct elements. Thus, we have exactly n distinct elements, and $|G| = n$.

($\Longrightarrow$) If G is generated by σ, then the order of σ is finite, because $\sigma^1, \cdots, \sigma^{n+1}$ cannot all be distinct, so $\sigma^{j-i} = 1$ for some $1 \leq i < j \leq n+1$. But by the above, $\mathrm{ord}(\sigma) \neq n \implies |G| \neq n$, a contradiction, so we're done. $\square$

Theorem 9. *Every cyclic group is isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}/m\mathbb{Z}$ for some $m \in \mathbb{N}$.*

Proof. Let G be a cyclic group with generator $g \in G$. If the order of G is finite(say n), we have a map $f : G \to \mathbb{Z}/n\mathbb{Z}$ by $g^i \mapsto i[1]$. This map is bijective because $g^i = g^j$ if and only if $i \equiv j \mod n$ if and only if $f(g^i) = f(g^j)$, and clearly $f(g^i) = [i]$ for any equivalence class $[i]$. Also, $f(g^i g^j) = f(g^{i+j}) = [i+j] = [i] + [j] = f(g^i) + f(g^j)$, so f is an isomorphism as desired.

If the order of G is infinite, then g^i is distinct for all $i \in \mathbb{Z}$. Consider the map $f : G \to \mathbb{Z}$ by $g^i \mapsto i$. Because each g^i is distinct, this map is well defined, so it's clearly bijective. And $f(g^i g^j) = f(g^{i+j}) = i + j = f(g^i) + f(g^j)$, as desired so f is an isomorphism.

$\square$

Lecture 10

Subgroups

Definition 17. *A subset $H \subseteq G$ of a group $G = (G, *)$ is a subgroup if $H = (H, *)$ is a group.*

Proposition 23. *$H \subseteq G$ is a subgroup $\iff e_G, x^{-1}, xy \in H$ for all $x, y \in H$.*

Proof. Obviously, if $e_G \in H$ and $x^{-1} \in H$, with inherited associativity from G, we get H is a group by associativity, closure, identity, and inverses.

If H is a group, it must have an identity. But the only element $x \in G$ such that $xa = a$ for all $a \in H$ is $x = e_G$ by the Cancellation law, so $e_G \in H$. Likewise, H has inverses and the unique inverse of $a \in H$ in G is a^{-1}, so $a^{-1} \in H$. □

Examples of subgroups are $\{e_G\}$ for any group G, $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

Proposition 24. *All subgroups $H \subseteq \mathbb{Z}$ are $n\mathbb{Z}$ for some $n \in \mathbb{Z}$.*

Proof. Assume $H \neq \{0\}$, because that case is trivial. So because every element of H has an inverse, and H has at least one positive integer, because if H has a negative element then it's inverse is in H. Let n be the smallest positive integer in H. Then we claim $H = n\mathbb{Z}$.

Because $n \in H$, $an \in H$ for all $a \in \mathbb{Z}$, so $n\mathbb{Z} \subseteq H$.

If $x \in H$, use division algorithm to get $x = nq + r$, $0 \leq r < n$. Then $r = x - nq \in H$ by closure of H, but $r < n$ so $r = 0$. Thus, $x = nq$ and $x \in n\mathbb{Z}$. So $H \subseteq n\mathbb{Z}$.

Thus, $H = n\mathbb{Z}$. □

Obviously $\mathbb{Q}^\times$ is a subgroup of $\mathbb{R}^\times$ is a subgroup of $\mathbb{C}^\times$.

$H = \{\sigma \in S_n | \sigma(n) = n\}$ is a subgroup of S_n. Furthermore, $H \cong S_{n-1}$ by the obvious bijection.

If $\{H_i\}_{i\in I}$ is a family of subgroups of G, then $\bigcap_{i\in I} H_i$ is a subgroup of G.

For $a \in G$, $\langle a \rangle = \{a^i | i \in \mathbb{Z}\}$ is a subgroup of G. By repeated applications of closure, we have $\langle a \rangle$ is the smallest subgroup containing a.

Definition 18. *For a homomorphism $f : G \to H, \ker f = \{x \in G | f(x) = e_H\}$.*

Definition 19. *For a homomorphism $f : G \to H, \mathrm{Im}(f) = \{f(x) | x \in G\}$.*

$f(e_G) = e_H$, and for $x_1, x_2 \in \ker f$, $f(x_1 x_2^{-1}) = f(x_1) f(x_2)^{-1} = e_G$, so $x_1 x_2^{-1} \in \ker f$, so the kernel is a subgroup of G.

$f(e_G) = e_H$, and for $f(x_1), f(x_2) \in \mathrm{Im}(f)$, $f(x_1) f(x_2)^{-1} = f(x_1 x_2^{-1})$, so $f(x_1) f(x_2)^{-1} \in H$ and $\mathrm{Im}(f)$ is a subgroup of H.

For the obvious homomorphism $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\ker(f) = n\mathbb{Z}$, $\mathrm{Im}(f) = \mathbb{Z}/n\mathbb{Z}$. More generally, for any quotient group G/H, the projection homomorphism $f : G \to G/H$ has $\ker(f) = H$, $\mathrm{Im}(f) = G/H$.

Consider $f : GL_n(\mathbb{R}) \to \mathbb{R}^\times$ by $A \mapsto \det(A)$. $\ker(f) = \{A | \det(A) = 1\}$.

$\mathrm{Im}(f) = \mathbb{R}^\times$.

Midterm 1 goes through cyclic groups, 5 proofs during class.

Lecture 11

Let H be a subgroup of G, then the inclusion map $f : H \to G$ has $\ker f = \{e_H\}$, $\mathrm{Im}(f) = H$.

In fact, for any injective homomorphism $f : H \to G$, $\ker f = \{e_H\}$, and because $f' : H \to \mathrm{Im}(f)$ by restricting the codomain of f but keeping the same mappings, f' is surjective and injective, so H is isomorphic to a subgroup $\mathrm{Im}(f)$ of G.

Proposition 25. *Let $f : G \to H$ be a group homomorphism. Then f is injective $\iff \ker(f) = \{e_G\}$, and f is surjective $\iff \mathrm{Im}(f) = H$, and f is bijective if and only if the former two equivalences are satisfied.*

Proof. The second statement is obvious, and the third is a combination of the first and second. We already know that f injective $\implies \ker(f) = \{e_G\}$, but now suppose $\ker(f) = \{e_G\}$, then if $f(x) = f(y)$, $f(x)f(x^{-1}) = f(y)f(x^{-1})$, so $e_H = f(e_G) = f(yx^{-1})$, so because $\ker(f) = \{e_G\}$, $yx^-1 = e_G$, so $y = x$, as desired. $\square$

Theorem 10. *Every group G of order n is isomorphic to a subgroup of S_n.*

Proof. It suffices to find an injective homomorphism from G to S_n. Because S_n is the set of bijections on a set of n elements, we can rephrase as $S_n = \mathrm{Sym}(G)$, or the set of bijections on the set G. For any $x \in G$, consider $f_x : G \to G, y \mapsto xy$. $f_x \in S_n$ because $f_x(y_1) = f_x(y_2)$ implies $xy_1 = xy_2$, so $y_1 = y_2$, and $f_x(x^{-1}y) = y$ for all $y_1, y_2, y \in G$. Now, $f_e(y) = y = \mathrm{Id}_G$, and $f_{x_1}f_{x_2}(y) = x_1x_2y = f_{x_1x_2}(y)$, so $f_{x_1}f_{x_2} = f_{x_1x_2}$.

So $f' : G \to S_n$ by $x \mapsto f_x$ is a group homomorphism. It's injective because if $f_x(y) = \mathrm{Id}$, then $xy = y$, then $x = e_G$, so $\ker(f') = \{e_G\}$. Thus, $G \cong \mathrm{Im}(f') \subseteq S_n$ $\square$

Let G be a group, $X \subset G$. And consider

$$\langle X \rangle = \bigcap_{H \text{ subgroup } G, X \subset H} H$$

We call $\langle X \rangle$ the subgroup of G generated by X. $X \subset \langle X \rangle$ by definition.

Proposition 26. *For $X \subset G$, $\langle X \rangle = \{x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} | x_i \in X, \epsilon = \pm 1, n \geq 0\}$.*

Proof. The righthand side(let's call it H)is a subgroup of G because the empty product yields e_G, the product of two elements in H is an element of H by concatenation, and the inverse of $x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$ is $x_n^{-\epsilon_n} \cdots x_1^{-\epsilon_1} \in H$, so H is a subgroup of G containing X, so $\langle X \rangle \subset H$.

By closure under multiplication and existence of inverses for $\langle X \rangle$, any $x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} \in H$ is also an element of $\langle X \rangle$, so $H \subset \langle X \rangle$, so $H = \langle X \rangle$, as desired. $\square$

Lecture 12

Cosets

Definition 20. *For $X, Y \subset G$, $X \cdot Y := \{xy \in G | x \in X, y \in Y\}$. If $X = \{x\}$, we can write $X \cdot Y$ as xY, and $Y \cdot X = Yx$.*

Set products are associative by associativity of G, $H \cdot H = H$ for any subgroup H because H is closed under group operation and contains identity.

Definition 21. *For $H \subset G$ subgroup, $x \in G$ the left coset of H is xH, the right coset is Hx*

Lemma 3. $xH = H \iff x \in H \iff Hx = H$

Proof. If $x \in H$, for any $h \in H$, we have $h = x(x^{-1}h) \in xH$. If $xh \in xH$, obviously $xh \in H$ by closure.

If $xH = H$, $x = xe \in xH = H$. □

Let $x \sim y$ if $y^{-1}x \in H$ for some subgroup $H \subset G$.
$x \sim x$ because $x^{-1}x = e \in H$.
If $y^{-1}x \in H$, then $x^{-1}y = (y^{-1}x)^{-1} \in H$, so $y \sim x$.
If $x \sim y$, $y \sim z$, $(z^{-1}y)(y^{-1}x) = z^{-1}x \in H$, so $x \sim z$.
So $\sim$ is an equivalence relation.

So the equivalence classes of G are $[x] = \{y \in G, x \sim y\} = xH$, so because equivalence classes are either equivalent or disjoint, any cosets xH, yH are either the same or disjoint.

Definition 22. *The index $[G : H]$ of H in G is the number of distinct left cosets xH for $x \in G$.*

Lemma 4. $|xH| = |H| = |Hx|$

Proof. If $xh_1 = xh_2$, then $h_1 = h_2$, so $f : H \to xH$ by $h \mapsto xh$ is a bijection. □

Theorem 11 (Lagrange's Theorem)**.** *Let G be a finite group, H a subgroup, then $|G| = |H|[G : H]$*

Proof. All the cosets of H have the same size $|H|$ and partition G; □

Corollary 6. $|H|$ *divides* $|G|$

Corollary 7. $\mathrm{ord}(x)$ *divides* $|G|$

Proof. $\mathrm{ord}(x) = |\langle x\rangle|$ divides G. □

For $(\mathbb{Z}/n\mathbb{Z})^\times$, $|G| = \phi(n)$, so $[a]^{\phi(n)} = [1]$, so $a^{\phi(n)} \equiv 1 \mod n$ when a is relatively prime with n.

When n is prime, we get

Theorem 12 (Fermat's Little Theorem)**.** $a^{p-1} \equiv 1 \mod p$ *when p doesn't divide a.*

Theorem 13. *Every group of order p is cyclic.*

Proof. $|G| = p > 1$, so there exists an element x whose order isn't 1, so $\mathrm{ord}(x) = |\langle x\rangle|$ which divides p, so $|\langle x\rangle| = p = |G|$, so $G = \langle x\rangle$ which is cyclic. □

Lecture 13

Normal Subgroups

Definition 23. *A subgroup $H \subset G$ is normal if $xH = Hx$ for all $x \in G$. We can write this as $H \trianglelefteq G$.*

Proposition 27. *A subgroup $H \subset G$ is normal $\iff$ $xhx^{-1} \in H$ for all $x \in G, h \in H$.*

Proof. If H is normal, $xH = Hx$, so $xHx^{-1} = Hxx^{-1} = He = H$, so $xHx^{-1} = H$, so $xhx^{-1} \in H$.

If $xhx^{-1} \in H$ for all $x \in G, h \in H$, $xh \in Hx$, so $xH \subset Hx$, and also $x^{-1}hx \in H$, so $hx \in xH$, so $Hx \subset xH$, so $xH = Hx$, as desired. □

Corollary 8. *Let $f : G \to H$ be a group homomorphism. Then* $\ker f \trianglelefteq G$.

Proof. If $y \in \ker f$, $x \in G$, then $f(xyx^{-1}) = f(x)f(y)f(x^{-1}) = f(x)f(x^{-1}) = e$, so $xyx^{-1} \in \ker f$. □

Key property of normal subgroups. If $H \trianglelefteq G$, then $(xH)(yH) = x(Hy)(H) = x(yH)H = xy(HH) = (xy)H$. Then consider G/H, the set of all cosets of H.

Proposition 28. *G/H, the cosets of $H \trianglelefteq G$, is a group with operation of coset multiplication.*

Proof. $(xH \cdot yH)zH = (xyH)zH = (xy)zH = x(yz)H = xH(yzH) = xH(yH \cdot zH)$

$xH \cdot eH = xHH = xH$

$xH \cdot x^{-1}H = eH = H$

So G/H is associative, has inverse, and has identity, so G/H is a group. □

Definition 24. *G/H is called the quotient group of G modulo H where $H \trianglelefteq G$.*

Definition 25. *For $H \trianglelefteq G$, we can define $\pi : G \to G/H$ by $\pi(x) = xH$.*

By earlier, we know that $\pi(xy) = xyH = xHyH = \pi(x)\pi(y)$, so π is a canonical group homo from G to G/H. $\mathrm{Im}\pi = G/H$, $\ker \pi = H$. So any normal subgroup H is the kernel of some group homo.

Lecture 14

Consider the group homos $f : G \to H$, and $\pi : G \to G/N$ for $N \trianglelefteq G$. Then we want to find a group homo $\bar{f} : G/N \to H$ such that $f = \bar{f} \circ \pi$. Then if such an $\bar{f}$ exists, for all $n \in N$, $\bar{f}(\pi(n)) = \bar{f}(e_{G/N}) = e_H$, so $N \subset \ker f$. Conversely, if $N \subset \ker f$, we claim that $\bar{f}$ exists and is unique. Obviously, if $\bar{f}$ exists, then it's unique because $\bar{f}(xN) = f(x)$ for all $x \in G$. Now, let's try to define $\bar{f}$ by $xN \mapsto f(x)$. Suppose $xN = yN$. Then $x = yn$ for some $n \in N$, so $f(x) = f(y)f(n) = f(y)(e) = f(y)$ because $N \subset \ker f$, so $\bar{f}(xN) = \bar{f}(yN)$, so

$\bar{f}$ is well defined. $\bar{f}$ is a group homo because $\bar{f}(xNyN) = \bar{f}(xyN) = f(xy) = f(x)f(y) = \bar{f}(xN)\bar{f}(yN)$ for all $x, y \in G$. In summary,

Theorem 14 (Universal Property of the quotient group)**.** *Let $N \trianglelefteq G$ and $f : G \to H$ a group homomorphism, and $\pi : G \to G/N$ the projection mapping. Then there exists a homomorphism $\bar{f} : G/N \to H$ such that $f = \bar{f} \circ \pi$ if and only if $N \subset \ker f$. Furthermore, $\bar{f}$ is unique when this condition is satisfied.*

Isomorphism Theorems

Let $f : G \to H$ be a group homo, $N = \ker f \trianglelefteq G$. Then by the theorem, there exists $\bar{f} : G/N \to H$ such that $\bar{f}(xN) = f(x)$, so $\mathrm{Im}(\bar{f}) = \mathrm{Im}(f)$.

Theorem 15 (First Isomorphism Theorem)**.** *Let $f : G \to H$ be a group homomorphism. Then the unique group homomorphism $\bar{f} : G/\ker f \to \mathrm{Im}(f)$ such that $\bar{f} \circ \pi = f$ is an isomorphism. Note that $\pi : G \to G/N$ is the projection mapping.*

Proof. Let $N = \ker f$. Then $\mathrm{Im}(\bar{f}) = \mathrm{Im}(f)$, so $\bar{f}$ is surjective. If $xN \in \ker(\bar{f})$, then $x \in \ker(f)$, so $x \in N$, so $xN = N$. Thus, $\ker(\bar{f}) = \{N\} = \{e_{G/N}\}$, so $\bar{f}$ is injective. Thus, $\bar{f}$ is bijective hence an isomorphism. □

We use this result in lecture to show $\mathbb{C}/\mathbb{R} \cong \mathbb{R}, C^{\times}/U = \mathbb{R}^{>0}$, where U is the complex unit circle, not too bad.

Here's another proof of an earlier theorem of cyclic groups.

Theorem 16. *If G is a cyclic group of order n, then $G \cong \mathbb{Z}/n\mathbb{Z}$.*

Proof. Let $x \in G$ be a generator of G. THen define $f : \mathbb{Z} \to G$ by $f(a) = x^a$. Then $f(a+b) = x^{a+b} = x^a x^b = f(a)f(b)$, so f is a group homomorphism. f is surjective by definition of a generator. And $\ker(f) = n\mathbb{Z}$ because $x^a = e \iff n|a$, since x has order n. □

Theorem 17 (Second Isomorphism Theorem)**.** *Let K, N be subgroups of G, and $N \trianglelefteq G$. Then KN is a subgroup of G such that $N \trianglelefteq KN$, $K \bigcap N \trianglelefteq K$, and $KN/N \cong K/(K \bigcap N)$.*

Proof. $e \in KN$ because $e \in K, N$. And $(k_1n_1)(k_2n_2) = (k_1k_2)(k_2^{-1}n_1k_2n_2)$. Then $k_1k_2 \in K$, $k_2^{-1}n_1k_2 \in N$, and $n_2 \in N$, so $(k_1n_1)(k_2n_2) \in KN$. And $(kn)^{-1} = n^{-1}k^{-1} = k^{-1}(kn^{-1}k^{-1}) \in KN$. So KN is a subgroup. Obviously $N \subset KN$ because $e \in K$. For all $kn_1 \in KN, n_2 \in N$, $kn_1n_2n_1^{-1}k^{-1} = (kn_1n_2k^{-1})(kn_1^{-1}k^{-1})$, which is the product of two elements in N, so $N \trianglelefteq KN$ because $N \trianglelefteq G$.

Consider $f : K \to KN/N$ by $f(k) = kN$. f is clearly surjective because $(kn)N = kN$, and $k \in \ker(f) \iff kN = N \iff k \in K \bigcap N$, so by the first isomorphism theorem, we have $K/(K \bigcap N) \cong KN/N$. Also, because $K \bigcap N = \ker f$, we have that $K \bigcap N \trianglelefteq K$ because $\ker f \trianglelefteq K$. □

Lecture 15

Theorem 18 (Third Isomorphism Theorem)**.** *Let $K \subseteq H \subseteq G$ where K, H are subgroups of G, such that $K, H \trianglelefteq G$. Then $H/K \trianglelefteq G/K$, and $(G/K)/(H/K) \cong G/H$.*

Proof. Consider $f : G/K \to G/H$ by $f(xK) = xH$. This is well-defined because $xK = yK \iff x^{-1}y \in K \implies x^{-1}y \in H \iff xH = yH$. It's a group homo because $f(xKyK) = f(xyK) = xyH = xHyH = f(xK)f(yK)$. Then $xK \in \ker f \iff f(xK) = H \iff xH = H \iff x \in H$, so $\ker f = H/K$, and $\mathrm{Im} f = G/H$, so by the First Isomorphism Theorem, $(G/K)/(H/K) \cong G/H$. $\square$

Ex. If we have $nm\mathbb{Z} \subseteq n\mathbb{Z} \subseteq \mathbb{Z}$, we have $(\mathbb{Z}/nm\mathbb{Z})/(n\mathbb{Z}/nm\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$

Automorphism group

Definition 26. *Let G be a group. Then an endomorphism of G is a group homomorphism $f : G \to G$, and an automorphism of G is a group isomorphism $f : G \to G$.*

Definition 27. *Let $\mathrm{Aut}(G)$ be the group whose elements are all the automorphisms on G, and whose group operation is $f_1 \cdot f_2 = f_1 \circ f_2$.*

Function composition is associative, $\mathrm{Id} \in \mathrm{Aut}(G)$, and $\mathrm{Id} \circ f = f \circ \mathrm{Id} = f$, and the inverse of an iso is an iso, so $\mathrm{Aut}(G)$ is indeed a group.

Let $f_a : G \to G$ by $f_a(x) = axa^{-1}$. Then $f_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = f_a(x)f(y)$, $f_af_b(x) = abxb^{-1}a^{-a} = f_{ab}(x)$, and $(f_a)^{-1} = f_{a^{-1}}$.

f_a, conjugating all elements of G by a, is called an inner automorphism by a. Note that $\mathrm{ord}(x) = \mathrm{ord}(f_a(x))$ because $(axa^{-1})^n = ax^na^{-1}$.

Fact:$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

Let $G \cong H$. Then consider the map $\alpha : \mathrm{Iso}(G, H) \to \mathrm{Aut}(G)$ by $f \mapsto f_0 \circ f$, where f_0 is some pre-chosen iso $H \to G$. Then this is clearly a bijection, so $|\mathrm{Iso}(G, H)| = |\mathrm{Aut}(G)|$

Consider $G = GL_n(\mathbb{R})$. Then consider $f \in \mathrm{Aut}(G)$, $f(x) = (x^T)^{-1} = (x^{-1})^T$. Then f is not an inner automorphism if $n > 2$, and it is if $n = 2$(left as exercise).

Consider $f : G \to \mathrm{Aut}(G)$ by $a \mapsto f_a$. Then $\ker f = \{a \in G | ax = xa \forall x \in G\}$. This is called the center of G, or $Z(G)$. So $Z(G) \trianglelefteq G$. And $\mathrm{Im} f = \mathrm{Inn}(G)$, the group of inner automorphisms on G. So $G/Z(G) \cong \mathrm{Inn}(G)$.

Proposition 29. $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$

Proof. Let $h \in \mathrm{Aut}(G), f_a \in \mathrm{Inn}(G)$. Then $(h \circ f_a \circ h^{-1})(x) = h(ah^{-1}(x)a^{-1}) = h(a)xh(a^{-1}) = h(a)x(h(a))^{-1}$, so this composition is $f_{h(a)} \in \mathrm{Inn}(G)$, so $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$ as desired. $\square$

Definition 28. $\mathrm{Aut}(G)/\mathrm{Inn}(G) = \mathrm{Out}(G)$*, the group of outer automorphisms.*

If G is abelian, $\mathrm{Inn}(G) = \{\mathrm{Id}\}$, so $\mathrm{Aut}(G) \cong \mathrm{Out}(G)$.

$\mathrm{Out}(GL_n(\mathbb{R}))$ is cyclic of order 2 if $n > 2$.

S_2 has trivial outer automorphism group, S_n has trivial outer automorphism group except when $n = 6$.

Lecture 16

Basic stuff with symmetric groups, conjugation maps disjoint union of $m_1, \cdots, m_k$ cycles to disjoint union of $m_1, \cdots, m_k$ cycles, all such unions are in same conjugacy class, types on S_n, $\{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \trianglelefteq S_4$.

Lecture 17

Definition 29. *Let $\sigma \in S_n$ Then $A(\sigma)$ is defined by $A(\sigma)_{ij} = 1$ if $\sigma(j) = i$, and 0 otherwise.*

We claim that $A(\sigma\tau)_{ij} = \sum_{k=1}^{n} A(\sigma)_{ik} A(\tau)_{kj}$ because $\tau(j) = q$ for exactly one value of q, so $\sigma\tau(j) = i \iff \sigma(q) = i \iff A_{iq} = 1 \iff \sum_{k=1}^{n} A(\sigma)_{ik} A(\tau)_{kj} = 1$ because $A(\tau)_{kj} = 0$ for all $k \neq q$.

Definition 30. *We define the alternating group A_n as the kernel of* $\mathrm{sgn} = \det(A) \subseteq \{-1, 1\}$

$A_1 = \{e\}$, $A_2 = \{e\}$, $A_3 = \{e, (123), (132)\}$,
$N = \{e, (12)(34), (13)(24), (14)(23)\} \trianglelefteq A_4 = N \bigcup \{\sigma \in S_n | \sigma \text{ is a 3-cycle.}\}$

Definition 31. *We say a permutation $\sigma \in S_n$ is even if $\sigma \in A_n$, and σ is odd otherwise.*

Proposition 30. *Every $\sigma \in S_n$ is a product of transposition.*

Proof. For every cycle $(1, 2, \cdots, k)$, we can write the cycle as k transpositions $(1,2)(2,3) \cdots (k-1,k)$ □

Because each transposition has sign -1, σ is even if it's the product of an even number of transpositions, and σ is odd if it's composed of an odd number of transpositions.

Corollary 9. *S_n is generated by transpositions.*

Proof. We know from the proposition that any element of S_n is the product of transpositions. □

Corollary 10. *A_n is generated by the products of 2 transpositions.*

Proof. Each permutation of 2 transpositions is clearly in A_n, so we can break down the $2n$ transpositions in A_n into a product of n permutations of 2 transpositions □

Proposition 31. *A_n is generated by 3-cycles.*

Proof. It suffices to show $(ij)(kl)$ is the product of 3-cycles. If the transpositions have 1 symbol in common, WLOG, $(ij)(kl) = (ij)(jl) = (ijl)$. If the transpositions have 2 symbols in common, $(i,j)(i,j) = e$. If the transpositions have no symbols in common, $(ij)(kl) = (ij)(jk)(jk)(kl) = (ijk)(jkl)$, so we're done. $\square$

Definition 32. *A group G is simple if $G \neq \{e\}$, and G has no normal subgroup other than $\{e\}, G$.*

Ex. $\mathbb{Z}/p\mathbb{Z}$ is simple because there are no nontrivial subgroups, $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ is simple. A_4 isn't normal though because the identity with products of 2 transpositions form a normal subgroup of A_4.

Theorem 19. *For $n \geq 5$, A_n is simple.*

Proof. Suppose $N \neq \{e\}, N \trianglelefteq A_n$. Let $e \neq \sigma \in N$. Then either σ is a 3-cycle, or σ moves at least 4 symbols. We can write $\sigma = \sigma_1 \cdots \sigma_s$ of disjoint cycles. (Case 1)If there's at least one σ_i of length $k \geq 4$, then $\sigma = (1, 2, \cdots, k)\tau$ for some $\tau \in S_n$.

Note that $\sigma(123)\sigma^{-1}(132) \in N$, but $\sigma(123)\sigma^{-1}(132) = (234)(132) = (142)$, so N contains a 3-cycle in this case.

If all cycles in σ are of length at most 3(Case 2), then if the length of σ_i is 3 for at least two values of i(Case 2a), $\sigma = (123)(456)\tau$, so $\sigma(124)\sigma^{-1}(142) \in N$, but $\sigma(124)\sigma^{-1}(142) = (235)(142) = (14352) \in N$, contradiction of N having no cycles of length 4 or more.

If there is exactly one 3-cycle in σ(Case 2b), then $\sigma = (123)\tau = \tau(123)$, where τ is disjoint with (123), and τ is the product of disjoint transpositions. Then $\sigma^2 = (123)\tau(123)\tau = (123)^2\tau^2 = (123)^2 = (132) \in N$, so N contains a 3-cycle.

Otherwise(Case 2c), all σ_i are transpositions, so $\sigma = (12)(34)\tau$, so $\sigma(123)\sigma^{-1}(123)^{-1} = (214)(132) = (13)(24) \in N$. Let $\pi = (13)(24)$. Then $(135) = (315)(153) = \pi(135)\pi^{-1}(153) \in N$, so N contains a 3-cycle.

Thus, N always contains a 3-cycle, hence all 3-cycles because all 3-cycles are conjugate to each other, and N is normal. Indeed, if we have that $(123) \in N$, then for any other 3-cycle (abc), we have that N contains $(1a)(2b)(3c)(45)(123)(45)(3c)(2b)(1a) = (1a)(2b)(3c)(123)(3c)(2b)(1a) = (abc)$.

Because A_n is generated by 3-cycles, this implies that $N = A_n$, so we're done and A_n has no normal subgroups other than the trivial subgroup and itself, so A_n is simple for $n \geq 5$. $\square$

Lecture 18

Group Actions

Definition 33. *Let G be a group and X a set. Then G acts on X if there is a map(called a group action) $G \times X \to X$ by $(a, x) \mapsto ax$ such that $ex = x$ for all*

$x \in X$, and $a(bx) = ab(x)$ for all $a, b \in G, x \in X$.

Examples:

- The trivial action of G on x is given by $ax = x$ for all $x \in X, a \in G$.
- Let $G = S(X)$, the group of all bijections on X. Then $\sigma x = \sigma(x)$ is a group action, since $\mathrm{Id}x = \mathrm{Id}(x) = x$, and $(f_1 \circ f_2)x = f_1(f_2(x)) = f_1(f_2 x)$.
- A group G acts on $X = G$ by $a * x$ as a group action is ax as the group operation.
- A group G acts on $X = G$ by $a * x = axa^{-1}$ since $e * x = exe^{-1} = x$, and $a * (b * x) = a(bxb^{-1})a^{-1} = ab(x)(ab)^{-1} = ab * (x)$.
- Let $H \subset G$ a subgroup. Let $X = G/H$, the set of left cosets of H in G. Then G acts on X by $a * (bH) = (ab)H$, since $e * (bH) = (eb)H = bH$, and $xy * (bH) = (xy)bH = x(ybH) = x * (y * bH)$.
- Let G act on X, and $H \subset G$ a subgroup. Then restricting $* : G \times X \to X$ to $\cdot : H \times X \to X$, we get a group action of H on X by $h \cdot x = h * x$, since $e_G \in H$ and $h_1 \cdot (h_2 \cdot x) = h_1 * (h_2 * x) = (h_1 h_2) * x = (h_1 h_2) \cdot x$.
- Let $f : H \to G$ be a group homo, and G acts on X by $*$. Then H acts on X by $h \cdot x = f(h) * x$, since $e_H \cdot x = f(e_H) * x = e_G * x = x$, and $(h_1 h_2) \cdot x = f(h_1 h_2) * x = f(h_1) * (f(h_2) * x) = h_1 \cdot (h_2 \cdot x)$.

Let G be a group, and X a set. Let G' be the set of all G-actions on X. Then we have a a bijective correspondence between $G', \mathrm{Hom}(G, S(X))$ by $* \mapsto h : G \to S(X)$ by $h(g)(x) = g * x$ for all $x \in X$. These are group homos because $f(g_1 g_2)(x) = (g_1 g_2) * x = g_1 * (g_2 * x) = f(g_1) \circ f(g_2)(x)$, so h is a homo.

Lecture 19

Definition 34. *A G-action $*$ on X is **faithful** if the map $f : G \to S(X)$ by $f(g) = f_g : X \to X, x \mapsto g * x$ is injective.*

That is, for all $g_1, g_2 \in G$, there exists $x \in X$ such that $g_1 * x \neq g_2 * x$, or equivalently, $g_1 * x = x$ for all $x \in X$ implies $g_1 = e$.

Suppose G acts on $X = G$ by conjugation. Then $f : G \to S(X)$ has kernel $\{g \in G | gxg^{-1} = x \forall x \in G\} = Z(G)$, so G is faithful $\iff$ G has no commuting elements. Also, $\mathrm{Im} f = \mathrm{Inn}(G \subseteq \mathrm{Aut}(G) \subseteq S(G)$

Let G act on X. Then let $x \sim x'$ if $x' = gx$ for some $g \in G$.

Then $\sim$ is an equivalence relation since $x = e * x$(reflexive), $x' = g * x \implies x = g^{-1} * x$(symmetric), $a = g_1 * b, b = g_2 * c \implies a = (g_1 * g_2)c$(transitive).

Definition 35. *The equivalence classes of X under $\sim$ are called the **orbits** of X, or $[x]_\sim = \mathcal{O}(x)$.*

Definition 36. *A group action G on X is **transitive** if X has only one orbit.*

For $x \in X$, $G(x) := \{g \in G : g * x = x\} \subseteq G$ is a subgroup, since $e * x = x$, and $a*x = x$ implies $x = a^{-1}*x$, or $a^{-1} \in G(x)$, and $a*x = x, b*x = x$ implies $(ab)*x = a*(b*x) = a*x = x$, so $ab \in G(x)$.

Definition 37. *If G acts on X, for any $x \in X$, the subgroup $G(x) := \{g \in G : g * x = x\} \subseteq G$ is called the* ***stabilizer*** *of x.*

If $G = S_n$ acts on $X = \{1, 2, \cdots, n\}$, then $G(n) \cong S_{n-1}$, and the action is transitive.

If G acts on G by left translation, the action is transitive since $g_1 = (g_1 g_2^{-1}) * g_2$ for all $g_1, g_2 \in G$. $G(x) = \{g \in G | gx = x\} = \{e\}$, so stabilizers are trivial.

Definition 38. *G acts on X* ***simply transitively*** *if the action is transitive and $G(x) = \{e\} \forall x \in X$*

If G acts on itself by conjugation, the $\mathcal{O}(x) = \{gxg^{-1} | g \in G\}$, the conjugacy class of x. $G(x) = \{g \in G | gxg^{-1} = x\}$, the centralizer of x, $C_G(x)$.

Let $H \subseteq G$ a subgroup, $X = G/H$ the left cosets of H. Then let G acts on X by left translation. Then $g'H = (g'g^{-1})gH$, so the action is transitive. The stabilizer $G(H) = H$.

Let G a group, X the set of subgorups of G. Then G acts on X by conjugation, since conjugation is a homomorphism, so the image of H under conjugation is indeed a subgroup. Then $\mathcal{O}(H) = \{gHg^{-1} | g \in G\}$, and $G(H) = \{g \in G | gHg^{-1} = H\} := N_G(H)$, the normalizer of H in G. Obviously, $H \trianglelefteq N_G(H)$ and any $H' \subseteq G$ such that $H \trianglelefteq H'$ has that $H' \subseteq N_G(H)$.

Recall that any element $\sigma \in S_n$ is the product of disjoint cycles $\sigma_1 \sigma_2 \cdots$. Consider $H = \{\langle \sigma \rangle \subseteq S_n$.

Then H acts on $\{1, 2, \cdots, n\}$, and $\mathcal{O}(a_i) = b_i$, where a_i, b_i are in some cycle σ_i, since an element is in exactly one disjoint cycle under a permutation.

Theorem 20 (Orbit-Stabilizer Theorem)**.** *Let G act on X, $x \in X$. Then $|\mathcal{O}(x)| = [G : G(x)]$*

Proof. We construct a map $f : G/G(x) \to X$ by $f(gG(x)) = gx$. This is well-defined since if $gG(x) = g'G(x)$, then $g^{-1}g' \in G(x)$, so $f(gG(x)) = f(gg^{-1}g'G(x)) = g'x = f(g'G(x))$.

If $gx = g'x$, then $g^{-1}g' \in G(x)$, so $gG(x) = gg^{-1}g'G(x) = g'G(x)$, so f is injective.

Since $\mathrm{Im}(f) = \mathcal{O}(x)$, we have that $f : G/G(x) \to \mathcal{O}(x)$ is a bijection, so $[G : G(x)] = |G/G(x)| = |\mathcal{O}(x)|$. □

Lecture 20

Proposition 32. *Let G be a finite group, and p the smallest prime divisor of $|G|$. If $H \subseteq G$ is a subgroup of index p, then $H \triangleleft G$.*

Proof. Let G act on G/H by $g * xH = gxH$. Then we have $f : G \to S(G/H) = S_p$, and $N = \ker f \triangleleft G$.

We claim that $N \subseteq H$. Indeed, if $g \in N$, $f(g)aH = gaH$ for all $a \in G$. If $a = e$, this implies that $H = gH$, so $g \in H$.

Also, by the first Isomorphism Theorem, $G/N \cong \mathrm{Im} f \subseteq S_p$. So $[G : N]||S_p| = p!$. Also, $[G : N] = \frac{|G|}{|N|}$, so $[G : N]||G|$.

Thus, $[G : N]| \gcd(p!, |G|) = p$, so $|N| \geq \frac{|G|}{p} = |H|$, so because $N \subseteq H$, we must have that $N = H$, so $H = N \lhd G$. $\square$

Sylow's Theorems

Definition 39. *Let p be prime. Then a group G is a p-group if $|G| = p^s$ for some $s > 0$.*

By Lagrange's theorem, if G is a p-group, then a subgroup $H \subseteq G$ is also either a p-group or the trivial group because $|H|||G| = p^s$.

Definition 40. *If G acts on X, let $X^G = \{x \in X | \forall g \in G, gx = x\}$.*

Lemma 5. *If G is a p-group, then $|X^G| \equiv |X| (\mod p)$ if X is finite.*

Proof. $X = \bigcup_{i=1}^N \mathcal{O}_i$ a disjoint union of orbits. Then let $\mathcal{O}_i = [x_i]$, where $[x_i] \in X$. Suppose the first m orbits have that $\mathcal{O}_i$ is a singleton, and the other orbits are larger. Then $|X| = \sum_{i=1}^n |\mathcal{O}_i| = m + \sum_{i=m+1}^n |\mathcal{O}_i|$. Note that for $i > m$, $|\mathcal{O}_i| = [G : H_i] = \frac{p^s}{p^t} \neq 1$, where $H_i = \mathrm{Stab}(x_i) \subseteq G$, so $p|[G : H_i] = |\mathcal{O}_i|$. Thus, $|X^G| = m \equiv m + \sum_{i=m+1}^n |\mathcal{O}_i| = |X| (\mod p)$. $\square$

Theorem 21 (Cauchy)**.** *Let p be a prime divisor of the order of a group G. Then G has an element of order p.*

Proof. Let $X = \{(a_1, a_2, \cdots, a_p) | a_i \in G, a_1 a_2 \cdots a_p = e\} \subseteq G^p$. Then pretty clearly $|X| = |G|^{p-1}$ since we get one element of X for any choice of the first $p - 1$ a_i. So p divides $|X|$

Also, a permutation σ on an element $a \in X$ has that $\sigma(a) \in X$.

Let H be a cyclic group of order p with $\sigma \in H$ as a generator. Let H act on X by $\sigma(a_1, \cdots, a_p) = (a_p, a_1, \cdots, a_{p-1})$. Then $|X^H| \equiv |X| \equiv 0 \mod p$, so $p||X^H|$. Note that $(e, e, \cdots, e) \in \{(a, a, \cdots, a) | a^p = e\} = X^H$, so $|X^H| \neq 0$. Thus, $|X^H| \geq p > 1$, so there exists $e \neq a \in G$ such that $a^p = 1$, so by Lagrange's Theorem, we must have that $\mathrm{ord}(a) = 1$. $\square$

Proposition 33. *The center of a p-group is nontrivial.*

Proof. Let G act on $X = G$ by conjugation. Then $X^G = Z(G)$. So by the earlier lemma, $|Z(G)| \equiv |G| \equiv 0 \mod p$, so because $|Z(G)| \geq 1$, we must have that $|Z(G)| > 1$. $\square$

Definition 41. *A subgroup $H \subseteq G$ is called a p-subgroup if H is a p-group.*

Lemma 6. *Let H be a p-subgroup of G. Then $[N_G(H) : H] \equiv [G : H] \mod p$*

Proof. Let $X = G/H$, and let H act on X by left translations.

Then $a \in X^H \iff haH = ah \forall h \in H \iff a^{-1}haH = H \forall h \in H \iff a^{-1}ha \in H \forall h \in H \iff H = aHa^{-1} \iff a \in N_G(H)$.

So $X^H = \{aH | a \in N_G(H)\} = N_G(H)/H$, so $[N_G(H) : H] = |X^H| \equiv |X| = [G : H] (\mod p)$, as desired. ☐

Lecture 20

Theorem 22 (Sylow Theorem 1)**.** *Let G be a finite group and p a prime dividing $|G|$. Write $|G| = p^n m$, where $\gcd(m, p) = 1$. Then*

- *Every subgroup $H \subseteq G$ of order p^k for $k = 0, 1, \cdots, n-1$, is contained in a subgroup of order p^{k+1}*
- *G has subgroups of order p^k for all $k = 0, 1, \cdots, n$.*

Proof. The first claim implies the second, since starting with the trivial group H_0, which is contained in a subgroup H_1 of order p, etc. until $k = n-1$, and H_{n-1} is contained within a subgroup H_n of order p^n. So it suffices to show the first claim.

So if H is a p-group, by Lemma 6, $[N_G(H) : H] \equiv [G : H] \mod p$, but $[G : H] = \frac{p^n m}{p^k} = p^{n-k} m$ is divisible by p, so $[N_G(H) : H]$ is divisible by p. Thus, Theorem 21 implies that there exists a subgroup $F \subseteq N_G(H)/H$ of order p. Let $\pi : N_G(H) \to N_G(H)/H$ be the projection map, and let $\pi' : H' = \pi^{-1}(F) \to F$ be π restricted to $\pi^{-1}(F)$. We claim $H = \ker \pi = \ker \pi'$. Clearly $\ker \pi' \subseteq \ker \pi$. Conversely, $\ker \pi = \pi^{-1}(e) \subseteq \pi^{-1}(F) = H'$, so every element in $\ker \pi$ must also be in $\ker \pi' = \ker \pi \bigcap H'$, so $\ker \pi = \ker \pi'$. Note that $H \lhd H'$, so by the First Isomorphism Theorem on π', $H'/H \cong F$, so $p = |F| = [H' : H] = \frac{|H'|}{|H|}$, so $|H'| = p|H| = p^{k+1}$, as desired. ☐

Definition 42. *If $|G| = p^n m$, where $n > 0, \gcd(m, p) = 1$, a subgroup $P \subseteq G$ is a Sylow p-subgroup if $|P| = p^n$.*

Note that by Sylow Theorem 1, there exists a subgroup of order p^n, and also all conjugate subgroups aPa^{-1} for $a \in G$ are Sylow p-subgroups.

Theorem 23 (Sylow Theorem 2)**.** *Let G be a finite group and p a prime divisor of $|G|$ such that $|G| = p^n m, \gcd(p^n, m) = 1$. Then*

- *If $H \subseteq G$ is a p-subgroup and $P \subseteq G$ is a Sylow p-subgroup, then $H \subseteq aPa^{-1}$ for some $a \in G$.*
- *Every two Sylow p-subgroups of G are conjugate.*

Proof. Let $X = G/P$. Then H acts on X by left translations. By Lemma 5, $|X^H| \equiv |X| \mod p$, so $|X^H| \equiv [G : P] = m \not\equiv 0 \mod p$, so $|X^H| \neq 0$, so $X^H \neq \emptyset$.

Thus, there exists $aP \in X^H$ such that for all $h \in H$ $haP = aP \iff a^{-1}ha = P \iff a^{-1}ha \in P \iff a^{-1}Ha \subseteq P \iff H \subseteq aPa^{-1}$, yielding the first claim.

Applying the first claim to some Sylow p-subgroup $P' \subseteq G$, by the first claim, we have that $P' \subseteq aPa^{-1}$, so since they're the same finite size, $P' = aPa^{-1}$. $\square$

Corollary 11. *If $P \subseteq G$ is a Sylow p-subgroup, then $P \lhd G \iff N_p(G) = 1$, where $N_p(G)$ is the number of Sylow p-subgroups.*

Proof. If $P \lhd G$, then any Sylow p-subgroup is $P' = aPa^{-1} = P$ because P is normal, so P is the only Sylow p-subgroup, so $N_p(G) = 1$. $\square$

Theorem 24 (Sylow Theorem 3)**.** *Let G be a finite group such that $|G| = p^n m$, $n > 0, \gcd(m, p) = 1$. Then*

- $N_p(G)|m$
- $N_p(G) \equiv 1 \mod p$

Proof. Let X be the set of Sylow p-subgroups of G. Then if P is a Sylow p-subgroup, P acts on X by conjugation. Then by Lemma 5, $|X^P| \equiv |X| = N_p(G)$ mod p.

We claim that $X^P = \{P\}$. Let $Q \subseteq G$ be a Sylow p-subgroup. Then $Q \in X^P \iff aQa^{-1} = Q \forall a \in P \implies P \subseteq N_G(Q) \rhd Q$, so P, Q are Sylow p-subgroups of $N_G(Q)$. So by corollary 11, since $Q \lhd N_G(Q)$, we have $N_p(N_G(Q)) = 1$, so we must have that $P = Q$. Thus, $N_p(G) = |X| \equiv |X^P| = 1$ mod p, giving the second claim.

Notice that G acts on X by conjugation transitively, since all Sylow p-subgroups are conjugate. So $N_p(G) = |\mathcal{O}(P)| = [G : G_P] = [G : N_G(P)]$, so since $P \subseteq N_G(P)$, $N_p(G) = [G : N_G(P)]$ divides $[G : P] = \frac{|G|}{|P|} = m$, as desired. $\square$

Proposition 34. *G is a simple abelian group if and only if $G \cong \mathbb{Z}/p\mathbb{Z}$ for a prime p.*

Proof. If G is abelian simple, then for all primes p dividing $|G|$, Cauchy implies that there's an $a \in G$ of order p, so because G is abelian, $\langle a \rangle \lhd G$, so we must have that $\langle a \rangle = G$, so $G \cong \mathbb{Z}/p\mathbb{Z}$.

The other direction is obvious. $\square$

4 Lecture 21

Just showing that all simple groups of order less than 60 are prime cyclic. Using facts that group of order pq aren't simple, groups of order $4p$ aren't simple, groups of order $2p^n$ aren't simple, 3rd Sylow Theorem

5 Lecture 22

Let $K, H \subseteq G$ be subgroups, where $K, H \lhd G$, $K \bigcap H = \{e\}$, and $KH = G = G^{-1} = (KH)^{-1} = H^{-1}K^{-1} = HK$. If G is finite, the last condition can be replaced by $|G| = |H||K|$. If these conditions are satisfied, we say $G = H \times K$ is the internal product of H and K.

Note that $kh = hk$ since $khk^{-1}h^{-1} = (khk^{-1}) \in H$ and $khk^{-1}h^{-1} = k(hk^{-1}h^{-1}) \in K$.

Then $f : H \times K \to G$ by $f(h, k) = hk$ is a bijection since the sceond condition on H, K implies injectivity, and the third implies surjectivity.

Furthermore, f is a homomorphism since $f((h_1, k_1)(h_2, k_2)) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = f(h_1, k_1)f(h_2, k_2)$.

If G_1, G_2 are groups, then $G = G_1 \times G_2$, then $H = G_1 \times e_2$, $K = e_1 \times G_2$ satisfy the conditions on the internal product in G, so we have the internal product $G = H \times K$, where $H \cong G_1, K \cong G_2$, so we can get a bijection between external products and internal products by mapping the external product $G_1 \times G_2$ to the internal product $(G_1 \times e_2) \times (e_1 \times G_2)$ and mapping the internal product $H \times K$ to the external product $H \times K$.

Obviously, if $G = HK$ is an internal product, then $G \cong H \times K$ by $hk \mapsto (h, k)$ which is well defined since each element of G can be written uniquely as hk.

Examples: $\mathbb{C} = \mathbb{R} \oplus \mathbb{R}_i \cong \mathbb{R} \times \mathbb{R}$
$\mathbb{C}^\times = U \oplus R^{>0} \cong U \times R^{>0}$
$\mathbb{Z}/6\mathbb{Z} = 3\mathbb{Z}/6\mathbb{Z} \oplus 2\mathbb{Z}/6\mathbb{Z} \cong 3\mathbb{Z}/6\mathbb{Z} \times 2\mathbb{Z}/6\mathbb{Z}$

Definition 43. *If $H \lhd G$, $K \bigcap H = \{e\}, HK = G$, then G is the internal semidirect product of H and K, or $G = H \rtimes K$*

The second and third conditions imply that $f : H \times K \to G$, $f(h, k) = hk$ is a bijection.

Note that $(h_1k_1)(h_2k_2) = h_1(k_1h_2k^{-1})k_1k_2 \in HK$. Also, since H is normal, we have for all $k \in K$ the automorphism $\alpha_k : H \to H$ by $\alpha_k(h) = khk^{-1}$. Since $\alpha_{k_1}\alpha_{k_2} = \alpha_{k_1k_2}$, we have a homomorphism $\alpha : K \to \mathrm{Aut}(H)$.

Definition 44. *Let K, H be groups with a homo $\alpha : K \to \mathrm{Aut}(H)$. Then let $G = H \times K$ as sets. Then define an operation on G by $(h_1, k_1)(h_2, k_2) = (h_1\alpha(k_1)(h_2), k_1k_2)$. This operation makes G a group, and G is the external semidirect product of H and K with respect to α.*

The internal and external semidirect products are isomorphic, since if $G = H \rtimes K$ is the internal product, then we can map hk to (h, k) bijectively with $\alpha(k)(h) = khk^{-1}$, and we can write the external product as the inner product $H_1 \rtimes K_1$ by $H_1 = H \times e_K \cong H$, $K_1 = e \times K \cong K$, and $H_1 \lhd H_1 \rtimes K_1$, and obviously H_1, K_1 have trivial intersection.

Ex. $S_3 = \langle\sigma\rangle \rtimes \langle\tau\rangle \cong (\mathbb{Z}/3\mathbb{Z}) \rtimes (\mathbb{Z}/2\mathbb{Z})$

$N = \{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\} \lhd S_4$, and $K = S_3 \subseteq S_4$, then $S_4 = N \rtimes K$.

Let p, q prime, $q \equiv 1 \mod p$. Then consider a nontrivial $\alpha : K = \mathbb{Z}/p\mathbb{Z} \to H = \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong (\mathbb{Z}/q\mathbb{Z})^{\times}$. Then $G = \mathbb{Z}/q\mathbb{Z} \rtimes_{\alpha} \mathbb{Z}/p\mathbb{Z}$ is not abelian and is of order pq.

Lecture 23

If $|G| = pq$, $q \not\equiv 1$, then G has exactly one normal Sylow p-subgroup P and one normal Sylow q-subgroup Q with trivial intersection since they're cyclic, so we have the internal product $G = P \times Q \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$. Thus, the only isomorphism class of groups of order 15 is $\mathbb{Z}/15\mathbb{Z}$.

For $n \geq 1$, let $C_n = \{e, \sigma, \sigma^2, \cdots, \sigma^{n-1}\}, C_2 = \{e, \tau\}$ where $\sigma^n = e, \tau^2 = e$. Then let $f \in \mathrm{Aut}(C_n)$, where $f(x) = x^{-1}$. Then $f \circ f = \mathrm{Id}$. Then construct the map $\alpha : C_2 \to \mathrm{Aut}(C_n)$ by $e \mapsto \mathrm{Id}, \tau \mapsto f$.

Then we get the external semidirect product $G = C_n \rtimes C_2 = D_{2n}$, since $\tau\sigma = (e, \tau)(\sigma, e) = (ef(\sigma), \tau e) = (\sigma^{-1}, \tau) = \sigma^{-1}\tau$

We can get D_{∞} by letting C_{∞} being an infinite cyclic group with σ as a generator, and $f \in \mathrm{Aut}(C_{\infty})$ by $f(x) = x^{-1}$. Then define $D_{\infty} = C_{\infty} \rtimes C_2$, with $\alpha = f$.

Classification of small groups

Let $|G| = n$.

For $n = 1$, $G \cong \{e\}$.

For n prime, $G \cong \mathbb{Z}/n\mathbb{Z}$.

For $n = 4$, either $G \cong \mathbb{Z}/4\mathbb{Z}$ or $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We claim that there are no other possibilities for G.

If $n = 4$, and $G \not\cong \mathbb{Z}/4\mathbb{Z}$, all elements of G have order 1 or 2. Take any non-identity $x \in G$. Then $\langle x \rangle$ is a proper subgroup of G. Then take $y \in G/H$. Then $\langle y \rangle$ is another proper subgroup of G with trivial intersection with $\langle x \rangle$. Both these subgroups are normal, so $G = \langle x \rangle \times \langle y \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This proof in fact works for any $n = p^2$, so if $n = p^2$, either $G \cong \mathbb{Z}/p^2\mathbb{Z}$ or $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

If $n = 6$, then either $G \cong \mathbb{Z}/6\mathbb{Z}, G \cong S_3$.

Let $|G| = 6$. Then G has Sylow subgroups H, K or order $3, 2$. These subgroups are cyclic of different prime order, hence have trivial intersections, and $H \lhd G$, so $G = H \rtimes_{\alpha} K$, where α is a homo $K : \mathrm{Aut}(H)$. If $\alpha(k) = \mathrm{Id}$ for all k, we get $G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$. Otherwise, $\alpha(k)(h) = h^{-1}$ for the nontrivial $k \in K$, then $G = H \rtimes_{\alpha} K \cong D_6 \cong S_3$.

If $n = 8$, if there exists an element $a \in G$ of order 8, $G = \langle a \rangle \cong \mathbb{Z}/8\mathbb{Z}$.

If $x^2 = e$ for all $x \in G$, then G is abelian since $xyx^{-1}y^{-1} = xyxy = (xy)^2 = e$. Then, take distinct non-identity $x, y, z \in G$, $z \neq xy$, then we have that $G = (\langle x \rangle \times \langle y \rangle) \times \langle z \rangle$ since these normal(because G is ableian)subgroups have trivial intersection and are of order 2, so $G \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

If there exists $\sigma \in G$ of order 4, then let $H = \langle \sigma \rangle \lhd G$.

If there exists $\tau \in G\backslash H$ of order 2, then $K = \langle\tau\rangle$, then $H \bigcap K = \{e\}$, so $G = H \rtimes_\alpha K$, where $\alpha : K \to \text{Aut}(H)$. We can either send τ to Id, giving us $G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, or to f, $f(x) = x^{-1}$, in which case $G \cong D_8$.

Otherwise, all $\tau \in G\backslash H$ have order 4. Note that $\tau\sigma\tau^{-1} \in H$. If $\tau\sigma\tau^{-1} = \sigma$, then $\tau\sigma = \sigma\tau$, so $(\sigma\tau)^2 = \sigma^2\tau^2 = e$, so $\sigma\tau \in H$, implying $\tau \in H$, contradiction. If $\tau\sigma\tau^{-1} = e$, then $\tau\sigma = \tau$, so $\sigma = e$, contradiction. If $\tau\sigma\tau^{-1} = \sigma^2$, then $e = \sigma^4 = (\tau\sigma\tau^{-1})^2 = \tau\sigma^2\tau^{-1}$, so $\sigma^2 = e$, contradiction. Thus, we must have that $\tau\sigma\tau^{-1} = \sigma^3 = \sigma^{-1}$, which does indeed yield another group, namely Q_8, which is non-abelian and distinct from D_8.

Lecture 24

Didn't really take notes, but found that only remaining group of order 8 is Q_8, groups of order 12 are $A_4, \mathbb{Z}/12\mathbb{Z}, D_12, \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, M_12 = \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ with $f : \mathbb{Z}/4\mathbb{Z} \to \text{Aut}(\mathbb{Z}/3\mathbb{Z})$ non-trivial.

Lecture 25

Definition 45. *A group G is solvable if there's a chain of normal subgroups $\{e\} \lhd N_1 \lhd N_2 \lhd \cdots \lhd G$, such that each quotient group N_i/N_{i-1} is abelian.*

Proposition 35. *For $N \lhd G$, G is solvable if and only if $N, G/N$ are solvable.*

If G is solvable, then $\{e\} \lhd G_1 \lhd \cdots \lhd G$, so $\{e\} \lhd N \bigcap G_1 \lhd N \bigcap G_2 \lhd \cdots \lhd N \bigcap G = N$, and for $x, y \in N \bigcap G_{i+1}$, $xy(N \bigcap G_i) = yx(N \bigcap G_i)$ if and only if $x^{-1}y^{-1}xy \in N \bigcap G_i$, which is always true since $x^{-1}(y^{-1}xy) \in N$ and $x^{-1}(y^{-1}xy) \in G_i$ because G_{i+1}/G_i is abelian implies the commutator $(G_{i+1})' \subseteq G_i$.

Thus, N is solvable.

Then, note that $\{e\}N/N \lhd G_1N/N \lhd \cdots \lhd G/N$ since for $g \in G_i, g' \in G_{i+1}$, $g'NgNg'^{-1}N = g'gg'^{-1}N \in G_iN/N$.

Then by the 3rd Isomorphism Theorem, the quotients $(G_{i+1}N/N)/(G_iN/N) \cong G_{i+1}/G_i$ is abelian, so G/N is solvable.

Conversely, suppose $N, G/N$ are solvable. Then each subgroup $\bar{G_i}$ in the normal chain of G/N is in the form G_i/N for some subgroup $G_i \subseteq G$(just take all $g \in G$ such that $gN \in \bar{G_i}$ to get a subgroup G_i). Then by third iso $\bar{G_{i+1}}/\bar{G_i} = (G_{i+1}/N)/(G_i/N) \cong G_{i+1}/G_i$ is abelian, so we get a normal chain $e \lhd N_1 \lhd \cdots \lhd N \lhd G_1 \lhd \cdots \lhd G_n = G$ of G with abelian quotients along the way, so G is solvable.

Corollary 12. *S_n is not solvable if $n \geq 5$.*

Proof. $A_n \lhd S_n$, but for $n \geq 5$, A_n is simple, hence not solvable, so S_n isn't solvable. $\square$

Corollary 13. *Every group of order < 60 is solvable.*

Proof. Proceeding by induction on $|G|$, if G is abelian then it's clearly solvable since every quotient group is abelian, and if G is not abelian, then G has a normal proper nontrivial subgroup $N \lhd G$ since G isn't simple, which is solvable by induction, as is G/N, so G is solvable. $\square$

Theorem 25. *G is solvable $\iff \exists n$ s.t. $G_n = \{e\}$, where $G_0 = G$, $G_{i+1} = (G_i)'$, the commutator of G_i.*

Proof. The reverse implication is obvious, since the commutator of a group is normal in that group.

To show $\implies$, suppose $G = H_0 \rhd H_1 \rhd \cdots \rhd H_m = \{e\}$.

We claim $G_i \subseteq H_i$ by induction on i. Clearly $G_0 = H_0 = G$, and if the statement holds for i, then $G_{i+1} = (G_i)' \subseteq (H_i)'$, so since H_i/H_{i+1} is abelian, we have that $G_{i+1} \subseteq H_{i+1}$ by induction. Thus $G_m = H_m$ and we're done. $\square$

Free groups

Definition 46. *Consider an alphabet X, the free group $F = \{x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n}\}|0 \leq n \in \mathbb{Z}, x_i \in X, \epsilon_i \in \{-1, 1\}\}$, with group action of concatenation, where $x_i x_i^{-1} = x_i^{-1} x_i = e$, where e is the empty word*