Math 250A

Fall 2015

8/27

Group Action

A group G acts on a set S:
$G \times S \to S$
$(g, s) \mapsto g \cdot s$
$e \cdot s = s$
$(gg') \cdot s = g \cdot (g' \cdot s)$
Alternatively,
$\phi : G \to Perm(S)$
ϕ is a homomorphism (gives the corresponding properties)
$(\phi(g))(s) = g \cdot s$

Examples of Group Actions

The trivial action:
$G \to Perm(S)$ where $g \mapsto e_{Perm(S)}$
G acting on self by left/right translation, conjugation
G acting on the set of subgroups of G by conjugation:
$g \cdot H = gHg^{-1} = \{ghg^{-1} | h \in H\}$
Normal subgroup $N \trianglelefteq G$
G acting on N, $g \cdot n := gng^{-1} \in N$
$G = S_3$ where S is the set of subgroups of G of order 2.
S = {{1, (1 2)}, {1, (1 3)}, {1, (2 3)}}
recall $\sigma(a_1, a_2, a_3, ...a_k)\sigma^{-1} = (\sigma a_1, \sigma a_2, \sigma a_3, ...\sigma a_k)$
V vector space over a field K
G = GL(V) = group of invertible linear maps $V \to V$
e.g. if $V = K^n$ then G = GL(n, K)
G acts on V (rather simply) by $L \cdot v = L(v)$

Orbits and Stabilizers

Given G acting on S by $G \times S \to S$ there is an obvious relation on S:
s, s′: $s \sim s' \leftrightarrow \exists g \in G, s' = gs$
the orbit of s is just the equivalence class of s under this relation
i.e., $G \cdot s = \{g \cdot s | g \in G\}$
The conjugacy classes of s are the orbits of S under the group action of G by conjugation
the orbit of s, $O(s) = \{s\} \leftrightarrow s = gsg^{-1} \forall g$
$\leftrightarrow (\forall g) gs = sg$
$\leftrightarrow s \in Z(G)$ the center of the group
Example, for $G = S_3$
the orbit of 1 is $\{1\}$
the orbit of (1 2) = $\{$(1 2), (1 3), (2 3)$\}$
the orbit of (1 2 3) = $\{$(1 2 3), (1 3 2)$\}$
Stabilizer (isotropy group) of a given element $s \in S := G_s$
$G_s = \{g \in G | g \cdot s = s\}$
stabilizer is closed under inverses: $g \in G_s \to g \cdot s = s \to g^{-1}gs = g^{-1}s \to s = g^{-1}s$

large stabilizer$\leftrightarrow$ small orbit

there exists a natural bijection $\alpha : G/G_s \to O(s)$ defined $gG_s \mapsto g \cdot s$
well-definition:
if $g_1 G_s = g_2 G_s$ then $\exists g \in G_s, g_1 = g_2 g$ and $\alpha(g_1 G_s) = g_1 \cdot s = g_2 g s = g_2 s = \alpha(g_2 G_s)$
injectivity:
if $\alpha(g_1 G_s) = g_1 \cdot s = g_2 \cdot s = \alpha(g_2 G_s)$ then $g_2^{-1} g_1 \cdot s = s$, $g_2^{-1} g_1 \in G_s$ and $g_1 G_s = g_2 G_s$

Lang 1.1-1.4

1.1: Monoids

A *monoid* is a set with associative binary operation and unit element.
Abelian $\leftrightarrow$ commutative
A *submonoid* is a subset of a monoid with identity and closure under the operation
Such a submonoid is, itself, a monoid

1.2: Groups

A *group* is a monoid with inverses for each element
The *permutation group* of S is the set of all bijections $S \to S$ (with composition as product)
A direct product of groups has product defined componentwise
A *subgroup* of a group is a subset closed under composition and inverse
$S \subset G$ *generates* G if $\forall g \in G, g = \prod s_i$, where $s_i \in S$ or $s_i^{-1} \in S$
$G = \langle S \rangle$
The **group of symmetries of the square** is a non-abelian group of order 8

generated by σ, τ such that $\sigma^4 = \tau^2 = e$ and $\tau\sigma\tau^{-1} = \sigma^3$

The **quaternions** are a non-abelian group of order 8

generated by i, j where defining $k = ij$, $m = i^2$

$i^4 = j^4 = k^4 = e$, $i^2 = j^2 = k^2 = m$, and $ij = mji$

A *monoid-homomorphism* $f : G \to G'$ satisfies $f(xy) = f(x)f(y)$ and $f(e_G) = e_{G'}$

If G and G′ are groups, f is a group homomorphism ($f(x^{-1}) = f(x)^{-1}$ is implied)

An *isomorphism* is a bijective homomorphism.

An *automorphism* or *endomorphism* of G is an isomorphism $\varphi : G \to G$

The group **Aut(G)** is the set of all automorphisms of G

The *kernel* of a homomorphism $f : G \to G'$ is $\{g \in G : f(g) = e_{G'}\}$

the kernel and the image f are subgroups of their respective groups

An *embedding* is a homomorphism $f : G \to G'$ where $G \cong Im(f)$.

Fact: A homomorphism with trivial kernel is injective.

Forward is obvious.

Supposing trivial kernel: $f(x) = f(y) \leftrightarrow f(x)[f(y)]^{-1} = e \leftrightarrow f(xy^{-1}) = e \leftrightarrow xy^{-1} = e$

For G a group, and $H, K \leq G$ such that $H \cap K = e$, $HK = G$, and $xy = yx \; \forall x \in H \; \forall y \in K$

The map $H \times K \to G$ defined $(x, y) \mapsto xy$ is an isomorphism

This generalizes to finitely many such subgroups by induction

A *left coset* of H in G ($H \leq G$) is $aH = \{ax : x \in H\} \leq G$

$x \mapsto ax$ gives bijection between cosets of H, are all of equal cardinality

The *index* of H in G (G : H) is the number of cosets of H in G (right or left)

The *order* of G is the index (G : 1) of its trivial subgroup

For any subgroup H of G, G is the disjoint union of its cosets in H

For $H \leq G$, $(G : H)(H : 1) = (G : 1)$, holding if at least two are finite

If (G : 1) is finite, the order of H divides the order of G.

Given:

$H, K \leq G$, $K \subset H$

$\{x_i\}$ a set of coset representatives of K in H

$\{y_i\}$ a set of coset representatives of H in G

Then:

$\{y_j x_i\}$ is a set of coset representatives of K in G.

Therefore the above can be generalized to $(G : K) = (G : H)(H : K)$

Conclusion: groups of prime order are cyclic.

$J_n = \{1, ..., n\}$, $S_n = Perm(J_n)$

$\tau \in s_n$ is a **transposition** if $\exists r \neq s \in J_n$, $\tau(r) = s$, $\tau(s) = r$, $\tau(k) = k \; \forall k \neq r, s$

The set of transpositions generate S_n

Consider $H \leq S_n$ those which leave n fixed. Then $H \cong S_{n-1}$.

Now if $\sigma_i \in S_n$ for $1 \leq i \leq n$ are defined with $\sigma_i(n) = i$, $\{\sigma_i\}$ are coset reps for H

Hence $(S_n : 1) = n(H : 1) = n!$.

1.3: Normal subgroups

For H the kernel of $f : G \to G'$ a group-homomorphism, $xH = f^{-1}(f(x)) = Hx$

Such a relation is equivalent to e.g. $xH \subset Hx$ and $H \subset xHx^{-1}$

A subgroup $H \trianglelefteq G$ (satisfying $xHx^{-1} = H\ \forall x \in G$) is termed *normal*
H is normal $\leftrightarrow$ H is the kernel of some homomorphism
The *factor group* of G by $H \trianglelefteq G$ is the group of cosets, denoted G/H
$f : G \to G/H$ defined $x \mapsto xH$ is the canonical map for H
The *normalizer* N_S of $S \subset G$ is $\{x \in G | xSx^{-1} = S\}$
The normalizer of H is the largest subgroup of G in which H is normal
The *centralizer* Z_S of S is $\{x \in G | xyx^{-1} = y\ \forall y \in S\}$
The centralizer of G is called its *center*; its elements commute with all others in G
The **special linear group** is the kernel of the determinant (a homomorphism)
G is the *semidirect product* of N and H if $G = NH$ and $H \cap N = \{e\}$
An *exact* sequence $G' \xrightarrow{f} G \xrightarrow{g} G''$ satisfies $Im(f) = Ker(g)$.
Can extend to larger sequences as long as each triple satisfies the above
Some canonical homomorphisms, given $f : G \to G'$
$H = ker(f) \to \exists! f' : G/H \to G'$ injective $\to \exists \lambda : G/H \to Im(f)$ an isomorphism
$H \leq G$, N the minimal $N \trianglelefteq G$ s.t. $H \leq N$, $H \subset ker(f)$, then $N \subset ker(f)$, $\exists! f' : G/N \to G'$
$H, K \trianglelefteq G$, $K \subset H$, then $K \trianglelefteq H \to (G/K)/(H/K) \cong G/H$
$H, K \leq G$, $H \subset N_K \to H \cap K \trianglelefteq H$, $HK = KH \leq G$, $\to H/(H \cap K) \cong HK/K$
$H' \trianglelefteq G'$, $H = f^{-1}(H') \to H \trianglelefteq G \to \overline{f} : G/H \to G'/H'$ injective
A *tower* of subgroups of G is a sequence $G = G_0 \supseteq G_1 \supseteq G_2 ... \supseteq G_m$
Such a tower is normal if each $G_{i+1} \trianglelefteq G_i$ and abelian if each factor group is abelian
The preimage of a normal tower under a homomorphism is itself a normal tower
And similarly with the preimage of an abelian tower
Inserting finitely many subgroups into a tower yields a *refinement* of that tower
A *solvable* group has an abelian tower with $G_m = \{e\}$
An abelian tower of finite G admits a cyclic refinement.
$H \trianglelefteq G \to$ G is solvable $\leftrightarrow$ H and G/H are solvable
A *commutator* in G is an element of the form $xyx^{-1}y^{-1}$
The *commutator subgroup* of G is the subgroup generated by its commutators
A *simple* group is a non-trivial group whose only normal subgroups are {e} and itself
An abelian group G is simple $\leftrightarrow$ G is cyclic and of prime order
$U, V \leq G$, $u \trianglelefteq U$, $v \trianglelefteq V$, then we have the following:
$u(U \cap v \trianglelefteq u(U \cap V)$ and $(u \cap V)v \trianglelefteq (U \cap V)v$ with isomorphic factor groups, that is,
$u(U \cap V)/u(U \cap v) \cong (U \cap v)v/(u \cap V)v$
Two towers $G = G_1 \supseteq G_2 \supseteq \cdots \supseteq G_r$, $G = H_1 \supseteq H_2 \supseteq \cdots \supseteq H_s$ are *equivalent* if:
$r = s$ and $\exists i \mapsto i'$ such that $G_i/G_{i+1} \cong H_{i'}/H_{i'+1}$
Theorem (Schreier): Given a group G and two towers of that group.
If they are normal and end with the trivial group they have equivalent refinements
$G = G_1 \supseteq G_2 \supseteq \cdots \subseteq G_r = \{e\}$ normal, each G_i/G_{i+1} simple, $G_i \neq G_{i+1}$ for $1 \leq i \leq r-1$
Then any normal tower of G with these properties is equivalent to this tower.

1.4: Cyclic groups

A group G is *cyclic* if $\exists a \in G$ such that $\forall x \in G$, $x = a^n$ for some $n \in \mathbb{Z}$
Such an a is the *generator* of G.

If $a^m = e$ and $m > 0$ m is an *exponent* of a.
Such is an *exponent of* G if it is an exponent of a $\forall a \in G$.
Let G be a group, $a \in G$, $f : \mathbb{Z} \to G$ defined $f(n) = a^n$ and $H = ker(f)$
If the kernel is trivial, a has *infinite period* and generates an infinite cyclic subgroup
With a nontrivial kernel, its *period* d is the smallest positive element of the kernel
G a finite group, order > 1, $a \in G$, $a \neq e$, then the period of a divides n.
G cyclic: every subgroup of G is cyclic, and for f a homomorphism on G, $Im(f)$ is cyclic
Proposition:
(i) An infinite cyclic group has exactly two generators (if a is one, a^-1 is the other)
(ii) G finite cyclic of order n, x a generator; the set of generators is $\{x^v | gcd(v, n) = 1\}$
(iii) G cyclic, a and b two generators: $\exists f \in Aut(G)$, $f(a) = b$
(iii) conversely, if $f \in Aut(G)$, $f(a)$ is some generator of G
(iv) G cyclic of order n, d positive divisor of n $\to \exists! H \leq G$, $\#H = d$
(v) G_1, G_2 cyclic, $\#G_1 = m$, $\#G_2 = n$. If $gcd(m, n) = 1$, then $G_1 \times G_2$ is cyclic.
(vi) G finite abelian, noncyclic $\to \exists p$ prime and $H \leq G$, $H \cong C \times C$, C cyclic of order p

9/1

Group Actions $\to$ Sylow theorems

Recall:
the stabilizer $G_s = \{g \in G | g \cdot s = s\}$
the orbit $O(s) = \{g \cdot s | g \in G\}$
$G/G_s \cong O(s)$ and $\#(G/G_s) = \#O(s)$
Let $\Sigma =$ set of representatives for $s \sim s' \leftrightarrow O(s) = O(s')$
$\#S = \sum_{s \in \Sigma} \#O(s) = \sum_s (G : G_s)$
G finite $(G : G_s) = \frac{\#G}{\#G_s}$
Mass formula $\#S = (\sum_s \frac{1}{\#(G_s)})(\#G)$
A subgroup H of G acting upon G has as orbits, cosets, and trivial stabilizer.
Hence from the above $\#H_s = \#H$, and $\#G = (G : H) \cdot \#H$.
This is a statement of Lagrange's Theorem, $(G : H) = \frac{\#G}{\#H}$.
We can relate the stabilizers of points in the same orbit.
$G_s' = G_{g \cdot s} = gG_sg^{-1}$
See $(gxg^{-1})s' = (gxg^{-1})gs = g(xs)$
The stabilizer of s' is a conjugate of the stabilizer of s.
The kernel of the action

$$K = \{g \in \bigcap_{s \in S} G_s\}$$

This is just the kernel of $G \xrightarrow{\phi} Perm(S)$.
Assume $x \in G_s$. Claim $gxg^{-1} \in G_{gs}$, showing $gG_sg^{-1} \subset G_{gs}$
Since $x \in G_s$, $(gxg^{-1})s' = (gxg^{-1})gs = g(xs) = gs$.
Applying this relation with $g \to g^{-1}$ and $s \to gs$, $G_{gs} \subset gG_sg^{-1}$

Applications

p : prime
p-group: a finite group G, $\#G = p^n, n \geq 1$
"A p-group has a non-trivial center."
(Recall: the center $Z(G) = Z = \{g \in G | gs = sg \forall s \in G\}$).
Since $gs = sg \to s = gsg^{-1}$, will be useful to consider action on self by conjugation.
G a p-group, S a finite set. Then $\#O(s) = \frac{\#G}{\#G_s} = \frac{p^n}{p^k}$.
Two cases: 1) $\#O(s) = 1$ s is fixed by G, $s \in S^G$ (set of fixed points of S)
2) ($k < n$), thus $\#O(s)$ is divisible by p.
$\#S =$ sum of # of elements in the orbits $\equiv_{mod p}$ # of orbits of size $1 = \#(S^G)$.
Take S = G, with action $g : s \mapsto gsg^{-1}$. Then $S^G = Z(G)$.
Thus, $\#Z(G) \equiv_{mod p} p^n \equiv_{mod p} 0$. Center has order divisible by p.
$H \leq G$ a finite group, $(G : H) = p$, p the smallest prime dividing #G $\to H \trianglelefteq G$
Let $S = G/H$; $\#(S) = (G : H) = p$, and let G act on S by left translation.
This induces $\varphi : G \to S_P$; recall $\#S_p = p!$
The stabillizer of H, $G_H = \{x \in G | xH = H\} = H$.
By inspection, we can see that $G_{gH} = gHg^{-1}$.
Let $K = \bigcap_{g \in G} gHg^{-1}$, the largest normal subgroup contained in H.
Note that $K = ker(\varphi)$ induced above; by the First Isomorphism Theorem $\varphi(G) \leq S_p$.
$(G : K) = \#(G/K) = \#(\varphi(G))$, which divides $\#(S_p) = p!$
Further, since $K \leq H \leq G$, $(G : K) = (G : H)(H : K)$.
Since $(G : K)$ divides $p!$ and $(G : H)$ divides p, $(H : K)$ divides $(p-1)!$.
But p is the smallest prime dividing $\#G$, so $(H : K) = 1$, $K = H$ and H is normal.
A familiar embedding of a group into a larger group; "Cauchy's Theorem"
$G \hookrightarrow Perm(G)$ by letting G act on itself by left-translation.
Its kernel $K = \{g \in G | gs = s \forall s\} = \{e\}$ (consider $s = e$), hence is an injection.
Since an injection, an embedding.
Recall $S_n \subset$ group of $n \times n$ invertible matrices. $\sigma \mapsto M(\sigma)$ a permutation matrix.
Need to be careful in the construction to ensure $M(\sigma\tau) = M(\sigma)M(\tau)$!
E.g. $\sigma = (132)$ does $M(\sigma)$ have 1 in the 1st column, 3rd row?
Or in the 1st row, 3rd column? One of these yields $M(\sigma\tau) = M(\tau)M(\sigma)$.

G finite of order n; V the vector space of functions $G \xrightarrow{f} \mathbb{Z}$; note $V \cong \mathbb{Z}^n$
Linear maps $V \to V \leftrightarrow n \times n$ matrices over $\mathbb{Z}$; this is $GL(V) \approx GL(n, \mathbb{Z})$.
Similarly, invertible linear maps correspond to $n \times n$ invertible matrices over $\mathbb{Z}$.
We can embed G in $GL(n, \mathbb{Z})$ by using a left action of G on $GL(n, \mathbb{Z}) = \{\phi : V \to V\}$
Recall that $V = \{f : G \to \mathbb{Z}\}$.
This left action takes the form $L_g : f(x) \mapsto f(xg)$
Verify for yourself that $L_{gg'} = L_g \circ L_{g'}$ and $g \mapsto L_g$ is a homomorphism $G \to GL(V)$
Using $\mathbb{F}_p$ instead of $\mathbb{Z}$, get $G \hookrightarrow GL(n, \mathbb{F}_p)$, an embedding into a finite group

Lang 1.5-1.6

1.5: Operations of a group on a set