Abstract Algebra. Math 6320. Bertram/Utah 2022-23.
Groups

We start this semester with groups.

Definition. A *group* $(G, \cdot)$ is a set G with a multiplication operation:

$$\cdot : G \times G \to G \text{ that is}$$

(i) Associative: $g_1(g_2 \cdot g_3) = (g_1 \cdot g_2)g_3$ for all $g_1, g_2, g_3 \in G$.

(ii) Equipped with a two-sided multiplicative identity $e \in G$, i.e. for all $g \in G$:

$$e \cdot g = g \text{ (left identity) and } g \cdot e = g \text{ (right identity)}$$

(iii) Pairs each $g \in G$ with a two-sided inverse g^{-1}, i.e. $g^{-1} \cdot g = e = g \cdot g^{-1}$

Examples. Abelian groups, which are also commutative (with + as the operation)

The group S_n of permutations of the set $[n] = \{1, ..., n\}$. More generally, we will write $\text{Perm}(S)$ for the automorphism group of a set S.

The group $\text{GL}(n, k)$ of linear automorphisms of k^n. More generally, we will write $\text{GL}_k(V)$ for the group of linear transformations of a vector space V over k.

These last two examples are instances of the:

MetaExample. $G = \text{Aut}_{\mathcal{C}}(X)$ for an object X of a category $\mathcal{C}$.

Let's dispose of some uniqueness properties first:

Uniqueness of the Identity. If e' is any (right) identity, then in particular,

$$ee' = e \text{ in addition to the equality } ee' = e'$$

since e is a left identity. So $e = e'$ and there is no other right identity than the two-sided identity e. Similarly, there is no other left identity.

Uniqueness of the Inverse. Suppose that h is a (right) inverse to g. Then:

$$g^{-1}(gh) = g^{-1} \text{ in addition to the equality } (g^{-1}g)h = h$$

so by the associative property and the fact that g^{-1} is a left inverse of g, we have $g^{-1} = h$ and there is no other right inverse. Similarly, there is no other left inverse.

Corollary. Given a group G, there is a well-defined inverse map:

$$i : G \to G;\ i(g) = g^{-1} \text{ satisfying } i \circ i = 1_G$$

Definition. A set mapping $f : G \to G'$ of groups is a *homomorphism* if:

$$f(e) = e' \text{ and } f(g_1g_2) = f(g_1)f(g_2)$$

for all $g_1, g_2 \in G$. This defines a category $\mathcal{G}r$ of groups $(G, \cdot)$ since the composition:

$$(f' \circ f)(g_1 \cdot g_2) = f'(f(g_1) \cdot f(g_2)) = (f' \circ f)(g_1) \cdot (f' \circ f)(g_2)$$

of group homomorphisms is a group homomorphisms.

Proposition 1. A bijective group homomorphism $f : G \to G'$ is an isomorphism.

Proof. Given a bijective homomorphism $f : G \to G'$, we note that $f^{-1}(e') = e$ and given $g_1' = f(g_1), g_2' = f(g_2)$, then $g_1' \cdot g_2' = f(g_1)f(g_2) = f(g_1g_2)$, and so

$$f^{-1}(g_1' \cdot g_2') = g_1g_2 = f^{-1}(g_1')f^{-1}(g_2'). \quad \square$$

Examples. (a) The determinant $\det : \mathrm{GL}(n,k) \to (k^*, \cdot) = \mathrm{GL}(1,k)$

(b) The inverse $i : G \to G$ is not a homomorphism since:

$$i(g \cdot h) = (g \cdot h)^{-1} = h^{-1} \cdot g^{-1} = i(h) \cdot i(g)$$

i.e. the inverse mapping reverses the product.

(c) Left multiplication by an element $g \neq e$ is not a homomorphism, since:

$$g(g_1 g_2) \neq (gg_1)(gg_2) \text{ (for most } g \text{ in most groups)}$$

However, left multiplication by g, denoted by l_g, defines a homomorphism

$$l : G \to \mathrm{Perm}(G);\ g \mapsto l_g$$

from G to the group of permutations of G, since $l_e = 1_G$ and $l_{gh} = l_g \circ l_h$. Moreover, since $l_g(e) = g$ recovers the left translator, the l homomorphism is injective.

(d) Similarly, right multiplication by the *inverse* of $g \in G$ is a homomorphism:

$$r : G \to \mathrm{Perm}(G);\ g \mapsto r_{g^{-1}}$$

since $r_{(gh)^{-1}}(a) = a \cdot (gh)^{-1} = (ah^{-1})g^{-1} = r_{g^{-1}} \circ r_{h^{-1}}(a)$.

(e) *Conjugation* by $g \in G$ is given by:

$$c : G \to \ \mathrm{Aut}_{\mathcal{G}r}(G) \subset \mathrm{Perm}(G);\ c_g(h) = (l_g \circ r_{g^{-1}})(h) = ghg^{-1}$$

Each c_g is a *group automorphism* of G since $c_e = 1_G$, and:

$$c_g(h_1 h_2) = gh_1 h_2 g^{-1} = (gh_1 g^{-1}) \cdot (gh_2 g^{-1}) = c_g(h_1) \cdot c_g(h_2)$$

Definition. A subset $H \subset G$ is a *subgroup* if:

(i) $e \in H$, (ii) $h \in H$ implies $h^{-1} \in H$, and (iii) $h_1, h_2 \in H$ imply $h_1 \cdot h_2 \in H$

In other words, $(H, \cdot)$ is a group sitting inside G (with the same multiplication).

Example. The image $f(G) \subset G'$ of a homomorphism $f : G \to G'$ is a subgroup. Also, if $H' \subset G'$ is a subgroup, then the preimage $f^{-1}(H') \subset G$ is a subgroup.

This, together with Example (c) above give:

Cayley's Theorem. Every group G is isomorphic to a subgroup of $\mathrm{Perm}(G)$.

In fact, it is a subgroup in potentially two distinct ways, since both left and right multiplication (by the inverse) are injections of G into $\mathrm{Perm}(G)$. Note, however, that conjugation is **not** (usually) an injection of G into $\mathrm{Aut}_{\mathcal{G}r}(G)$.

Definition. Given a subgroup $H \subset G$, the *left cosets* of H are:

$$gH = \{gh \mid h \in H\}$$

and the right cosets are defined analogously.

Proposition 2. The left cosets are equivalence classes for the equivalence relation:

$$g_1 \sim g_2 \text{ if and only if } g_1 h = g_2 \text{ for some (unique) } h \in H$$

In particular, if H is finite, then each equivalence class has the same number:

$$|gH| = |H| \text{ of elements}$$

and if G is finite, then we have:

Lagrange's Theorem: $|G| = |H| \cdot |G/H|$ where $|G/H|$ is the number of left cosets.

Definition. The *order* of $g \in G$ is the smallest $d \geq 1$ so that $g^d = e$, or else, if there is no such d, we say that g has infinite order.

Proposition 3. If $|G| = n$, then the order of each $g \in G$ divides n.

Proof. Consider the $n+1$ elements $e, g, g^2, ..., g^n \in G$. Since $|G| = n$, at least two of them must coincide. Let $d \geq 1$ be the minimal "gap" so that $g^a = g^{a+d}$ for some a. Then $e = g^d$ (multiplying by g^{-a}), and so $H = \{e, g, g^2, ..., g^{d-1}\}$ is a cyclic subgroup of G consisting of d distinct elements. Thus $d = |H|$ divides n. □

Remark. As a consequence of the Proposition, $g^n = e$ for all $g \in G$ if $|G| = n$.

Corollary (Euler). The units in the ring $\mathbb{Z}/n\mathbb{Z}$, consisting of the elements that are relatively prime to n, form a group $(\mathbb{Z}/n\mathbb{Z})^*$, whose order is $\phi(n)$. Then:

$$a^{\phi(n)} \equiv 1 \pmod{n} \text{ if } \gcd(a, n) = 1$$

by the Proposition. In particular, we have **Fermat's Little Theorem**:

$$a^{p-1} \equiv 1 \pmod{p}$$

when p is prime not dividing a.

Proposition 4. The kernel $K \subset G$ of a homomorphism $f : G \to G'$, is a subgroup with the additional property:

$$c_g(K) = K \text{ for all } g \in G$$

This follows directly from the definitions. For example,

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

so $gkg^{-1} \in K$ whenever $k \in K$ showing that $c_g(K) \subset K$.

Definition. A subgroup $N \subset G$ with the additional property:

$$c_g(N) = N \text{ for all } g \in G$$

is called a *normal* subgroup of G.

Remark. All subgroups of an abelian group are normal, but we will see that there are plenty of subgroups of a general group G that are not normal.

Example. Let $H \subset \mathrm{GL}(2, k)$ be the subgroup of linear transformations that fix the x-axis. Such matrices are all of the form:

$$\begin{bmatrix} * & * \\ 0 & * \end{bmatrix}$$

but if we conjugate these by the reflection matrix:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

we get the matrices that fix the y-axis, which are all of the form:

$$\begin{bmatrix} * & 0 \\ * & * \end{bmatrix}$$

Thus H is not normal.

Definition. The *center* $Z(G) \subset G$ of a group G is the set:

$$Z(G) = \{h \in G \mid c_g(h) = ghg^{-1} = h \text{ for all } g \in G\}$$

i.e. $Z(G)$ consists of the elements of G that commute with all elements of G.

Remarks. (i) The center of a group always contains the identity element e.

(ii) Every subgroup $H \subset Z(G)$ is a normal, abelian subgroup of G.

Example. The center of $\mathrm{GL}(n,k)$ consists of the (nonzero) scalar multiples of $e = I_n$.

First Isomorphism Theorem. Each normal subgroup $N \subset G$ is the kernel of a surjective group homomorphism to the *quotient group* of (left) cosets:

$$q : G \to G/N = \{gN \mid g \in G\}$$

and conversely, if $K \subset G$ is the kernel of a group homomorphism $f : G \to G'$, then f factors through q followed by an isomorphism with the image: $\overline{f} : G/K \cong f(G)$.

Proof. The product of cosets:

$$(g_1H)(g_2H) = (g_1g_2)H$$

is not automatically well-defined for a general subgroup of G, since multiplication is not commutative. However, because N is a normal subgroup of G, we have:

$$g_2^{-1}Ng_2 = N \text{ and so } Ng_2 = g_2N$$

i.e. the left cosets and right cosets are the same. But then:

$$(g_1N)(g_2N) = (g_1N)(Ng_2) = g_1Ng_2 = (g_1g_2)N$$

is well-defined, and the rest of the proof is the same as we've seen in the context of commutative rings and ideals. □

For the rest of this section, we introduce ourselves to:

The Permutation Groups S_n

Definition. A *d-cycle* is a permutation $f : [n] \to [n]$ with the property that:

$$f(a), f^2(a), f^3(a), ..., f^d(a) = a$$

are distinct, for some $a \in [n]$, and all other elements $b \in [n]$ satisfy $f(b) = b$.

The notation for the cycle is: $C = (a\ f(a)\ f^2(a)\ \cdots\ f^{d-1}(a))$ which is ambiguous only in the choice of the initial element of the cycle.

Example. The two-cycles (transpositions) $(a\ b)$ and $(b\ a)$ are the same, as are

$$(a\ b\ c),\ (b\ c\ a) \text{ and } (c\ a\ b)$$

Remarks.(i) The identity $e \in S_n$ is the only one-cycle.

(ii) Disjoint cycles commute with each other, but:

$$(a\ b)(b\ c) = (a\ b\ c) \neq (a\ c\ b) = (b\ c)(a\ b)$$

when $a \neq b \neq c$. Thus, for example, S_n is not abelian when $n \geq 3$.

Cycle Notation. Every permutation $f \in S_n$ is a product of disjoint cycles.

Proof. Start with $a_1 = a \in [n]$ and consider the list of elements.

$$a, f(a), f^2(a), ..., f^n(a)$$

There must be a repetition in the list (since this consists of $n+1$ elements of $[n]$). Let $f^b(a) = f^{b+d}(a)$ with the smallest (positive) gap value d. Then:

$$a = f^{-b}f^b(a) = f^{-b}f^{b+d}(a) = f^d(a)$$

and each of $a, f(a), \cdots, f^{d-1}(a)$ are distinct. So this determines a cycle C_1.

Given cycles $C_1, ..., C_i$ with initial elements $a_1, ..., a_i$ associated to f, choose a_{i+1} distinct from the list of elements in the cycles, and consider the cycle:

$$C_{i+1} = (a_{i+1}, f(a_{i+1}), ..., f^{d_{i+1}-1}(a_{i+1}))$$

constructed as above. Then C_{i+1} is disjoint from each of the cycles $C_1, ..., C_i$. Eventually this process uses up all elements of $[n]$ and produces:

$$C_1 \cdot C_2 \cdots C_m$$

which *accounts for every value* $f(a)$ *for* $a \in [n]$. This represents the permutation.

Uniqueness. The disjoint cycles commute with each other and can start with any element in their list. Thus, the expression: $f = C_1 \cdots C_m$ is uniquely determined by f, if we make the convention that:

(a) Each cycle C_i commences with the smallest element a_i in the list, and

(b) The cycles are ordered so that $a_1 < a_2 < \cdots < a_m$

Moreover, since one-cycles are redundant, they are left out of the notation.

Lists of Elements. $S_2 = \{e, (1\ 2)\}$, $S_3 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$

$$S_4 = \{e, (**), (***), (****), (**)(**)\}$$

i.e. every element of S_4 is either a single cycle or a product of disjoint two-cycles.

These are easily counted:

(i) $\{(**)\}$ is comprised of $\binom{4}{2} = 6$ elements.

(ii) $\{(***)\}$ is comprised of $\binom{4}{3} \times 2 = 8$ elements.

(iii) $\{(****)\}$ is comprised of $\binom{4}{4} \times 3! = 6$ elements.

(iv) $\{(**)(**)\}$ is comprised of the 3 elements $(1\ 2)(3\ 4), (1\ 3)(2\ 4)$ and $(1\ 4)(2\ 3)$

which, including the identity, accounts for the $1+6+8+6+3 = 4!$ elements of S_4.

Lists of Subgroups.

The only (proper) subgroup of S_2 is $\{e\}$.

The subgroups of S_3 are $\{e\}$, $\{e, (1\ 2)\}$, $\{e, (1\ 3)\}$, $\{e, (2\ 3)\}$, $\{e, (1\ 2\ 3), (1\ 3\ 2)\}$. Notice that all of these are cyclic (of order dividing 6).

The subgroups of S_4 are of the following types:

- The cyclic subgroups $\{e, f, f^2, ..., f^{d-1}\}$ with $f^d = e$.

  Typical examples are the subgroups:

  $\{e, (1\ 2)\}, \{e, (1\ 2\ 3), (1\ 3\ 2)\}, \{e, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\}, \{e, (1\ 2)(3\ 4)\}$

- The Klein group (isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$):

$$K_4 := \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

- The four subgroups (isomorphic to S_3) each fixing one element of $[4]$:

$$H_i = \{f : [4] \to [4] \mid f(i) = i\} \text{ for } i = 1, 2, 3, 4$$

- The three dihedral subgroups (symmetries of a square) with 8 elements each.
- The group A_4 of rotations of a regular tethahedron (with 12 elements):

$$\{e, (***), (**)(**)\}$$

Observation. S_4 is the group of rotational symmetries of a cube, permuting the four long diagonals (joining pairs of opposite vertices). This group also permutes the three short diagonals (joining midpoints of opposite faces), resulting in a surjective group homomorphism:

$$S_4 \to S_3 \to 1$$

with kernel equal to the Klein group K_4, which is therefore a normal subgroup.

There is another way to see that the Klein group is normal:

Conjugacy Classes. Let G be a group. Then:

$$h_1 \sim h_2 \text{ if and only if } h_2 = c_g(h_1) = gh_1g^{-1} \text{ for some } g \in G$$

defines an equivalence relation on G. The equivalence classes $\mathrm{Cl}(h)$ for this relation are the *conjugacy classes* of G.

Thus a subgroup $N \subset G$ is normal if and only if it is a union of conjugacy classes.

Proposition 5. The conjugacy classes of S_n are in bijection with the *partitions*

$$n = d_1 + d_2 + \cdots + d_k \text{ (in weakly decreasing order) } d_1 \geq d_2 \geq \cdots \geq d_k$$

corresponding to the permutations of the form $C_1 \cdots C_k$ with $|C_i| = d_i$.

Remark. This ordering of cycles may not conform to the "unique" form.

Proof. When $C = (a_1\ a_2\ a_3\ \cdots\ a_d)$ is conjugated by $f \in S_n$, the result is:

$$f \circ C \circ f^{-1} = (f(a_1)\ f(a_2)\ \cdots\ f(a_d))$$

since

$$f \circ C \circ f^{-1}(f(a_i)) = f \circ C(a_i) = f(a_{i+1})$$

i.e. it is another cycle of the same length with entries specified by the permutation. The proposition now follows. □

Examples. The conjugacy classes of S_2 are:

$$\mathrm{Cl}(e) = \{e\} \text{ and } \mathrm{Cl}(1\ 2) = \{(1\ 2)\}$$

In fact, the conjugacy classes of any *abelian group* are the singleton sets.

There are three conjugacy classes of S_3, corresponding to the partitions:

$$3 = 3 \text{ with } \{(***)\} = \mathrm{Cl}(1\ 2\ 3) = \{(1\ 2\ 3), (1\ 3\ 2)\}$$

$$3 = 2 + 1 \text{ with } \{(**)\} = \mathrm{Cl}(1\ 2) = \{(1\ 2)(3), (1\ 3)(2), (2\ 3)(1)\}$$

(and recall that we've agreed to suppress the singletons from the notation), and

$$3 = 1 + 1 + 1 \text{ with } \mathrm{Cl}(e) = \{e\}$$

Comparing with the list of subgroups, we see that:

$$\{e, (1\ 2\ 3), (1\ 3\ 2)\} = \mathrm{Cl}(e) \cup \{(***)\}$$

is the only (nontrivial) normal subgroup of S_3.

Moving on to S_4, we see that the conjugacy classes are:

$$\{(****)\}, \{(***)\}, \{(**)\}, \{(**)(**)\}, \{e\}$$

corresponding, in order, to the partitions $4, 3+1, 2+1+1, 2+2, 1+1+1+1$.

Thus we get another verification that K_4 is a normal subgroup since:

$$K_4 = \{e\} \cup \{(**)(**)\}$$

Similarly, the alternating group A_4 is normal since:

$$A_4 = \{e\} \cup \{(**)(**)\} \cup \{(***)\}$$

and as a bonus, we see that K_4 is a normal subgroup of A_4.

Proposition 6. There is a "sign" group homomorphism:

$$\text{sgn} : S_n \to (\{\pm 1\}, \cdot)$$

with the property that $\text{sgn}(a\ b) = -1$ for all transpositions (two-cycles) (a, b).

Corollary. The sign of a d-cycle is $(-1)^{d-1}$ since

$$(a_1\ a_2 \cdots a_d) = (a_1\ a_2)(a_2\ a_3) \cdots (a_{d-1}\ a_d).$$

Proof. We need a definition of the sign. Given $f : [n] \to [n]$, let:

$$\text{sgn}(f) = \prod_{1 \le i < j \le n} \frac{f(j) - f(i)}{j - i}$$

Then:

(i) Each factor is unchanged if i and j are switched.

(ii) Applying f permutes the two-element subsets of $[n]$.

Thus by (i), the product may be unambiguously taken over the set of two-element subsets of $[n]$ (instead of pairs $i < j$), and by (ii), we have:

$$\prod_{\{i,j\}} |j - i| = \prod_{\{f(i), f(j)\}} |f(j) - f(i)| = \prod_{\{i,j\}} |f(j) - f(i)|$$

so $|\text{sgn}(f)| = 1$.

(iii) The sgn function is a group homomorphism. Given $f_1, f_2 : [n] \to [n]$,

$$\prod_{\{i,j\}} \frac{f_2(f_1(j)) - f_2(f_1(i))}{j - i} = \prod_{\{i,j\}} \frac{f_2(f_1(j)) - f_2(f_1(i))}{f_1(j) - f_1(i)} \cdot \frac{f_1(j) - f_1(i)}{j - i}$$

$$= \prod_{\{i,j\}} \frac{f_2(f_1(j)) - f_2(f_1(i))}{f_1(j) - f_1(i)} \cdot \prod_{\{i,j\}} \frac{f_1(j) - f_1(i)}{j - i}$$

$$= \prod_{\{f_1(i), f_1(j)\}} \frac{f_2(f_1(j)) - f_2(f_1(i))}{f_1(j) - f_1(i)} \cdot \prod_{\{i,j\}} \frac{f_1(j) - f_1(i)}{j - i}$$

$$= \prod_{\{i,j\}} \frac{f_2(j) - f_2(i)}{j - i} \cdot \prod_{\{i,j\}} \frac{f_1(j) - f_1(i)}{j - i}$$

again using (i) and (ii).

(iv) Applying $\tau = (a\ b)$ (with $a < b$) has the following effect on pairs $(i < j)$.

(a) Pairs $(i < j)$ with $i = a$ and $j \in [a + 1, b]$ satisfy $(\tau(i) > \tau(j))$

(b) Pairs $(i < j)$ with $i \in [a, b - 1]$ and $j = b$ satisfy $(\tau(i) > \tau(j))$.

(c) All other pairs satisfy $(\tau(i) < \tau(j))$.

Thus, counting the sign switches in (a) and (b), we get:

$$(b - a) + (b - a)$$

but the pair $(i, j) = (a, b)$ is counted twice, so there are an odd number overall. □

Definition. The *alternating group* A_n is the kernel of the sign homomorphism:

$$\text{sgn} : S_n \to \{\pm 1\}$$

and therefore it is a normal subgroup of S_n, with two cosets, and

$$|S_n| = 2|A_n|$$

by Lagrange's Theorem.

Looking back over the examples, we see that:

$\text{sgn}(**) = -1$,

$\text{sgn}(***) = 1$,

$\text{sgn}(****) = -1$,

$\text{sgn}(**)(**) = 1$

so that the normal cyclic subgroup of S_3 is A_3, and A_4 is indeed aptly named.

One More Example. The alternating group A_5 consists of:

$$\{e, (***), (**)(**) \text{ and } (*****)\}$$

We will see that this group with 60 elements, unlike $K_4 \subset A_4$, has no non-trivial normal subgroups.