Math 451: Abstract Algebra I

Wolmer V. Vasconcelos

Set 3

Fall 2009

Outline

More Stuff on Groups

- Groups acting on itself
- Counting Formulas
- Sylow Theorems
- The groups of low order
- The symmetric group

Outline

Groups acting on itself

By an operation of a group **G** on itself, we mean that in the definition of the action, **G** plays the role both of the group and of the set on which it operates.
Any group operates on itself in several ways, three of which we single out here. The first is left multiplication:

$$(g, x) \mapsto gx.$$

This is obviously a transitive operation of **G** on **G**, that is, **G** forms a single orbit, and the stabilizer of any element is the identity subgroup (1). So the action is faithful, and the homomorphism

$$\mathbf{G} \mapsto \mathrm{Perm}(\mathbf{G}) : g \mapsto m_g = \text{left multiplication by } g$$

Cayley's Theorem

Theorem

(Cayley's Theorem) *Every finite group* **G** *is isomorphic to a subgroup of a permutation group. If* **G** *has order n, then it is isomorphic to a subgroup of the symmetric group* S_n.

Proof. Since the operation by left multiplication is faithful, **G** is isomorphic to its image in $\mathrm{Perm}(\mathbf{G})$. If **G** has order n, then $\mathrm{Perm}(\mathbf{G})$ is isomorphic to S_n.

Discuss the pros/cons of this theorem.

Conjugation

The second operation we will consider is more subtle. It is conjugation:

$$\mathbf{G} \times \mathbf{G} \mapsto \mathbf{G}: \quad g : x \to gxg^{-1}$$

The stabilizer of an element $x \in \mathbf{G}$ for the operation of conjugation is called the centralizer of x and is denoted by $Z(x)$:

$$Z(x) = \{g \in \mathbf{G} : gxg^{-1} = x\} = \{g \in \mathbf{G} : gx = xg\}.$$

The centralizer is the set of group elements which commute with x. Note $x \in Z(x)$, because x commutes with itself.

The orbit of x for the operation of conjugation is called the conjugacy C_x. It consists of all conjugate elements gxg^{-1}.

By the Counting Formula

$$|\mathbf{G}| = \sum_{\text{conjugacy classes}} |C_x|.$$

Since the conjugacy classes are orbits for a group operation, they partition **G**, giving the Class Equation.

Proposition

An element x is in the center of a group G if and only if its centralizer $Z(x)$ is the whole group.

Center of a p-group

Definition

If p is a prime number, a p-group is a group $\mathbf{G}$ of order a power of p, $|\mathbf{G}| = p^e$, $e \geq 1$.

Proposition

The center of a p–group G has order > 1.

Proof.

- Recall that $| G | = \sum | C_x |$, where C_x runs over the conjugacy classes. The left side of this equation is a power of p, say p^e. Also, every term on the right side is a power of p too, because it divides p^e.

- We want to show that some group element $x \neq 1$ is in the center, which is the same as saying that more than one term on the right side of the equation is equal to 1. Now the terms other than 1, being positive powers of p, are divisible by p. Suppose that the class C_1 made the only contribution of 1 to the right side. Then the equation would read

$$p^e = 1 + \sum \text{multiples of } p,$$

which is impossible unless $e = 0$. □

Groups of order p^2

Proposition

Let G be a p–group, and let S be a finite set on which G operates. Assume that the order of S is not divisible by p. Then there is a fixed point for the action of G on S, that is, an element $s \in S$ whose stabilizer is the whole group.

There are nonabelian groups of order p^3. The dihedral group D_4, has order 8.

Let us classify groups of order p^2.

The Class Equation

Proposition

Every group of order p^2 is abelian.

Proof. Let G be a group of order p^2. We will show that for every $x \in G$, the centralizer $Z(x)$ is the whole group. Proposition 2 will then finish the proof.

So let $x \in G$. If x is in the center Z, then $Z(x) = G$ as claimed. If $x \notin Z$, then $Z(x)$ is strictly larger than Z, because it contains Z and also contains the element X. Now the orders of Z and $Z(x)$ divide $| G | = p^2$, and Proposition 4 tells us that $| Z |$ is at least p.

The only possibility is that $| Z(x) | = p^2$. Hence $Z(x) = G$, and x was in the center after all. □

Corollary

Every group of order p^2 is of one of the following types :

1. *a cyclic group of order p^2.*
2. *a product of two cyclic groups of order p.*

Proof. : Volunteer please.

More operations

Let **G** be a group. Another important action is:

Fix an integer m and let S be the set of subsets of **G** of m elements. Define:

$$\mathbf{G} \times S \mapsto S : (g, U) \to gU.$$

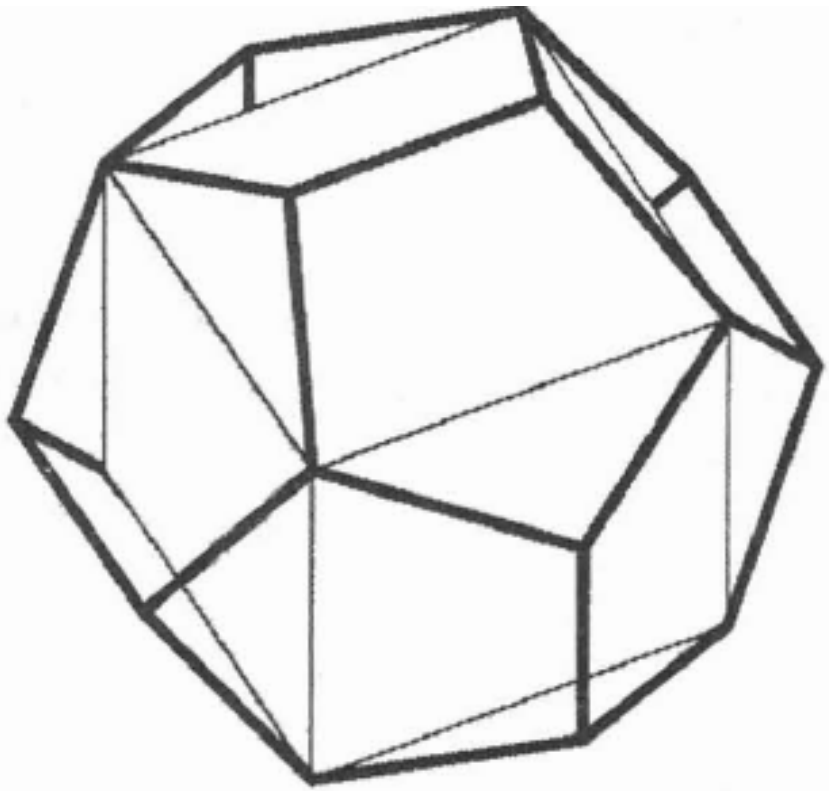
We will soon see its significance.

Outline

Icosahedral Group

Theorem

The icosahedral group I has no proper normal subgroup.



(2.7) **Figure.** One of the cubes inscribed in a dodecahedron.

Outline

Operations on Subsets

Let **G** be a group acting on a set S. For any subset $U \subset S$,

$$gU = \{gu : u \in U\}$$

is another subset of S. Thus there is a corresponding action of **G** on the power set $\mathcal{P}(S)$ of S.
There are many other examples: Sets of pairs $\{a, b\}$ of elements of S, ...

Proposition

Let H be a group which operates on a set S, and let U be a subset of S. Then H stabilizes U if and only if U is a union of H–orbits.

Proof. The assertion just restates the fact that the H-orbit of an element $u \in U$ is the set Hu of all elements hu. If H stabilizes U, then U contains the H-orbit of any of its elements.

Proposition

Let U be a subset of a group G. The order of the stabilizer $\mathrm{Stab}(U)$ of U for the operation of left multiplication divides the order of U.

Proof. Let H denote the stabilizer of U. The previous Proposition tells us that U is the union of orbits for the operation of H on **G**. These H-orbits are right cosets Hg. So U is a union of right cosets,

$$|U| = \sum |Hg|,$$

so $|H|$ divides $|U|$.

Normalizer of a subgroup

Let **H** be a subgroup of a group **G** and let S be the set of conjugate subgroups of **H**,

$$S = \{a\mathbf{H}a^{-1}, a \in \mathbf{G}.$$

G acts on S. The stabilizer of **H** is the set

$$N(\mathbf{H}) = \{a \in \mathbf{G} : a\mathbf{H}a^{-1} = \mathbf{H}\}.$$

The **G**-orbit of **H** is the set S, and

$$|S| = [\mathbf{G} : N(\mathbf{H})].$$

Outline

Groups acting on sets: Recall

- Let **G** be a group acting on a set S,

$$\mathbf{G} \times S \to S, \quad (g, s) \to gs$$

- S can be **G** itself, sets of cosets, set of subsets, lots of possibilities.
- One thing the action does is to decompose S into orbits

$$S = S_1 \cup S_2 \cup \cdots \cup S_r, \quad S_i = \mathbf{G}x_i, \quad x_i \in S$$

- The stabilizer of x_i is the set

$$\mathbf{H}_i = \{g \in \mathbf{G} : gx_i = x_i\}$$

  $\mathbf{H}_i$ is a subgroup (check).

- Note that $|S_i|$ is the index of $\mathbf{H}_i$: $\mathbf{G}/\mathbf{H}_i \leftrightarrow S_i$ as $g\mathbf{H}_i x_i = gx_i$.
- Each action gives rise to a counting formula

$$|S| = \sum_i |S_i| = \sum_i [\mathbf{G} : \mathbf{H}_i]$$

  Some actions–e.g. conjugation–have special names–e.g class equation

Sylow Theorems

Let **G** be a finite group of order $|\mathbf{G}| = n = p^e m$, where p is prime and does not divide m. $48 = 2^4 \times 3$.

- If **H** is a subgroup of **G**, Lagrange's Theorem asserts that $|\mathbf{H}|$ divides $|\mathbf{G}|$. The converse does not hold.
- Sylow Theorem(s) are assertions about the subgroups of **G** of order a power of p. Such groups are called p-groups .
- These theorems roughly say: (I) there are subgroups of order p^e–called Sylow subgroups; (II) describe some relationhips among such subgroups–in particular they are conjugate; and (III) give information on their numbers.

First Sylow Theorem

Theorem

Let G be a group of order $n = |G|$ and let p be a prime number which divides n. Write $n = p^e m$, for some integer m and p does not divide m. Then there is a subgroup of G whose order is p^e.

There are several proofs. One we will follow originated by Wielandt [who proved additional properties].

Proof

1. Let S be the set of subsets of $\mathbf{G}$ of order p^e.
2. We argue that one of these subsets is actually a subgroup.
3. More precisely, we will argue that one of these subsets has a stabilizer of order p^e.

Lemma

The number of subsets of order p^e in a set of $n = p^e m$ elements (p not dividing m) is the binomial coefficient

$$N = \binom{n}{p^e} = \frac{n(n-1)\cdots(n-k)\cdots(n-p^e+1)}{p^e(p^e-1)\cdots(p^e-k)\cdots 1}$$

Moreover N is not divisible by p.

Proof. It is a standard fact that the number of subsets of order p^e is this binomial coefficient. To see that N is not divisible by p, note that every time p divides a term $(n-k)$ in the numerator of N, it also divides the term (p^e-k) of the denominator exactly the same number of times: If we write k in the form $k = p^i l$, where p does not divide l, then $i < e$. Therefore $(n-k)$ and (p^e-k) are both divisible by p^i but not divisible by p^{i+1}. □

Proof of Sylow I

- Decompose S into orbits under the action: $\mathbf{g} \in \mathbf{G}$, $U \in S$, $U \to \mathbf{g}U$:

$$N = \mid S \mid = \sum_{\text{orbits}} \mid O \mid .$$

- Since p does not divide N, p does not divide some $\mid O \mid$, say $O = O_U$ is the orbit of U.
- Since

$$\mid \mathrm{Stab}(U) \mid \cdot \mid O_U \mid = \mid \mathbf{G} \mid = p^e m$$

and since $\mid O_U \mid$ is not divisible by p, $\mid \mathrm{Stab}(U) \mid$ is divisible by p^e.

- To prove that $\mathbf{H} = \mathrm{Stab}(U)$ has order p^e, we make use of a previous result, or argue directly:
  H acts on the set U of cardinality p^e. By the counting formula,
  $$|U| = p^e = \sum_{\text{orbits}} |O_i|,$$
  where the O_i are the distinct orbits.

  But each O_i is of the form $O_i = \mathbf{H}u$, $u \in U$, has cardinality equal to $|\mathbf{H}|$. But this would be impossible if $|\mathbf{H}| > p^e$.
- $\mathrm{Stab}(U)$ is a Sylow p-group.

Examples: The groups of order 6

- A first consequence: If $|\mathbf{G}| = n = mp^e$, and $p \not| m$, then there are elements of order p: Let $\mathbf{H}$ be a subgroup of order p^e and $1 \neq x \in \mathbf{H}$. Then x has order p^i, $0 < i \leq e$, and therefore x or one of its powers has order p.
- If $|\mathbf{G}| = 6$, $\mathbf{G}$ has an element x of order 3 and an element y of order 2. It is easy to verify that the 6 elements

$$1, x, x^2, y, xy, x^2y$$

  are distinct.
- In particular, yx must be one of these elements, but clearly cannot be any of the first 4,

$$xy = yx, \quad \text{or} \quad yx = x^2y.$$

- If $xy = yx$, $\mathbf{G} = C_6$, while $yx = x^2y$ means that $\mathbf{G} = D_3 = S_3$.

Corollary

Let **G** *be a group of order* $n = p^e m$*, with* p *prime and* $\gcd(p, m) = 1$*. Then for each* $i \leq e$ *there are subgroups of order* p^i*.*

Proof. Sylow (I) asserts the existence of a subgroup **H** of order p^e. ETS to show that **H** has a subgroup of order p^i. We induct on e.

We already proved that a p-group has a nontrivial center, in particular $Z(\mathbf{H}) \neq (1)$. The elements of $Z(\mathbf{H})$ have order a power of p. If g has order p^r, $x = g^{p^{r-1}}$ has order p.

Since $\langle x \rangle$ is a normal subgroup of **H**, $\mathbf{H}/\langle x \rangle$ is a p-group of order p^{e-1}, so by the induction it has subgroups of all orders p^j, $j \leq e - 1$. Since these subgroups are of the form $\mathbf{K}/\langle x \rangle$, we have that **K** can have any order p^j, $j \leq e$.

Second Sylow Theorem

While Sylow (I) guarantees the existence of a Sylow p-group $\mathbf{H}$ of a group $\mathbf{G}$ of order $p^e m$, $\gcd(p, m) = 1$, Sylow (II) gives some relationships among the Sylow p-groups:

Theorem

Let $\mathbf{K}$ *be a subgroup of* $\mathbf{G}$ *whose order is divisible by p, and let* $\mathbf{H}$ *be a Sylow p–subgroup of* $\mathbf{G}$*. There is a conjugate subgroup* $\mathbf{H}' = g\mathbf{H}g^{-1}$ *such that* $\mathbf{K} \cap \mathbf{H}'$ *is a Sylow subgroup of* $\mathbf{K}$*.*

Proof of Sylow II

- Let S denote the set of left cosets $b\mathbf{H}$ of $\mathbf{G}/\mathbf{H}$. $\mathbf{G}$ acts transitively on this set, that is there is a single orbit, that of the coset $s = 1H$,

$$a\mathbf{H} = a \cdot 1\mathbf{H}$$

  The stabilizer of s is $\mathbf{H}$

$$as = s \Rightarrow a \in \mathbf{H}$$

  and the stabilizer of as is the conjugate subgroup $a\mathbf{H}a^{-1}$.

- Restrict the action to $\mathbf{K}$ on the cosets S, and decompose S into $\mathbf{K}$-orbits. We know that $|S|$ is not divisible by p, so there is a $\mathbf{K}$-orbit O whose order is prime to p.

- Let O be the $\mathbf{K}$-orbit of as, and let $\mathbf{H}' = a\mathbf{H}a^{-1}$ be the stabilizer of as for the operation of $\mathbf{G}$.
- Then the stabilizer of as for the operation of $\mathbf{K}$ is $\mathbf{K} \cap \mathbf{H}'$, and the index $[\mathbf{K} : \mathbf{K} \cap \mathbf{H}']$ is $|O|$, which is prime to p.
- Since $\mathbf{H}'$ is a conjugate of $\mathbf{H}$, $\mathbf{H}'$ is a Sylow p-group. It follows that $\mathbf{H}' \cap \mathbf{K}$ is a Sylow p-group of $\mathbf{K}$.

Corollary

1. *If* **K** *is any subgroup of* **G** *which is a p-group, then* **K** *is contained in a Sylow p-subgroup of* **G**.
2. *The Sylow p-subgroups of* **G** *are all conjugate.*

Third Sylow Theorem

Theorem

Let $|\ G\ | = n$, *and* $n = p^e m$, *where* p *does not divide* m. *Let* s *be the number of Sylow* p*–subgroups. Then* s *divides* m *and is congruent* 1 *(modulo* p*) :* $s \mid m$, *and* $s = ap + 1$ *for some integer* $a \geq 0$.

Proof of Sylow III

- Let **H** be a Sylow p-group of **G**. According to the Corollary to Sylow(II), all Sylow p-groups are conjugate. This means that $s = [\mathbf{G} : N]$, where N is the normalizer of **H**. Since $\mathbf{H} \subset N$, s divides $[\mathbf{G} : \mathbf{H}] = m$.
- Consider the set $S = \{H = \mathbf{H}_1, H_2 \ldots, \mathbf{H}_s\}$ of Sylow p-groups and decompose it into the orbits by the action of conjugation by **H**.

  An orbit consists of a single group iff **H** is contained in the normalizer N_i of $\mathbf{H}_i$. If so, $\mathbf{H}_i$ and $\mathbf{H}_1$ are both Sylow subgroups of N_i. This implies $\mathbf{H}_i = \mathbf{H}_1$.

- Therefore there is a single **H**-orbit of order 1, namely $\{\mathbf{H}\}$.
- The other orbits have order divisible by p because their orders divide $|\mathbf{H}|$, by the Counting Formula. This proves $s \equiv 1$ (modulo p).

Examples: The groups of order 10

Proposition

Every group **G** *of order* 10 *is cyclic or isomorphic to* D_5.

Proof. Check the Sylow 2- and 5-subgroups.

Volunteer, please.

Examples: The groups of order 15

Proposition

Every group **G** *of order* 15 *is cyclic.*

Proof. Check the Sylow 3- and 5-subgroups.

Volunteer, please.

Examples: The groups of order 21

Proposition

There are two isomorphism classes of groups of order 21: The cyclic group C_{21} and the group of two generators x, y satisfying the relations

$$x^7 = 1, y^3 = 1, yx = xy^2.$$

Proof. Volunteer, please.
First prove:

Lemma

If **G** *is a group of order pq, p and q primes with $p < q$, then the Sylow q-group is normal.*

- The Lemma above shows that the Sylow 7-subgroup **K** must be normal.
- If the Sylow 3-subgroup **H** is also normal, as in the discussion of the groups of order 15, **G** would be cyclic.
- But the possibility that there are seven conjugate Sylow 3-subgroups **H** is not ruled out by the theorem, and in fact this case does arise. [see later]

- Let x denote a generator for **K**, and y a generator for one of the Sylow 3-subgroups **H**. Then $x^7 = 1$, $y^3 = 1$, and, since **K** is normal, it implies that

$$x = y^3 x y^{-3} = y^2 x^i y^{-2} = y x^{i^2} y^{-1} = x^{i^3}$$

  for some $i < 7$.

- We can restrict the possible exponents i by using the relation $y^3 = 1$. It implies that $i^3 = 1 \pmod 7$. This means that i can take the values 1, 2, 4.

- Case 1: $yxy^{-1} = x$. The group is abelian, and it is isomorphic to a direct product of cyclic groups of orders 3 and 7. Such a group is cyclic.
- Case 2: $yxy^{-1} = x^2$. The multiplication in **G** can be carried out using the rules $x^7 = 1$, $y^3 = 1$, $yx = x^2y$, to reduce every product of the elements x, y to one of the forms $x^i y^j$ with $0 \leq i < 7$ and $0 \leq j < 3$.
- The group is: The set of matrices $\begin{bmatrix} 1 & a \\ & c \end{bmatrix}$, where $a, c \in \mathbb{Z}_7$ and $c = 1, 2, 4$.

- Case 3: $yxy^{-1} = x^4$. In this case, we replace y by y^2, which is also a generator for **H**, to reduce to the previous case:
$$y^2xy^{-2} = yx^4y^{-1} = x^{16} = x^2$$

- Thus there are two isomorphism classes of groups of order 21, as claimed.

Outline

Homework #7

Do 3 Problems.

1. How many elements of order 5 are contained in a group of order 20?
2. Prove that no group of order p^2q, where p and q are prime, is simple.
3. Prove that no group of order 224 is simple.
4. Classify all groups of order 33.

Outline

The Groups of Order 12

Let us deploy the Sylow Theorems (ST) to classify all groups of order $12 = 2^2 \cdot 3$. Class, what can we expect?

According to (ST), there is a Sylow 2-group H of order 4, and a Sylow 3-group K of order 3. Moreover:

- The number of Sylow 2-subgroups is either 1 or 3, and that the number of Sylow 3-subgroups is 1 or 4.
- H is a group of order 4 and is therefore either a cyclic group or the Klein four group V, a product of two cyclic groups of order 2: $H = C_4$ or $H = V$.

Lemma

At least one of the subgroups H, K is normal.

Proof. Suppose that K is not normal. Then K has four conjugate subgroups $K = K_1, \ldots, K_4$. Since they have order 3, the intersection of any two of these groups must be the identity. Counting elements shows that there are only three elements of **G** which are not in any of the groups K_i.

The Sylow 2-subgroup H has order 4, and $H \cap K_i = (1)$. Therefore it consists of the three elements and 1. This describes H for us and shows that there is only one Sylow 2-subgroup. Thus H is normal.

The Groups of Order 12

Theorem

There are five isomorphism classes of groups of order 12*. They are represented by :*

1. *the product of cyclic groups* $C_3 \times C_4$*, (same as* C_{12}*),*
2. *the product of cyclic groups* $C_2 \times C_2 \times C_3$ *,*
3. *the alternating group* A_4*,*
4. *the dihedral group* D_6*,*
5. *the group generated by* x, y *with relations* $x^4 = 1$*,* $y^3 = 1$*,* $xy = y^2x$*.*

Proof

Since $H \cap K = (1)$, every element of HK has a unique expression $E : \{hk\}$, and since $|G| = 12$, $HK = G$.

If H is normal, K operates on H by conjugation, that is

$$k \in K, h \in H, \quad h \to khk^{-1},$$

and we will show that this operation, together the structure of H and K, determines the structure of G. Similarly, if K is normal–then H operates on K, and this operation determines G.

Case 1: H and K are both normal: Thus for $h \in H$ and $k \in K$,

$$hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1}) \in H \cap K = (1).$$

Then G is isomorphic to the product group $H \times K$. There are two possibilities: $G = C_4 \times C_3$ or $G = V \times C_3$. These are the abelian groups of order 12.

Case 2: H is normal but K is not. So there are four conjugate Sylow 3-subgroups, $\{K = K_1, K_2, K_3, K_4\}$, and G operates by conjugation on this set S of four subgroups. The operation determines a permutation representation

$$\varphi : \mathbf{G} \to S_4.$$

Let us show that φ maps **G** isomorphically to the alternating group A_4 in this case.
The stabilizer of K for the operation of conjugation is the normalizer $N(K_1)$ which contains K_1. The Counting Formula shows that $[N : K_1] = 3$, and hence $N(K_1) = K$. Since the only element common to the subgroups K_i, is the identity, only the identity stabilizes all of these subgroups. Thus φ is injective, **G** is isomorphic to its image in S_4.

Since **G** has four subgroups of order 3, it contains eight elements of order 3 and these elements certainly generate the group. If x has order 3, then $\varphi(x)$ is a permutation of order 3 in S_4. The permutations of order 3 are even. Therefore $\varphi(\mathbf{G}) \subset A_4$. Since the subgroups have the same order, they are equal.

As a corollary, we note that if H is normal and K is not, then H is the four group V, because the Sylow 2-subgroup of A_4 is V.

Case 3: K is normal, but H is not. In this case H operates on K by conjugation: conjugation by an element of H is an automorphism of K.

- We let y be a generator of the cyclic group K: $y^3 = 1$. There are only two automorphisms of K-the identity and the automorphism which interchanges y and y^2.
- Suppose that H is cyclic of order 4, and let x generate $H : x^4 = 1$. Then **G** is not abelian, $xy \neq yx$, and so conjugation by x is not the trivial automorphism of K. Hence $xyx^{-1} = y^2$. The Todd-Coxeter Algorithm show that these relations define a group of order 12

$$x^4 = 1, y^3 = 1, xyx^{-1} = y^2.$$

- The last possibility is that H is isomorphic to the Klein four group. Since there are only two automorphisms of K, there is an element $w \in H$, besides the identity operating trivially: $wyw^{-1} = y$.
- Since **G** is not abelian, there is also an element $u \in H$ which operates nontrivially: $uyu^{-1} = y^2$.
- Then the elements of H are $\{1, u, w, uw\}$ and the relations The element $x = vy$ has order 6, and

$$vxv^{-1} = vwyv^{-1} = wy^2 = y^2w = x^{-1}.$$

- The relations $x^6 = 1, v^2 = 1, vxv^{-1} = x^{-1}$ define the group D_6, so **G** is dihedral in this case.

Outline

The Symmetric Group

- Notation: For the natural number n, $[n] = \{1, 2, \ldots, n\}$ and S_n is the group of permutations of $[n]$.
- Representation: Let $\sigma \in S_n$; it can represented by the array

$$\sigma = \begin{bmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{bmatrix},$$

  where $\sigma(j) = i_j$.
- Efficiency: If $\sigma(i) = i$, in the representation we may leave out the corresponding column.

- Conventions: Let σ and τ be two permutations of $[n]$. There are two ways to interpret the composite $\tau\sigma$:
  1. First σ then τ: $\tau\sigma(i) = \tau(\sigma(i))$
  2. First τ then σ: $\sigma\tau(i) = \sigma(\tau(i))$ which is often written $(i)\tau\sigma$.

- Achtung: The textbook uses the second convention, but we shall use the first.

Cycles

- Cycles: A cycle is a permutation of the form: For distinct $a_i \in [n]$, $1 \leq i \leq r$,

$$\sigma : a_1 \to a_2 \to \cdots \to a_r \to a_1$$

  σ is said to be a cycle of length r. It is represented by $\sigma = (a_1, a_2, \ldots, a_r)$. Note that $\sigma^r = 1$.

- Transpositions: A cycle of length 2 is called a transposition: $\sigma = (a, b) = (b, a)$, $a \neq b$.

- Calculation: If σ is a cycle of length r, say $(1, 2, \ldots, r)$,

$$(1, 2, \ldots, r) = (1, r)(1, r-1) \cdots (1, 4)(1, 3)(1, 2)$$

- Read composition from right to left

$$1 \to 2 \to 1 \to 3 \to 1 \to 4 \to \cdots \to r$$

- Thus any cycle is the product of transpositions.

Elementary Properties

Proposition

Every finite group **G** *can be embedded as a subgroup of some* S_n.

Proof. Suppose $|\mathbf{G}| = n$, say $\mathbf{G} = \{a_1, \ldots, a_n\}$. Each $a \in \mathbf{G}$ defines a permutation of the set $[n]$ by the rule

$$a : a_i \to a \cdot a_i = a_{\varphi(i)}$$

$$\varphi : \mathbf{G} \to S_n$$

is a one-one homomorphism. □

A measure of commutativity

Proposition

Let σ, τ be permutations which operate on disjoint sets of indices. Then $\sigma\tau = \tau\sigma$.

Cycle Decomposition

For $p \in S_n$, consider the action of p on $[n]$: $i \to p(i)$, This defines an equivalence relation on $[n]$ that decomposes the set into the p-orbits

$$[n] = \bigcup_{r=1}^{k} O_r,$$

$O_r = \{u, pu, p^2u, \ldots\}$.

We denote the cycle $u \to pu \to p^2u \to \ldots \to u$ by $\sigma_r = (u, pu, \ldots, p^{r-1}u)$.

Proposition

Every permutation p not the identity is a product of cyclic permutations which operate on disjoint sets of indices : $p = \sigma_1\sigma_2\cdots\sigma_k$, and these cyclic permutations σ_r are uniquely determined by p.

Example of a cycle decomposition

$$p = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 5 & 8 & 1 & 2 & 9 & 7 & 4 \end{bmatrix}$$

$$\begin{aligned} \sigma_1 &: 1 \to 3 \to 5 \to 1 \\ \sigma_2 &: 2 \to 6 \to 2 \\ \sigma_3 &: 4 \to 8 \to 7 \to 9 \to 4 \end{aligned}$$

$$p = \sigma_1\sigma_2\sigma_3 = (1,3,5)(2,6)(4,8,7,9)$$

Order of a permutation

Corollary

Let p be a permutation which is a product of cyclic permutations which operate on disjoint sets of indices :

$$p = \sigma_1 \sigma_2 \cdots \sigma_k.$$

Then the order of p is the least common multiple of the orders of the cyclic permutations σ_r.

Proof. Volunteer, please.

Illustration: What is the maximal order of the elements of S_{10}?
Another volunteer, please.

Conjugation of cycles

Proposition

Let $\sigma = (a, b)$ be a transposition and p a permutation. Then $p^{-1}\sigma p = (p^{-1}(a), p^{-1}(b))$.

Proof.

If $p(c) \neq a, b$, then

$$p^{-1}\sigma p(c) = c.$$

If $p(c) = a$ (or b),

$$p^{-1}\sigma p(p^{-1}(a)) = p^{-1}(b).$$

Proposition

1. *Let σ denote the cyclic permutation $(\mathbf{i}_1\ \mathbf{i}_2\ \cdots\ \mathbf{i}_k)$, and let q be any permutation. Denote the index $q^{-1}\mathbf{i}_r$ by $\mathbf{j}_r$. Then the conjugate permutation $q^{-1}\sigma q$ is the cyclic permutation $(\mathbf{j}_1\ \mathbf{j}_2\ \cdots\ \mathbf{j}_k)$.*
2. *If an arbitrary permutation p is written as a product of disjoint cycles σ, then $q^{-1}pq$ is the product of the disjoint cycles $q^{-1}\sigma q$.*
3. *Two permutations p, p' are conjugate elements of the symmetric group if and only if their cycle decompositions have the same orders.*

Class Equation of S_4

Recall: The class equation of a group is the accounting of the orbits under the action of conjugation:

Volunteer, please.

Representations

Let S_n be the symmetric group on n symbols, say $[n]$, and let $\mathbf{G}$ be $GL_n(\mathbb{R})$, the group of invertible, real, $n \times n$ matrices.

The permutation representation is the following homomorphism

$$\varphi : S_n \to \mathbf{G}$$

defined as follows
Let $e_1, \ldots, e_n$ be the canonical basis of $\mathbb{R}^n$. For $\sigma \in S_n$, set

$$\varphi(\sigma)(e_i) = e_{\sigma(i)}$$

$\varphi(\sigma)$ is an injective homomorphism.

Parity

Definition

The signature or parity of $\sigma \in S_n$ is the integer $\operatorname{sign}(\sigma) = \det(\varphi(\sigma))$. The permutations of parity 1 are said to be even, those of parity -1 are called odd.

- Transpositions are odd permutations. More generally, σ is odd if and only if it is the product of an odd number of transpositions.
- The even transpositions form a subgroup, A_n, called the alternating subgroup. It has index 2, so it has order $n!/2$.
- A_n is a normal subgroup. It is involved in the solution of many problems. Why?

Generating A_n and S_n

Proposition

1. *A_n is generated by 3-cycles.*
2. *If a subgroup $\mathbf{G}$ of S_n contains a transposition and an n-cycle, then $\mathbf{G} = S_n$.*

- A_n consists of the even permutations, in particular every $p \in A_n$ can be written as a product of an even number of transpositions

$$p = \sigma_1 \sigma_2 \cdots \sigma_{2r-1} \sigma_{2r}$$

- It suffices to prove that each product $(a, b)(c, d)$ is a product of (r, s, t).

- If the transpositions (a, b) and (c, d) share exactly one symbol, say (a, b), (b, c), then $(a, b)(b, c) = (a, b, c)$. If they share two symbols, $(a, b)(a, b) = 1$.
- If all 4 symbols are different, $(a, b)(c, d) = (a, b, c)(d, b, c)$
- For the second assertion, we may assume $\sigma = (1, 2, \ldots, n) \in \mathbf{G}$ and some $\tau = (a, b) \in \mathbf{G}$. We must show that every transposition can be written as a product of σ and τ.
- Your turn!

A_4

The conjugacy classes of A_4 are:

$$(1)$$
$$(1,2)(3,4), (1,3)(2,4), (1,4)(2,3)$$
$$(1,2,3), (1,3,2), (1,2,4), (1,4,2), (2,3,4), (2,4,3), (1,3,4), (1,4,3)$$

$V = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ is a normal subgroup of A_4 (and of S_4 as well).

Warmup Exercise

Let p and q be permutations. Prove that pq and qp have cycle decompositions of equal length.

What is the hint?

A_n, $n \neq 4$, is simple

Definition

A group G is said to be simple if G has no proper normal subgroups.

Example: $|\mathbf{G}|$ prime. A_4 is not simple.

Theorem

For $n \geq 5$, A_n is a simple group.

A_n

Theorem

The alternating group A_n is simple if and only if $n \neq 4$.

The proof we shall give is quite elementary. It will be preceded by two lemmas. Recall that if τ is a 2-cycle, $\tau^2 = (1)$ and hence $\tau = \tau^{-1}$.

Special generation of A_n

We already know that A_3 is generated by its 3-cycles. The following lemma is more demanding:

Lemma

Let r, s be distinct elements of $\{1, 2, \ldots, n\}$. Then A_n ($n \geq 3$) is generated by the 3-cycles

$$\{(rsk) \mid 1 \leq k \leq n,\ k \neq r, s\}.$$

We are assuming that r and s are fixed, so there are only $n - 2$ 3-cycles of this type.

Proof. Assume $n > 3$ (the case $n = 3$ is trivial). Every element of A_n is a product of terms of the form $(ab)(cd)$ or $(ab)(ac)$, where a, b, c, d are distinct elements of $\{1, 2, \ldots, n\}$. Since $(ab)(cd) = (acb)(acd)$ and $(ab)(ac) = (acb)$, A_n is generated by the set of all 3-cycles.

Any 3-cycle is of the form $(rsa), (ras), (rab), (sab)$, or (abc), where a, b, c are distinct, and $a, b, c \neq r, s$. Since $(ras) = (rsa)^2$, $(rab) = (rsb)(rsa)^2$, $(sab) = (rsb)^2(rsa)$, and $(abc) = (rsa)^2(rsc)(rsb)^2(rsa)$, A_n is generated by

$$\{(rsk) \mid 1 \leq k \leq n,\ k \neq r, s\}.$$

□

Lemma

If N is a normal subgroup of A_n ($n \geq 3$) and N contains a 3–cycle, then $N = A_n$.

Proof. If $(rsc) \in N$, then for any $k \neq r, s, c$,

$$(rsk) = (rs)(ck)(rsc)^2(ck)(rs) = [(rs)(ck)](rsc)^2[(rs)(ck)]^{-1} \in N.$$

Hence $N = A_n$.

Theorem

The alternating group A_n is simple if and only if $n \neq 4$.

Proof. $A_2 = (1)$ and A_3 is the simple cyclic group of order 3. It is easy to verfify that

$$\{(1),\ (12)(34),\ (13)(24),\ (14)(23)\}$$

is a normal subgroup of A_4. If $n \geq 5$ and N is a nontrivial normal subgroup of A_n, we shall show $N = A_n$ by considering the possible cases.

Case 1. N contains a 3-cycle; hence $N = A_n$.

Case 2. N contains an element σ, the product of disjoint cycles, at least one of which has length $r \geq 4$. Thus $\sigma = (a_1 a_2 \cdots a_r)\tau$ (disjoint). Let $\delta = (a_1 a_2 a_3) \in A_n$. Then $\sigma^{-1}(\delta\sigma\delta^{-1}) \in N$ by normality. But

$$\begin{aligned} \sigma^{-1}(\delta\sigma\delta^{-1}) &= \tau^{-1}(a_1 a_r a_{r-1} \cdots a_2)(a_1 a_2 a_3)(a_1 a_2 \cdots a_r)\tau(a_1 a_3 a_2) \\ &= (a_1 a_3 a_r) \in N. \end{aligned}$$

Hence $N = A_n$.

Case 3. N contains an element σ, the product of disjoint cycles, at least two of which have length 3, so that $\sigma = (a_1 a_2 a_3)(a_4 a_5 a_6)\tau$ (disjoint). Let $\delta = (a_1 a_2 a_4) \in A_n$. Then as above N contains

$$\begin{aligned} & \sigma^{-1}(\delta\sigma\delta^{-1}) \\ = \; & \tau^{-1}(a_4 a_6 a_5)(a_1 a_3 a_2)(a_1 a_2 a_4)(a_1 a_2 a_3)(a_4 a_5 a_6)\tau(a_1 a_4 a_2) \\ = \; & (a_1 a_4 a_2 a_6 a_3). \end{aligned}$$

Hence $N = A_n$ by case 2.

Case 4. N contains an element σ that is the product of one 3-cycle and some 2-cycles, say $\sigma = (a_1 a_2 a_3)\tau$ (disjoint), with τ a product of disjoint 2-cycles. Then $\sigma^2 \in N$ and

$$\sigma^2 = (a_1 a_2 a_3)\tau(a_1 a_2 a_3)\tau = (a_1 a_2 a_3)^2\tau^2 = (a_1 a_2 a_3)^2 = (a_1 a_3 a_2),$$

whence $N = A_n$.

Case 5. Every element of N is the product of (an even number of) disjoint 2-cycles. Let $\sigma \in N$, with $\sigma = (a_1 a_2)(a_3 a_4)\tau$ (disjoint). Let $\delta = (a_1 a_2 a_3) \in A_n$; then $\sigma^{-1}(\delta\sigma\delta^{-1}) \in N$ as above. Now

$$\begin{aligned} \sigma^{-1}(\delta\sigma\delta^{-1}) &= \tau^{-1}(a_3 a_4)(a_1 a_2)(a_1 a_2 a_3)(a_1 a_2)(a_3 a_4)\tau(a_1 a_3 a_2) \\ &= (a_1 a_3)(a_2 a_4). \end{aligned}$$

Since $n \geq 5$, there is an element $b \in \{1, 2, \ldots, n\}$ distinct from a_1, a_2, a_3, a_4. Since $\zeta = (a_1 a_3 b) \in A_n$ and $\xi = (a_1 a_3)(a_2 a_4) \in N$, $\xi(\zeta\xi\zeta^{-1}) \in N$. But

$$\xi(\zeta\xi\zeta^{-1}) = (a_1 a_3)(a_2 a_4)(a_1 a_3 b)(a_1 a_3)(a_2 a_4)(a_1 b a_3) = (a_1 a_3 b) \in N.$$

Hence $N = A_n$.

Since the cases listed cover all the possibilities, A_n has no proper normal subgroups and hence is simple. $\square$

Outline

Homework #8

Do 3 Problems.

1. Show how to determine the parity of a permutation when it is written as a product of cycles.
2. Find all subgroups of S_4 of order 4. Which are normal (with proofs)?
3. Determine the cycle decomposition of the permutation on $[n]$ given by $i \to n + 1 - i$.
4. Prove that A_n is the only subgroup of S_n of index 2.

Outline

The free group

Proposition

There is only one reduced form of a given word w.

Proposition

The product of equivalent words is equivalent : If $w \sim w'$ and $v \sim v'$, then $wv \sim w'v'$.

Proposition

Let F denote the set of equivalence classes of words in W'. Then F is a group with the law of composition induced from W'.

Outline

Generators and Relations

Proposition

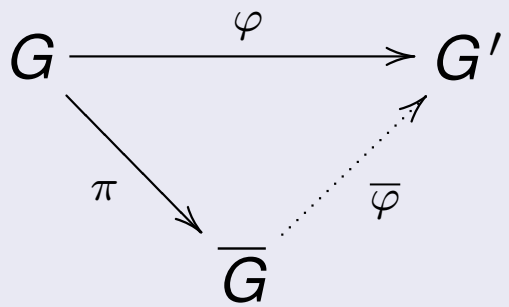
Let F be the free group on a set $S = \{a, b, \ldots\}$, and let G be a group. Every map of sets $f : S \to G$ extends in a unique way to a group homomorphism $\varphi : F \to G$. If we denote the image $f(x)$ of an element $x \in S$ by $\widetilde{x}$, then φ sends a word in $S' = \{a, a^{-1}, b, b^{-1}, \ldots\}$ to the corresponding product of the elements $\{\widetilde{a}, \widetilde{a}^{-1}, \widetilde{b}, \widetilde{b}^{-1}, \ldots\}$ in G.

Proposition

The elements $x^n, y^2, xyxy$ form a set of defining relations for the dihedral group.

Proposition

Let N be a normal subgroup of G, let $\overline{G} = G/N$, and let π be the canonical map $G \to \overline{G}$ defined by $\pi(a) = \overline{a} = aN$. Let $\varphi : G \to G'$ be a homomorphism whose kernel contains N. There is a unique homomorphism $\overline{\varphi} : \overline{G} \to G'$ such that $\overline{\varphi}\pi = \varphi$:



This map is defined by the rule $\overline{\varphi}(\overline{a}) = \varphi(a)$.

Proposition

Let F be the free group on x, y and let N be the smallest normal subgroup generated by the commutator $xyx^{-1}y^{-1}$. The quotient group $G = F/N$ is abelian.

Outline

Finitely Generated Abelian Groups

Definition

Let **G** be an abelian group. **G** is finitely generated if there is a set $S = \{a_1, \ldots, a_n\} \subset \mathbf{G}$ such that every $a \in \mathbf{G}$ can be written

$$a = r_1 a_1 + \cdots + r_n a_n, r_n \in \mathbb{Z}.$$

S is called a generating set.

Example

Let n be a positive integer.

$$\mathbb{Z}^n = \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n \text{ copies}}.$$

The elements $e_i = (0, \ldots, 1, \ldots, 0)$, $i = 1 \ldots n$ is a generating set

Proposition

The abelian group **G** *is finitely generated if and only if it is a homomorphic image of some* $\mathbb{Z}^n$.

Proof. If **G** has a set of generators $S = \{a_1, \ldots, a_n\}$, to define a surjection from $\mathbb{Z}^n$ onto **G** it suffices to pick

$$\varphi : \mathbb{Z}^n \to \mathbf{G}, \quad \varphi(e_i) = a_i$$

and set

$$\varphi(r_1, \ldots, r_n) = \varphi(\sum r_i e_i) = \sum r_i a_i$$

This is a well-defined surjection.

Matter of Notation

- If **G** is abelian, we tend to use the additive notation: $a + b$ instead of ab, $-a$ instead of a^{-1} and 0 for the identity.
- If $\varphi : \mathbf{G} \to \mathbf{G}'$ is a surjective homomorphism we may write it

$$\mathbf{G} \xrightarrow{\varphi} \mathbf{G}' \to 0$$

- If $\varphi : \mathbf{G} \to \mathbf{G}'$ is an injective homomorphism we may write

$$0 \to \mathbf{G} \xrightarrow{\varphi} \mathbf{G}'$$

- If **H** is a subgroup [and all subgroups are normal], we have a SES [short exact sequence] of homomorphisms

$$0 \to \mathbf{H} \to \mathbf{G} \to \mathbf{G}/\mathbf{H} \to 0$$

Short Exact Sequence

It is a sequence of abelian groups and homomorphisms

$$0 \to A \xrightarrow{\mathbf{f}} B \xrightarrow{\mathbf{g}} C \to 0$$

$$\begin{aligned} \mathbf{f} &: \text{one-one} \\ \mathbf{g} &: \text{onto} \\ \text{image}\,\mathbf{f} &= \ker \mathbf{g} \end{aligned}$$

Free abelian group

Definition

G is a free abelian group if $\mathbf{G} \simeq \mathbb{Z}^n$ for some n.

Of course there are plenty of non-free f.g. abelian groups:

$$\mathbf{G} = \mathbb{Z}^3 \oplus \mathbb{Z}_8^2 \oplus \mathbb{Z}_9$$

Suppose φ is a surjection from $\mathbb{Z}^n = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$ onto **G**, $\varphi(e_i) = a_i \in \mathbf{G}$. If φ is not an isomorphism, the kernel **K** of φ is the subgroup of all n-tuples $(r_1, \ldots, r_n)$ such that

$$r_1 a_1 + \cdots + r_n a_n = 0.$$

Definition

K is called the subgroup of relations of **G**, or the subgroup of syzygies of **G**.

Proposition

The subgroup of relations of a f.g. abelian group is finitely generated.

Proof. **K** is a subgroup of $\mathbb{Z}^n$ for some n. The assertion will follow from:

Proposition

Each subgroup of $\mathbb{Z}^n$ can be generated by at most n elements.

Proof. Let us argue by induction on n. For $n = 1$ we know well.

- To simplify we just consider the case $n = 2$. Write $\mathbb{Z}^2 = \mathbb{Z}e_1 + \mathbb{Z}e_2$. Consider $\mathbf{K}_1 = \mathbf{K} \cap \mathbb{Z}e_1$. By induction $\mathbf{K}_1 = \mathbb{Z}\mathbf{a}_1 e_1$.
- Consider the projection mapping $\psi : \mathbb{Z}^2 \to \mathbb{Z}e_2$. The image of $\mathbf{K}$ is a subgroup $\mathbf{K}_2$ of $\mathbb{Z}e_2$, so $\psi(\mathbf{K}) = \mathbf{K}_2 = \mathbb{Z}\mathbf{a}_2 e_2$.
- $\mathbf{b}$ be an element of $\mathbf{K}$ so that $\psi(\mathbf{b}) = \mathbf{a}_2 e_2$.
- Claim: $\mathbf{K}$ is generated by $\{\mathbf{a}e_1, \mathbf{b}\}$

- For any $\mathbf{c} \in \mathbf{K}$, $\psi(\mathbf{c}) = s\mathbf{a}_2 e_2$. Thus

$$\psi(\mathbf{c} - s\mathbf{b}) = s\mathbf{a}_2 e_2 - s\mathbf{a}_2 e_2 = 0$$

- Therefore

$$\mathbf{c} - s\mathbf{b} \in \mathbb{Z}e_1 \cap \mathbf{K}$$

that is

$$\mathbf{c} - s\mathbf{b} = r\mathbf{a}_1 e_1$$

that proves the assertion.

Exercise

Exercise

If $\mathbf{G}$ *is an abelian group generated by n elements, then any subgroup* $\mathbf{H}$ *can be generated by n elements.*

Proof.

- By assumption there is a surjective homomorphism $\varphi : \mathbb{Z}^n \to \mathbf{G} \to 0$.
- Let $\mathbf{K} = \varphi^{-1}(\mathbf{H})$. It is clear that $\mathbf{K}$ is a subgroup of $\mathbb{Z}^n$. By the previous Proposition, $\mathbf{K}$ is generated by a set $\mathbf{b}_1, \ldots, \mathbf{b}_m$, $m \leq n$.
- It follows that $\mathbf{H}$ is generated by the set $\varphi(\mathbf{b}_1), \ldots, \varphi(\mathbf{b}_m)$.

Situation

Proposition

An abelian group **G**, *generated be n elements, is a homomorphic image of* $\mathbb{Z}^n = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n$ *modulo the subgroup* **K** *generated by m elements* ($m \leq n$)

$$\begin{aligned} \mathbf{b}_1 &= r_{1,1}e_1 + \cdots + r_{1,n}e_n \\ &\vdots \\ \mathbf{b}_m &= r_{m,1}e_1 + \cdots + r_{m,n}e_n \end{aligned}$$

Conversely, any $m \times n$ *matrix with entries in* $\mathbb{Z}$ *defines a f.g. abelian group.*

The matrix

$$\mathbf{A} = \begin{bmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & \ddots & \vdots \\ r_{m1} & \cdots & r_{mn} \end{bmatrix}$$

is associated to the basis $\{e_1, \ldots, e_n\}$ of $\mathbb{Z}^n$ and the generators $\{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$ of $\mathbf{K}$. We are going to change the two sets to make the quotient group $\mathbf{G} = \mathbb{Z}^n/\mathbf{K}$ look nice.

Restricted row/column operations

$$\mathbf{A} = \begin{bmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & \ddots & \vdots \\ r_{m1} & \cdots & r_{mn} \end{bmatrix}$$

What is the meaning of

- Interchange two rows
- Add to a row a multiple of another

Similarly

- Interchange two columns
- Add to a column a multiple of another

Consider elementary row operations on **A**, with the exception of dividing a row or column by a non-unit of $\mathbb{Z}$.

- For example, adding c times the first row to the second, has the effect of replacing the generator $\mathbf{b}_2 \rightarrow \mathbf{b}_2 + c\mathbf{b}_1$, which does not change **K**. Similar effects for the other row operators.

- The interpretations of the column operations is the usual. For example, adding d times column 1, c_1, to column $c_2 \rightarrow c_2 + dc_1$, gives the representations of the vectors $\mathbf{b}_i$ in terms of the basis $\{e_1' = e_1 - de_2, e_2, e_3, \ldots, e_n\}$.

Example

$$\begin{bmatrix} 2 & 4 & 6 \\ 5 & 3 & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} 2 & 0 & 0 \\ 5 & -7 & -15 \end{bmatrix} \longrightarrow \begin{bmatrix} 2 & 0 & 0 \\ 1 & -7 & -15 \end{bmatrix}$$

$$\begin{bmatrix} 1 & -7 & -15 \\ 0 & 14 & 30 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 14 & 30 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix}$$

Key Theorem

Proposition

Given a matrix $\mathbf{A}$ *with entries in* $\mathbb{Z}$*, there exists a sequence of elementary row and column operations such that*

$$\mathbf{A} \rightsquigarrow \begin{bmatrix} d_1 & 0 & 0 & \cdots & 0 \\ 0 & d_2 & 0 & \cdots & 0 \\ 0 & 0 & d_3 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{bmatrix}$$

where $d_1 | d_2 | d_3 | \cdots$ *. Furthermore, the ideals* (d_i) *are unique.*

Proof

1. We induct on the size of the matrix **A**.
2. The proof of termination comes from the fact that the division algorithm of $\mathbb{Z}$ can place the gcd d_1 of all the entries of **A** in the position $(1, 1)$.
3. Now row and column operations are performed so that combined with those in step (1) give

$$\mathbf{A} \rightsquigarrow \mathbf{A}' = \begin{bmatrix} d_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \mathbf{B} & \\ 0 & & & \end{bmatrix}$$

4. This also shows that $d_1 | d_2 | d_3 | \cdots$.

Uniqueness

The uniqueness of the (d_i) comes from an additional observation.

1. The uniqueness of (d_1) comes directly from the construction.
2. To prove that of (d_2), we prove that $(d_1 d_2)$ is unique. This follows from the fact that just as every elementary operation leaves unchanged the gcd of the entries of the matrix, it also leaves unchanged the gcd of all 2×2 minors of $\mathbf{A}$ (or, more generally, of all $r \times r$ minors).

Structure Theorem for Finitely Generated Abelian Groups

What we have thus far:

- Start with an abelian group **G** given as a quotient $\mathbf{G} = \mathbb{Z}^n/\mathbf{K}$, where $\{e_1, \ldots, e_n\}$ is a basis of $\mathbb{Z}^n$ and **K** is generated by a set $\mathbf{b}_j = r_{1j}e_1 + \cdots + r_{nj}e_n$, $j \leq n$.

- There is a basis $f_1, f_2, \ldots, f_n$ of $\mathbb{Z}^n$, and a set of generators of **K**,

$$d_1 f_1, d_2 f_2, \ldots, d_n f_n, \quad d_1 | d_2 | \cdots .$$

- This implies

  $$\mathbf{G} \simeq (\mathbb{Z}e_1/d_1\mathbb{Z}e_1)\oplus\cdots\oplus(\mathbb{Z}e_n/d_n\mathbb{Z}e_n) \simeq \mathbb{Z}/(d_1)\oplus\cdots\oplus\mathbb{Z}/(d_n).$$

- Some of the $d_i = 1$, and $\mathbb{Z}/(d_i) = 0$, or $d_i = 0$, and $\mathbb{Z}/(d_i) \simeq \mathbb{Z}$.

Example

$$\begin{bmatrix} 2 & 4 & 6 \\ 5 & 3 & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix}$$

$$\mathbf{G} \simeq \mathbb{Z}f_1 + \mathbb{Z}f_2 + \mathbb{Z}f_3/\mathbb{Z}f_1 + \mathbb{Z}2f_2$$

$$\mathbf{G} \simeq \mathbb{Z}f_2/\mathbb{Z}2f_2 \oplus \mathbb{Z}f_3 \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}$$

Theorem

Every finitely generated abelian group **G** *is isomorphic to*

$$\mathbb{Z}/(d_1) \oplus \cdots \oplus \mathbb{Z}/(d_n),$$

where $d_1|d_2|d_3|\cdots$. *The ideals* (d_i) *are uniquely determined, in particular the number* r *of* $d_i = 0$, *is uniquely determined (called torsionfree rank of* $\mathbb{Z}$*),*

$$\mathbb{Z} \simeq R^r \oplus T,$$

where T *is a finite subgroup. The ideals* (d_i) *are called the rational invariants of* **G**.

Corollary

Every finite abelian group $\mathbf{G}$ *is a direct sum of cyclic groups, more precisely*

$$\mathbf{G} \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r}, \quad 1 < d_1 | d_2 | \cdots | d_r.$$

Observe that for any $s \in \mathbf{G}$, $d_r s = 0$, that is d_r is the highest order of all $s \in \mathbf{G}$.

Exercise

Let **F** be a field and **G** be a finite set of nonzero elements of **F** forming a group under multiplication.

Proposition

G *is a cyclic group.*

G is a finite abelian group therefore

$$\mathbf{G} \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r}, \quad d_1 | d_2 | \cdots | d_r.$$

This means that all elements of **G** satisfy the equation $x^{d_r} - 1 = 0$. But this equation has at most d_r roots, while $|\mathbf{G}| = d_1 \cdots d_r$. So $r = 1$.

Outline

Homework #9

Do 4 Problems.

1. Compute the order of $GL_n(\mathbb{F}_p)$. [Done in class for $n = 2$]
2. Find all subgroups of order 4 of S_4. Which are normal?
3. Let **G** be a group of order 30. Prove that either the Sylow 5-subgroup **K** or the 3-Sylow group **H** is normal.
4. What is the highest order of an element in S_{11}?
5. Find a direct sum of cyclic group which is isomorphic to the abelian group presented by the matrix $\begin{bmatrix} 2 & 2 & 2 \\ 2 & 2 & 0 \\ 2 & 0 & 2 \end{bmatrix}$.