

Math 551 – Algebra – Fall 2000

A. Groups

2. Group Actions

The close connection between groups and permutations is captured in the fundamental idea of group actions. Groups are important because they act on things.

Definition. Let G be a group and Ω a set. A (group) action of G on Ω is a mapping

$$G \times \Omega \rightarrow \Omega, (g, \omega) \mapsto g\omega,$$

such that

- 1) $1\omega = \omega$ for all $\omega \in \Omega$;
- 2) $g(h\omega) = (gh)\omega$ for all $g, h \in G$ and all $\omega \in \Omega$.

We could add the property:

- 3) $g\omega = \omega' \iff g^{-1}\omega' = \omega$, but it is redundant. The second equation follows from the first by applying g^{-1} to both sides and using the above properties; the first follows from the second by applying g to both sides.

Notice that for fixed $g \in G$, there is the mapping $\ell_g : \Omega \rightarrow \Omega$ given by $\ell_g(\omega) = g\omega$. The axioms are that $\ell_1 = id_\Omega$ and $\ell_g\ell_h = \ell_{gh}$. In particular $\ell_g\ell_{g^{-1}} = \ell_{g^{-1}g} = \ell_1 = id_\Omega$, and so

Each ℓ_g is a permutation of Ω , i.e. a bijection from Ω to Ω .

Some important examples of group actions follow.

Ex. A. Let $G \leq \Sigma_\Omega$. Then G acts on Ω via $\sigma\omega = \sigma(\omega)$.

Ex. B. Let G be a group. Then G acts on itself via $gh = gh$. This is the “left regular” action of G . There is also a “right regular” action, defined by $gh = hg^{-1}$. (The “products” on the left are the results of the action of a group element g on a set element h ; on the right, the products are from the multiplication in G .)

2a. Cosets; classification of transitive actions; counting principle

Ex. C. Let G be a group and H a subgroup of G . We define an equivalence relation \sim_H on G as follows:

$$a \sim_H b \iff a^{-1}b \in H.$$

The facts that $1 \in H$, H is closed under inversion, and H is closed under multiplication translate directly into the reflexivity, symmetry and transitivity of \sim_H . (Check this!) The equivalence classes of G are called the left cosets of H in G , and the set of all left cosets of G is denoted G/H . It is a partition of G , as is the set of equivalence classes for any equivalence relation. The cardinality of G/H is the “index” of H in G and is written $|G : H|$. Thus by definition, $|G : H| = |G/H|$.

Lemma. *The left coset of H containing the element $a \in G$ is the set $aH = \{ah \mid h \in H\}$. Moreover $|H| = |aH|$ for any $a \in G$.*

Proof. If $a \sim_H b$, then $b = a(a^{-1}b) \in aH$. Conversely if $b \in aH$, then $b = ah$ for some $h \in H$, and $a^{-1}b = h$, so $a \sim_H b$. Finally the mapping $h \mapsto ah$ is a bijection between H and aH . □

Lagrange’s Theorem. *If $H \leq G$, then $|G| = |H||G : H|$. If G is finite, then $|G : H| = |G|/|H|$.*

The first statement is actually true even if G is infinite, with cardinal multiplication. In any case for G finite, it is a trivial consequence of the previous lemma.

Corollary. *If $H \leq G$ and G is finite, then $|H|$ divides $|G|$.*

Corollary. *If $g \in G$ and G is finite, then $|g|$ divides $|G|$.*

Corollary. *A group of prime order is cyclic.*

Proof. Let G have order p and choose $g \in G$ with $g \neq 1$. Then $|g| > 1$, so $|g| = p$ by the previous corollary, and hence $|\langle g \rangle| = p$. Therefore $G = \langle g \rangle$. □

Given H , the equivalence relation \sim_H is “preserved” by the left regular action of G :

$$\forall a, b \in G, a \sim_H b \iff ga \sim_H gb.$$

This is trivial as $(ga)^{-1}(gb) = a^{-1}g^{-1}gb = a^{-1}b$. Hence the left regular action of G must permute the equivalence classes, and thus induces an action of G on G/H , via

$$g(aH) = (ga)H.$$

Definition. *A group action of G on Ω is transitive if and only if for every $\omega, \omega' \in \Omega$ there exists $g \in G$ such that $g\omega = \omega'$.*

Proposition. *If $H \leq G$, then the action of G on G/H defined above is transitive.*

Proof. $(g(g')^{-1})g'H = gH$. □

Theorem. (Classification of transitive actions) Suppose that G acts transitively on Ω . Let $\omega \in \Omega$ and set $G_\omega = \{g \in G \mid g\omega = \omega\}$. Then

- 1) $G_\omega \leq G$.
- 2) There exists a bijection $\phi : G/G_\omega \rightarrow \Omega$ such that $\phi(G_\omega) = \omega$ and for every $g \in G$ and $\Gamma \in G/G_\omega$,

$$\phi(g\Gamma) = g\phi(\Gamma).$$

Thus the actions of G on G/G_ω and Ω are “isomorphic”.

Proof. If $g\omega = \omega = h\omega$, then $(gh)\omega = g(h\omega) = g\omega = \omega$, and also $g^{-1}\omega = g^{-1}(g\omega) = (g^{-1}g)\omega = 1\omega = \omega$. This proves 1).

Define $\Phi : G \rightarrow \Omega$ by $\Phi(g) = g\omega$. The transitive action of G on Ω implies that Φ is surjective. For any $g, h \in G$,

$$\Phi(g) = \Phi(h) \iff g\omega = h\omega \iff h^{-1}g\omega = \omega \iff h^{-1}g \in G_\omega \iff g \sim_{G_\omega} h.$$

So the fibers of Φ are the left cosets of G_ω . Therefore Φ induces an injective mapping $\phi : G/G_\omega \rightarrow \Omega$ such that $\phi(gG_\omega) = \Phi(g) = g\omega$. Since Φ is surjective, so is ϕ , so ϕ is a bijection. Finally for any $\Gamma = hG_\omega \in G/G_\omega$ we have

$$\phi(g\Gamma) = \phi(g(hG_\omega)) = \phi((gh)G_\omega) = (gh)\omega = g(h\omega) = g\phi(hG_\omega),$$

completing the proof.

Corollary. (The counting principle, transitive case) Let G act transitively on Ω . Then for any $\omega \in \Omega$,

$$|\Omega| = |G : G_\omega|.$$

Ex. C. Let I be a regular icosahedron and $G = \text{Aut}(I)$, the group of all its symmetries. Then G acts on I , and in particular on the set Ω of the 12 vertices of I . The action is clearly transitive. The stabilizer G_ω of a particular vertex ω contains 5 rotations and 5 reflections, which permute the 5 faces containing ω in the manner D_{10} permutes the 5 vertices of a regular pentagon. Therefore $|G| = |G_\omega||I| = 10 \cdot 12 = 120$.

A corollary of the counting principle is that $|G_\omega| = |G_{\omega'}|$ for any $\omega, \omega' \in \Omega$ (in the case of transitive actions). In fact more is true: $G_\omega \cong G_{\omega'}$. In fact more is true: G_ω and $G_{\omega'}$ are conjugate.

Definition. Let G be a group and $g, x \in G$. Then ${}^g x = gxg^{-1}$. The elements x and y of G are conjugate in G if and only if $y = {}^g x$ for some $g \in G$.

Conjugation has the following important properties for all $x, g, h \in G$:

- 1) ${}^1 x = x$.
- 2) ${}^g ({}^h x) = {}^{gh} x$.

In other words, G acts on itself by conjugation. (The action is not transitive unless $G = \{1\}$, since ${}^g 1 = 1$ for all $g \in G$.) Moreover,

- 3) ${}^g(xy) = {}^g x {}^g y$ for all $g, x, y \in G$. This is easily verified, and so for fixed $g \in G$, the mapping

$$\text{Int}(g) : G \rightarrow G \text{ defined by } \text{Int}(g)(x) = {}^g x$$

is an automorphism of G (we saw above that it is a bijection as a consequence of the group action properties). It is called the inner automorphism of G determined by g . Two elements, subsets or subgroups A, B of G are said to be conjugate in G if and only if $\text{Int}(g)(A) = B$ for some $g \in G$. If A and B are subgroups, then the restriction $\text{Int}(g)|_A$ is a bijection between A and B which is multiplicative, and so is an isomorphism between A and B . In particular

Conjugate subgroups are isomorphic.

Conjugation gives lots of examples of transitive actions. Let X be a subset (such as a subgroup) of G and let $\Omega = \{{}^g X \mid g \in G\}$ be the set of all G -conjugates of X . Then G acts on Ω by conjugation: $g {}^h X = {}^{gh} X$. We define $N_G(X) = \{g \in G \mid {}^g X = X\}$. This is the stabilizer in G of the element $X \in \Omega$. Thus the counting principle yields:

Corollary. *Let G be a group and X a subset of G . Then $N_G(X)$ is a subgroup of G and the number of distinct G -conjugates of X is $|G : N_G(X)|$.*

Taking X to be a singleton $X = \{x\}$, we see that $N_G(X)$ is the set of all elements of G which commute with x . This is called $C_G(x)$, the centralizer of x in G .

Corollary. *Let G be a group and $x \in G$. Then $C_G(x)$ is a subgroup of G and the number of distinct G -conjugates of x is $|G : C_G(x)|$.*

Returning to a transitive action of G on Ω , let $\omega, \omega' \in \Omega$. Write $\omega' = g\omega$ for some $g \in G$. Then for any $h \in G$,

$$h\omega' = \omega' \iff hg\omega = g\omega \iff g^{-1}hg\omega = \omega \iff g^{-1}hg \in G_\omega \iff h \in gG_\omega g^{-1}.$$

That is,

$$G_{g\omega} = {}^g G_\omega.$$

Now we consider not necessarily transitive actions. Let G act on Ω . Define a relation \equiv on Ω by

$$\omega \equiv \omega' \iff \exists g \in G \text{ such that } g\omega = \omega'.$$

By properties 1), 2) and 3) in the definition of group action, this relation is reflexive, transitive and symmetric. So it is an equivalence relation. The equivalence classes are called **orbits**, more precisely the G -orbits on Ω . Notice that G acts transitively on each orbit.

Theorem. (Counting principle, general case) Let G act on Ω . Let the set of orbits be $\{\Omega_i \mid i \in I\}$ and choose for each $i \in I$ an element $\omega_i \in \Omega_i$. Then

$$|\Omega| = \sum_i |G : G_{\omega_i}|.$$

Proof. $|\Omega| = \sum_i |\Omega_i| = \sum_i |G : G_{\omega_i}|$, the first since the orbits partition Ω , and the second by the transitive case of the counting principle.

2b. Class equation of a finite group; actions of groups of prime power order

An interesting application is the “class equation” of a group. Let G be any group, and consider G to act on itself by conjugation. The action is certainly not transitive (unless $G = 1$), since $\{1\}$ is an orbit. The orbits of this action are called the **conjugacy classes** of G . If C is a conjugacy class and $x \in C$ then $|C| = |G : C_G(x)|$ by the previous corollary. Thus if we choose a set of representatives $\{g_i \mid i \in I\}$ for the conjugacy classes (i.e., a subset of G which consists of one element from each conjugacy class), the counting principle yields

$$|G| = \sum_{i \in I} |G : C_G(g_i)|.$$

It is customary to separate out the terms in this sum which are equal to 1; i.e., those for which $C_G(g_i) = G$. This condition is equivalent to g_i not having any conjugates in G other than itself, which is equivalent to $g_i x = x g_i$ for all $x \in G$. The center of G is defined by

$$Z(G) = \{g \in G \mid gx = xg \forall x \in G\},$$

and so consists of the elements contributing 1 to the sum above. We have proved

Theorem. (The Class Equation) Let G be a finite group. Then

$$|G| = |Z(G)| + \sum_j |G : C_G(g_j)|,$$

where the sum is over a set of representatives for all the conjugacy classes of G except those in $Z(G)$, and thus $|G : C_G(g_j)| > 1$ for each term in the sum.

Proposition. For any G , $Z(G) \leq G$.

Proof. Left to reader. QED

The class equation has important consequences for finite groups; one cute one is the following:

Theorem. Let G be a group such that $|G|$ is a positive power of a prime. Then $Z(G) \neq \{1\}$.

Proof. Let p be the prime. In the class equation, $|G|$ as well as each term $|G : C_G(g_j)|$ is a positive power of p , by Lagrange's Theorem. Therefore $|Z(G)| \equiv 0 \pmod{p}$. Certainly $1 \in Z(G)$ so $|Z(G)| \geq p$. □

Before giving an application of this we observe that virtually the same argument proves the following:

Theorem. Let G be a finite group of order p^a , p a prime, and suppose that G acts on the finite set Ω . Define $\text{Fix}_\Omega(G) = \{\omega \in \Omega \mid g\omega = \omega \ \forall g \in G\}$. Then

$$|\text{Fix}_\Omega(G)| \equiv |\Omega| \pmod{p}.$$

□

Now for an application:

Corollary. Let G be a group whose order is p^2 , p a prime. Then G is abelian (and is isomorphic either to $Z_p \times Z_p$ or to Z_{p^2}).

Proof. We prove that G is abelian, i.e., $Z(G) = G$, and leave the rest as an exercise. Assume by way of contradiction that $Z(G) < G$. We can choose $g \in Z(G)$ with $g \neq 1$ by the theorem, and choose $h \in G - Z(G)$. Then $|\langle g \rangle| = p$ and as $\langle g, h \rangle$ properly contains $\langle g \rangle$ and has order which divides p^2 ,

$$G = \langle g, h \rangle.$$

But $gh = hg$ and it quickly follows that any word in g and h commutes with any other, so that G is abelian. □

2c. Sylow's Theorem

Here is another interesting consequence, a "baby Sylow theorem":

Theorem. Let G be a finite group, and let p be a prime divisor of $|G|$. Then G possesses an element of order p .

Proof. Define

$$\Omega = \{(g_1, g_2, \dots, g_p) \mid g_i \in G \ \forall i = 1, \dots, p \text{ and } g_1 g_2 \cdots g_p = 1\}.$$

Notice that this condition is equivalent to

$$g_p = (g_1 \cdots g_{p-1})^{-1},$$

and so for each $g_1, \dots, g_{p-1} \in G$, there is a unique p -tuple in Ω starting with g_1, \dots, g_{p-1} . Therefore

$$|\Omega| = |G|^{p-1}.$$

Now let $H = \langle h \rangle$ be a cyclic group of order p , and let H act on Ω by $h^i(g_1, g_2, \dots, g_p) = (g_{i+1}, g_{i+2}, \dots, g_{i+p})$, where we interpret subscripts as having been reduced to their residue modulo p in the range between 1 and p . It is easy to check that this defines an action of H on Ω . Therefore by the previous theorem,

$$\text{Fix}_{\Omega}(H) \equiv |\Omega| = |G|^{p-1} \equiv 0 \pmod{p}.$$

Notice that $(1, 1, \dots, 1)$ is a fixed point of H , and so there exists another fixed point (z_1, z_2, \dots, z_p) . Since this point is fixed, we have $z_1 = z_2 = \dots = z_p$. Therefore $z_1 \neq 1$, and the definition of Ω yields $z_1^p = 1$. QED

We can even almost prove the full version of Sylow's Theorem. The proof we shall give is old—it is very close to Sylow's original proof—and I think that it's still the best.

Sylow's Theorem. (unusual version) *Let G be a finite group and let p be a prime. Let $\mathcal{P}(G)$ be the set of all subgroups of G whose cardinality is a power of p and which are maximal with this property with respect to inclusion. Then the following hold:*

- 1) Write $|G| = p^m b$ with p not dividing b . Then $|P| = p^m$ for every $P \in \mathcal{P}(G)$.
- 2) Any two elements of $\mathcal{P}(G)$ are conjugate.
- 3) $|\mathcal{P}(G)| \equiv 1 \pmod{p}$.
- 4) For any $P \in \mathcal{P}(G)$, $|\mathcal{P}(G)| = |G : N_G(P)|$.

Here the criterion for a subgroup P to belong to $\mathcal{P}(G)$ is that $|P|$ is a power of p , and whenever $P \leq Q \leq G$ with $|Q|$ also a power of p , then $P = Q$. Thus if a is the largest integer such that G has a subgroup of order p^a , then every subgroup of G of order p^a lies in $\mathcal{P}(G)$. It is possible *a priori* that some smaller subgroups also lie in $\mathcal{P}(G)$. But in any case, since G has subgroups whose order is a power of p (e.g., the trivial subgroup), it is obvious that

$$\mathcal{P}(G) \neq \emptyset.$$

Sylow's Theorem. (usual version) *Let G be a finite group, p a prime, and write $|G| = p^m b$ with p not dividing b . Let $\text{Syl}_p(G)$ be the set of subgroups of G of cardinality p^m . The the following hold:*

- 1) $\text{Syl}_p(G)$ is not empty.
- 2) Any two elements of $\text{Syl}_p(G)$ are conjugate.
- 3) $|\text{Syl}_p(G)| \equiv 1 \pmod{p}$.
- 4) For any $P \in \text{Syl}_p(G)$, $|\text{Syl}_p(G)| = |G : N_G(P)|$.
- 5) Any subgroup of G whose order is a power of p lies in some element of $\text{Syl}_p(G)$.

Lemma. *The unusual version implies the usual version.*

Proof. The unusual 1) implies that $\mathcal{P}(G) \subseteq \text{Syl}_p(G)$. But also if $P \in \text{Syl}_p(G)$ and $P \leq Q \leq G$ with $|Q|$ a power of p , then $|Q| \leq |P|$ by Lagrange's Theorem so $P = Q$. Therefore

$$\mathcal{P}(G) = \text{Syl}_p(G).$$

Now 1), 2), 3) and 4) are immediate. In 5), if $R \leq G$ with $|R|$ a power of p , then there exist subgroups $Q \leq G$ such that $R \leq Q \leq G$ and $|Q|$ is a power of p (namely, R itself is such a subgroup). Choosing such a Q of largest order, we find that $Q \in \mathcal{P}(G)$. Hence $Q \in \text{Syl}_p(G)$ and 5) holds. \square

We shall prove 2), 3) and 4) of the unusual version now. For 1) we need a teeny bit more; but we shall present the argument anyhow, and it will be valid once we have proved the necessary extra (the third isomorphism theorem).

First, if $g \in G$ and $P \in \mathcal{P}(G)$, then ${}^gP \in \mathcal{P}(G)$. For conjugation by g is an automorphism of G , so preserves the cardinality and inclusion relation among subgroups. So

G acts on $\mathcal{P}(G)$ by conjugation.

The following lemma will allow us to use the counting principle effectively.

Lemma. *Let $P \in \mathcal{P}(G)$. Then $\text{Fix}_{\mathcal{P}(G)}(P) = \{P\}$.*

Proof. Of course ${}^gP = P$ for all $g \in P$ as P is a subgroup of G . So P is a fixed point. Now let $Q \in \mathcal{P}(G)$ be such that ${}^gQ = Q$ for all $g \in P$. We must prove that $Q = P$. To do this it is enough to show that $PQ = \{xy \mid x \in P, y \in Q\}$ is a subgroup of G whose order is a power of p . For then $P \leq PQ \leq Q$ so by the definition of $\mathcal{P}(G)$, $P = PQ = Q$.

To see that PQ is a subgroup of G , notice that $gQg^{-1} = Q$ for all $g \in P$, so $gQ = Qg$ for all $g \in P$. Therefore $PQ = QP$. It follows that $(PQ)(PQ) = P(QP)Q = P(PQ)Q = PPQQ = PQ$ and $(PQ)^{-1} = Q^{-1}P^{-1} = QP = PQ$, so PQ is indeed a subgroup. Moreover every element of PQ may be written xy , $x \in P$, $y \in Q$, and $xy = x'y' \iff x^{-1}x' = y(y')^{-1} \in P \cap Q$. So each element of $h \in P \cap Q$ gives a way to vary xy to another representation $(xh)(h^{-1}y)$ of the same element. Consequently xy can be represented exactly $|P \cap Q|$ ways as a product of an element of P and one of Q , so

$$|PQ| = |P||Q|/|P \cap Q| = |P : P \cap Q||Q|,$$

a power of p as required. \square

Exercise. *For any subsets X and Y of a group G , define $XY = \{xy \mid x \in X, y \in Y\}$, and also define $X^{-1} = \{x^{-1} \mid x \in X\}$. Suppose now that X and Y are subgroups of G . Show that*

- 1) $XY \leq G$ if and only if $XY = YX$.
- 2) $|XY| = |X||Y|/|X \cap Y|$.

Proof of 2). Let P and Q belong to $\mathcal{P}(G)$. Since G acts on $\mathcal{P}(G)$ there is an orbit \mathcal{O}_P of G on $\mathcal{P}(G)$ containing P . If $Q \in \mathcal{O}_P$, then P and Q are G -conjugate. So assume by way of contradiction that $Q \notin \mathcal{O}_P$.

Now G acts on \mathcal{O}_P , so P and Q both do. Since \mathcal{O}_P contains P but not Q , P has a unique fixed point on \mathcal{O}_P but Q has none. Therefore

$$1 = |\text{Fix}_{\mathcal{O}_P}(P)| \equiv |\mathcal{O}_P| \equiv |\text{Fix}_{\mathcal{O}_P}(Q)| = 0 \pmod{p},$$

a contradiction.

Proof of 3). Since G acts on $\mathcal{P}(G)$, so does P . Then

$$|\mathcal{P}(G)| \equiv |\text{Fix}_{\mathcal{P}(G)}(P)| = 1 \pmod{p}$$

by the lemma.

Proof of 4). This is immediate from 2) and the transitive version of the counting principle.

Almost-Proof of 1). The proof is by induction on $|G|$. If $|G| = 1$, the result is trivially true! In general, choose $P \in \mathcal{P}(G)$; our task is to prove that $|G : P|$ is not divisible by p . Now $|G : N_G(P)| \equiv 1 \pmod{p}$, and in particular $|G : N_G(P)|$ is not divisible by p . Since P is maximal among subgroups of G of order a power of p , and $P \leq N_G(P)$, certainly P is maximal among subgroups of $N_G(P)$ whose order is a power of p . Hence $P \in \mathcal{P}(N_G(P))$. If $N_G(P) \neq G$, then by induction, $|N_G(P) : P|$ is not divisible by p . But $|G : P| = |G : N_G(P)| |N_G(P) : P|$ is then not divisible by p , as required. So we may assume that $N_G(P) = G$.

In terminology below, this means that $P \triangleleft G$. We can therefore form the group G/P , and assume that the order of this quotient group is divisible by p , and derive a contradiction to the maximality of P . By the little Sylow theorem above, G/P has a subgroup of order p . By the third isomorphism theorem below, this subgroup has the form R/P for some subgroup $R \leq G$ with $P \leq R$. But then $|R : P| = p$, so $|R| = p|P|$ and $R \geq P$, contradicting the maximality of P . QED

This unassuming result is unmatched for power in all of finite group theory.

As an example of its use we show:

Proposition. *There two isomorphism types of groups of cardinality 6, namely Z_6 and Σ_3 .*

Proof. These two groups of order 6 are not isomorphic since Z_6 is abelian and Σ_3 is not. Now let G be any group of order 6. We must show that either $G \cong Z_6$ or $G \cong \Sigma_3$.

Let $P \in \text{Syl}_3(G)$. By Sylow's theorem the number of Sylow 3-subgroups is $|G : N_G(P)|$, which divides $|G : P| = 2$ and is congruent to $1 \pmod{3}$. Therefore P is the unique Sylow 3-subgroup, so ${}^gP = P$ for all $g \in G$. We have $P = \langle x \rangle$ for some $x \in G$ of order 3.

Likewise by Sylow's Theorem there exists $y \in G$ of order 2. Then $\langle x \rangle \cap \langle y \rangle$ is a subgroup whose order divides both 2 and 3, so $\langle x \rangle \cap \langle y \rangle = 1$.

If $xy = yx$, then $(xy)^n = x^n y^n$ can equal 1 only if $x^n = y^{-n} \in \langle x \rangle \cap \langle y \rangle = 1$, which occurs only if n is divisible both by 3 and by 2, i.e., xy has order 6. In this case $G = \langle xy \rangle \cong Z_6$.

Suppose then that $xy \neq yx$. Then $xyx^{-1} \in \langle x \rangle$ but $xyx^{-1} \neq x$ (and of course $xyx^{-1} \neq 1$ as $x \neq 1$). Therefore $xyx^{-1} = x^{-1}$. We therefore know that

$$x^3 = 1, \quad y^2 = 1 \quad \text{and} \quad yxy^{-1} = x^2 = x^{-1}.$$

But we showed above that the symmetry group D_6 of an equilateral triangle a) has elements σ and τ satisfying the same relations and b) as a result of these relations and nothing else, can be shown to consist of the elements $\tau^i \sigma^j$, $0 \leq i \leq 1$, $0 \leq j \leq 2$, and have a uniquely determined multiplication table. Therefore $G \cong D_6$. In particular taking $G = \Sigma_3$, a noncyclic group of order 6, we have $\Sigma_3 \cong D_6$. QED

Corollary. *Let G be a group of order pq , where $p > q$ are primes. If $p \not\equiv 1 \pmod{q}$, then $G \cong Z_{pq}$.*

Proof. By Sylow's Theorem the number of Sylow p -subgroups divides q and is congruent to 1 mod p , so is 1 as $p > q$. Likewise using the hypothesis that $p \not\equiv 1 \pmod{q}$ we find that G has a unique Sylow q -subgroup. Let P and Q be these Sylow subgroups. Then ${}^g P = P$ for every $g \in G$ and similarly for Q . In particular, for any $x \in P$ and $y \in Q$ we have

$$xyx^{-1}y^{-1} = {}^x yy^{-1} \in Q \quad \text{and} \quad xyx^{-1}y^{-1} = x^y x^{-1} \in P.$$

But $P \cap Q = 1$ by Lagrange's Theorem (its order divides both p and q). Therefore $xyx^{-1}y^{-1} = 1$. This implies that $xy = yx$. Consequently, as in the previous corollary we find that xy has order pq , so $G \cong Z_{pq}$. QED

2d. Finite Symmetric Groups

Examples illustrating the previous results can be found in the symmetric groups. We introduce some standard notation for them, beginning with the "product of cycles" notation for permutations. The notation

$$(12357)(46)$$

for example refers to the permutation in Σ_7 taking 1 to 2, 2 to 3, 3 to 5, 5 to 7, and 7 to 1, and interchanging 4 and 6. Such notation is possible for any permutation in any symmetric group. We shall prove this intuitively obvious fact since in doing so we pass by some other useful concepts.

Let $g \in \Sigma_\Omega$. *Let Ω_1 be an orbit of $\langle g \rangle$ on Ω , and suppose that $|\Omega_1| = n$. Then for any $\omega \in \Omega_1$, we have*

$$\Omega_1 = \{\omega, g\omega, g^2\omega, \dots, g^{n-1}\omega\}.$$

Proof. For any $\alpha \in \Omega$, $\alpha = g^i \omega$ for some i , by transitivity. Moreover $\alpha = g^j \omega$ if and only if $g^{i-j} \in \langle g \rangle_\omega$. Now $G_\omega = \langle g^n \rangle$ for some n , and we may assume that n is the least positive integer with this property. Then we may write $\alpha = g^i \omega$ with $0 \leq i < n$, and different such i give different g 's.

Alternatively we may quote the classification of transitive actions, which says that there is a bijection $\Omega_1 \rightarrow \langle g \rangle / \langle g \rangle_\omega$ preserving the action of $\langle g \rangle$ and mapping ω to the trivial coset $\langle g \rangle_\omega$. Writing $G_\omega = \langle g^n \rangle$ with n again the least such positive integer, we see that $1, g, g^2, \dots, g^{n-1}$ represent the left cosets of $\langle g \rangle$. This implies the result. \square

We write $g|\Omega_1$ as the “ n -cycle”

$$g|\Omega_1 = (\omega g\omega, g^2\omega, \dots, g^{n-1}\omega). \quad 2A$$

Definition. A permutation $g \in \Sigma_\Omega$ is a cycle if and only if $\langle g \rangle$ has one orbit Ω_1 on which it acts by (2A), with $n > 1$, and g fixes every point of $\Omega - \Omega_1$.

Thus we do not consider the identity permutation to be a cycle.

We may use the same notation for the cycle g , with the convention that points of Ω omitted in this symbolism are fixed by g .

Definition. Two permutations $g, g' \in \Sigma_\Omega$ are disjoint if and only if each point of Ω is fixed by at least one of them.

Lemma. If g and g' are disjoint permutations then $gg' = g'g$, and points in the support of g are moved by gg' just as they are moved by g .

Proof. Left to reader. \square

Now we can prove

Theorem. Let $g \in \Sigma_\Omega$, with Ω finite. Then there exist uniquely determined disjoint cycles g_1, \dots, g_r (except for their order) such that $g = g_1 \dots g_r$.

Proof. Let $\Omega_1, \dots, \Omega_r$ be the nontrivial orbits of $\langle g \rangle$ on Ω , and let g_i be the permutation which agrees with g on Ω_i and acts trivially on all other Ω_j . Then g_i is a cycle by the first lemma, the g_i are obviously disjoint and $g = g_1 \dots g_r$. Conversely if $g = h_1 \dots h_s$, disjoint cycles, and we let Ω'_i be the nontrivial orbit of h_i on Ω , then it is clear that the Ω'_i are the nontrivial orbits of g on Ω , so that by reordering we have $r = s$ and $\Omega_i = \Omega'_i$. Then $h_i = g|\Omega_i = g_i$. \square

Lemma. The order of an n -cycle is n . If $g = g_1 \dots g_r$ as in the previous theorem, with g_i being an n_i -cycle, then the order of g is the l.c.m. of n_1, \dots, n_r . \square

Theorem. Two elements of Σ_Ω , Ω finite, are conjugate in Σ_Ω if and only if they have the same cycle shape.

Proof. If $h\alpha = \beta$, then $ghg^{-1}(g\alpha) = g\beta$. Hence if $h = (\alpha\beta \dots)(\gamma\delta \dots) \dots$, then $ghg^{-1} = (g\alpha g\beta \dots)(g\gamma g\delta \dots) \dots$. So conjugate elements have the same cycle shape; conversely if two elements have the same cycle shape a permutation g exists carrying the points in one cycle shape to corresponding points in the other. \square

Now of the $3!$ elements of Σ_3 , there are 2 3-cycles, 3 2-cycles and 1 identity element.

Of the $4! = 24$ elements of Σ_4 , there are 6 4-cycles, 8 3-cycles, 6 2-cycles, 3 elements of the form $(ab)(cd)$, and one identity element. The last four elements constitute the “Klein four-subgroup $V = \{1, (12)(34), (13)(24), (14)(23)\}$ ”.

Of the $5! = 120$ elements of Σ_5 , there are 24 5-cycles, 30 4-cycles, 20 3-cycles, 10 2-cycles, 15 “Klein elements” $(ab)(cd)$, and 20 elements $(abc)(de)$ of order 6.

It is not possible systematically to enumerate the subgroups of Σ_n ; if this were possible we would know all finite groups, by Cayley’s Theorem. However, there are very few subgroups of very small index. Taking $\Omega = \{1, \dots, n\}$, we of course have the point-stabilizers $(\Sigma_\Omega)_\omega$, $\omega \in \Omega$; clearly this is isomorphic to $\Sigma_{\Omega - \{\omega\}}$ and its index is $|\Omega| = n$. The only other subgroup of index $\leq n$ is the alternating group A_Ω .

2-cycles are also called “transpositions”.

Theorem. *Let Ω be a finite set. Then every element $g \in \Sigma_\Omega$ is the product $g = t_1 \cdots t_r$ of (not necessarily disjoint) transpositions. This decomposition is not unique, nor is r . However, the parity of r is uniquely determined by g , and accordingly g is called even or odd, and the sign ϵ_g of g is defined as -1 or 1 .*

Proof. $(\alpha_1 \alpha_2 \cdots \alpha_r)(\alpha_r \alpha_{r+1}) = (\alpha_1 \alpha_2 \cdots \alpha_r \alpha_{r+1})$. Hence an inductive argument shows that every cycle is the product of transpositions. But every element of Σ_Ω is the product of cycles, proving the first statement.

For the uniqueness, a representation of $G = \Sigma_\Omega$ is the most useful way to proceed. Say $\Omega = \{1, \dots, n\}$. Let $R = \mathbf{Z}[x_1, \dots, x_n]$ be the polynomial ring in n (commuting) indeterminates x_1, \dots, x_n . The action of G on Ω yields an action of G on R :

$$\text{For } g \in G \text{ and } p \in R, \text{ define } (g \cdot p)(x_1, \dots, x_n) = p(x_{g^{-1}1}, \dots, x_{g^{-1}n}). \quad 2B$$

If we put $q = g \cdot p$, notice that $h \cdot (g \cdot p)(x_1, \dots) = (h \cdot q)(x_1, \dots, x_n) = q(x_{h^{-1}1}, \dots) = p(x_{g^{-1}h^{-1}1}, \dots) = (hg) \cdot p(x_1, \dots, x_n)$. (For $i = h^{-1}1$ gets replaced by $g^{-1}i = g^{-1}h^{-1}1$, etc.) Thus

$$h \cdot (g \cdot p) = (hg) \cdot p, \quad 2C$$

whence we really have an action. Moreover, the multiplication in R is respected by this action:

$$g \cdot (pq) = (g \cdot p)(g \cdot q), \quad 2D$$

where the products are in the ring R , i.e., ordinary multiplication of polynomials. This is clear from the definition of the action.

What has this to do with even and odd permutations? The polynomial ring R contains an element δ which “detects” evenness and oddness, namely

$$\delta(x_1, \dots, x_n) = \prod_{i < j} (x_i - x_j).$$

The key point is that if t is a transposition, then

$$t \cdot \delta = -\delta. \quad 2E$$

Indeed t permutes and changes the signs of the factors of δ , and so $t \cdot \delta = \pm\delta$, where the sign is determined by whether the phenomenon $i < j$ but $ti > tj$ occurs an even or odd number of times. But if t interchanges k and l with $k < l$, then this phenomenon occurs only if $i = k$ and $j = l$, or $i = k$ and $k < j < l$, or $j = l$ and $k < i < l$. This is an odd number of times, proving (2E).

Now (2C, D, E) imply that if g is the product of r transpositions, then

$$g\delta = (-1)^r \delta.$$

Thus we may define ϵ_g by $g\delta = \epsilon_g \delta$, and the proof is complete. \square

Definition. A_Ω is the subgroup of Σ_Ω consisting of all even permutations.

Thus $\Sigma_\Omega = A_\Omega \cup A_\Omega t$ for any transposition t , so

$$|\Sigma_\Omega : A_\Omega| = 2.$$

In particular $A_3 = \langle (123) \rangle \cong \mathbf{Z}_3$. Also A_4 has order 12, and has four Sylow 3-subgroups (exhausting the set of 8 elements of order 3).

The alternating and symmetric groups are highly non-abelian. For instance, A_4 has no subgroup of order 6. One way to see this is to use Sylow's Theorem, and show that no elements of order 2 and 3 in A_4 can generate a subgroup of order 6. Another is to assume that such a subgroup H exists, let P be a Sylow 3-subgroup of H . Then P is a Sylow 3-subgroup of A_4 , and there are four of them, so $|A_4 : N_{A_4}(P)| = 4 = |A_4 : P|$, whence $N_G(P) = P$. On the other hand, $|H : P| = 2$ so by Sylow's Theorem $|H : N_H(P)|$ can only be 1, as it is 1 mod 3. Therefore $H = N_H(P) \leq N_G(P) = P$, a contradiction.

A fundamental fact about the alternating groups A_n is that they are simple for $n \geq 5$, and that the only nontrivial normal subgroup of Σ_n for $n \geq 5$ is A_n . This will have to wait for the next section.