This summary of elementary group theory is copied from the webpage
of Ben Lynn

http://rooster.stanford.edu/~ben/maths/group/

Groups

A **group** is a set G and a binary operation · such that

1. For all x ,y∈G , x ·y∈G (closure).
2. There exists an **identity** element 1 ∈G with x ·1=1·x=1 for all x ∈G (identity).
3. For all x ,y,z∈G we have (xy)z=x(yz) (associativity).
4. For all x ∈G there exists an element x - 1 with x x - 1=x - 1x=1 (inverse).

If we only have closure and associativity, then we call G a **semigroup**. If we have closure, associativity and an identity element, we call G a **monoid**.

If x y=yx for some x ,y∈G then we say x ,y **commute** (or are **commutative**, or **permutable**). If x y=yx for all x ,y∈G then we say G is **abelian** (or **commutative**).

Theorem: The following are alternative axioms for defining *finite* groups:

1. Closure.
2. Associativity.
3. Right and left cancellation, namely a x=bx⇒a=b and y a=yb⇒a=b .

We shall restrict our attention to finite groups for now.

A **homomorphism** between two groups G ,H is a map f :G→H with f (x)f(y)=f(xy) for all x ,y∈G . If f is bijective then we call f an **isomorphism**.

The **order** of an element g in a group G is the smallest positive integer k such that g k =1 . This must always exist in a finite group.

Theorem: If x ∈G has order h , then x m =1 if and only if h |m .

Theorem: If x ∈G has order m n , where m ,n are coprime, then x can be uniquely expressed in the form x =uv where u has order m and v has order n .

Proof: Find a ,b with a m+bn=1 , and pick u =x b n,v=x a m . Uniqueness is not difficult to prove. ▪

A subset H of G that also satisfy the group axioms is called a **subgroup** of G . Every group G contains two trivial or **improper subgroups**, G itself and the group consisting of the identity element alone. All other subgroups are called **proper subgroups**.

Theorem: A nonempty subset H of G is a subgroup if and only if it is closed under multiplication.

A nonempty subset H ⊂G is a subgroup if and only if H 2 ⊂H

Lemma: For a subgroup H , for all h ∈H we have h H=H=Hh .

Corollary: For any set S ⊂H we have S H=H=HS .

We can now strengthen a previous statement. A nonempty subset H ⊂G is a subgroup if and only if H 2 =H

Theorem: Let g ∈G . Then for a subgroup H , we have g - 1 Hg is also a subgroup of G isomorphic to H .

Lagrange's Theorem

Lemma: Let H be a subgroup of G . Let r ,s∈G . Then H r=Hs if and only if r s - 1∈H . Otherwise H r,Hs have no element in common. Similarly, r H=sH if and only if s - 1 r∈H , otherwise r H,sH have no element in common.

Proof: If r s - 1=h∈H , then H =Hh=(Hr)s - 1 . Multiplying both sides on the right by s gives H r=Hs . Conversely, if H r=Hs , then since r ∈Hr (because 1 ∈H) we have r =h's for some h '∈H . Multiplying on the right by s - 1 shows that r s - 1∈H .

Now suppose H r,Hs have some element in common, that is h 1 r=h 2s for some h 1 ,h 2∈H . This implies r s - 1=h 1 - 1h 2∈H , thus H r=Hs by above.

Lagrange's Theorem: If H is a subgroup of G , then | G|=n|H| for some positive integer n . This is called the **index** of H in G . Furthermore, there exist g 1 ,...,g n such that G =Hr 1∪...∪Hr n and similarly with the left-hand cosets relative to H .

Proof: Take any r 1 ∈G . Note | Hr 1|=|H| . If H r 1≠G then take any r 2 ∈G∖Hr 1 . By the lemma, H r 1,Hr 2 are disjoint so we have | Hr 1∪Hr 2|=2|H| . By continuing in this fashion, after n steps for some positive integer n , we will eventually have accounted for all of the elements of G . We will have | G|=n|H| and G =Hr 1∪...∪Hr n .

Corollary: Let G be a group and g ∈G . Then the order of g divides | G| .

Corollary: Let G be a group of prime order. Then G has no subgroups and hence is cyclic.

Cyclic Groups

A **cyclic** group G is a group that can be generated by a single element a , so that every element in G has the form a i for some integer i . We denote the cyclic group of order n by ℤ n , since the additive group of ℤ n is a cyclic group of order n .

Theorem: All subgroups of a cyclic group are cyclic. If G =⟨a⟩ is cyclic, then for every divisor d of | G| there exists exactly one subgroup of order d which may be generated by a | G|/d .

Proof: Let | G|=dn . Then 1 ,a n,a 2 n,...,a (d-1)n are distinct and form a cyclic subgroup ⟨ a n⟩ of order d . Conversely, let H ={1,a 1,...,a d -1 be a subgroup of G for some d dividing G . Then for all i , a i =a k for some k , and since every element has order dividing | H| , a i d =a k d=1 . Thus k d=|G| m=ndm for some m , and we have a i =a n m so each a i is in fact a power of a n . From above this means it must be one of the d subgroups already described.

Theorem: Every group of composite order has proper subgroups.

Proof: Let G be a group of composite order, and let 1 ≠a∈G . Then if ⟨ a⟩≠G we are done, otherwise the subgroup ⟨ a d⟩≠G for every divisor d of | G| .

Generators

Theorem: The intersection of subgroups H 1 ,H 2,.... is a subgroup of each of H 1 ,H 2,...

We say the elements g 1 ,...,g m are **independent** if none of them can be expressed in terms of the others, that is, g i ∉⟨g 1,...,g i -1,g i +1,...,g m⟩ . Clearly every finite group has at least one set of independent generators. Independent elements can have relations between them, e.g. if a ,b are independent then we may have (ab) 2=1 for example. Such a relation is called a **defining relation**.

Given any two groups G ,H we may form their **direct product** G ×H , whose elements are pairs (g,h) with g ∈G,h∈H , and the group operation applies coordinatewise. The direct product of abelian groups is abelian.

Suppose every element of a group F has the form g h where g ∈G,h∈H for some subgroups G ,H of F , and furthermore, suppose every element of G commutes with every element of H and G ∩H={1} . Then F ≅G×H .

It is clear how to generalize this to define the direct product to k groups.

Example: ℤ 15 * ≅ℤ 4×ℤ 2 .

Groups Up To Order Eight

We now classify all groups with at most eight elements. Recall groups of prime order are cyclic, so we need only focus on the cases | G|=4,6,8 . We make use of the following:

Lemma: If each element 1 ≠g∈G is of order 2, then G is abelian and isomorphic to ℤ 2 ×...×ℤ 2 and | G| is a power of 2.

Proof: Clearly true for | G|=2 . Otherwise, let 1 ≠a≠b∈G . We have a 2 =b 2=1 , that is a =a - 1,b=b - 1 . Then a b≠1 (otherwise a =b - 1=b) and 1 =(ab) 2=a(ba)b which implies b a=a - 1b - 1=ab . Thus G is abelian.

Since G is finite, it has a finite set of independent generators a 1 ,...,a n . As G abelian, we may write an element g ∈G in the form g =a 1 e 1 ...a n e n where each e i ∈{0,1} . Then G =⟨a 1⟩×...×⟨a n⟩ and | G|=2×...×2=2 n

Now we can classify the groups up to order eight:

- | G|=4 : Each element (besides the identity) must have order 2 or 4. If a ∈G has order 4 it generates G and we have G =ℤ 4 . Otherwise every element has order 2 and by the lemma we have G =ℤ 2×ℤ 2 (the **four-group** or **quadratic group**, sometimes denoted by V after F. Klein's "Vierergruppe").
- | G|=6 :
- If a ∈G has order 6 we have G =ℤ 6 . Otherwise all elements (besides the identity) have order 2 or 3. By the lemma, not all elements can have order 2 because 6 is not a power of 2. So let a be an element of order 3, that is 1 ,a,a 2 are distinct. Let b be some other element in G . It can be verified that 1 ,a,a 2,b,ab,a 2b must be distinct. In order to satisfy closure, b 2 must be one of these elements. The only possibilities are b 2 =1,a or a 2 .

- If b 2 =a,a 2 we find that b cannot have order 2, so it has order 3. Then 1 =ab or 1 =a 2b , both of which are contradictions. Hence b 2 =1 . Next we determine which element is equal to b a . The only possible choices are a b or a 2 b . If b a=ab , then G is abelian, but then (ab) 2=a 2 and (ab) 3=b implying that a b has order 6, a contradiction. Thus b a=a 2b , implying (ab) 2=1 . We have defining relations a 3 =b 2=(ab) 2=1 . We shall see later that this is indeed a group (associativity turns out to hold) because it is the symmetric group of degree 3 (which is isomorphic to the dihedral group of order 6).

- | G|=8 : It turns out there are 3 abelian groups and 2 nonabelian groups. The three abelian groups are easy to classify: ℤ 8 ,ℤ 4×ℤ 2,ℤ 2×ℤ 2×ℤ 2 .

- The other groups must have the maximum order of any element greater than 2 but less than 8. Hence there exists an element of order 4, which we denote by a . All the others (besides the identity) have order 2 or 4. Let b be an element not generated by a . Then we have the distinct elements $1 ,a,a^2,a^3,b,ab,a^2b,a^3b$. Now b^2 can only be one of the first four. But $b^2 =a,a^3$ imply b is not of order 2 or 4, so we must have $b^2 =1$ or $b^2 =a^2$.

- Suppose $b^2 =1$. Now $b a$ must be equal to one of the last three elements. If $b a=ab$ then the group is abelian and we end up with the aforementioned ℤ 4 ×ℤ 2 . If $b a=a^2b$, then we have $b^{-1} a^2b=a$. Upon squaring, we derive the contradictory $a^2 =1$. So we must have $b a=a^3b$, that is, $(ab)^2=1$. The defining relations are $a^4 =b^2=(ab)^2=1$, and this turns out to be the dihedral group of order 8, also known as the **octic group**.
- The other possibility is $b^2 =a^2$. In this case, b also has order 4. If $b a=ab$ then the group is abelian and again we wind up with the group ℤ 4 ×ℤ 2 . If $b a=a^2b$ we have $b a=b^3$, which is a contradiction because it implies $a =b^2=a^2$. Thus we must have $b a=a^3b$. Then we get a group with the defining relations $a^4 =1,a^2=b^2,ba=a^3b$, which is known as the **quaternion group**. To verify associativity, one can show it is isomorphic to the group generated by the matrices (0 i i 0) ,(0 1 - 1 0) or (0 1 0 0 - 1 0 0 0 0 0 0 - 1 0 0 1 0) ,(0 0 1 0 0 0 0 1 - 1 0 0 0 0 - 1 0 0) The quaternion group is a special case of a **dicyclic group**, groups of order $4m$ given by $a^{2m} =1,a^m=(ab)^2=b^2$, and whose elements can be written $1 ,a,...,a^{2m-1},b,ab,...,a^{2m-1}b$. The square of elements not generated by a is b^2 .

The Product Theorem

Product Theorem: Let A ,B be groups. Then $|AB|=|A||B|/|A\cap B|$ and $A B$ is a group if and only if A ,B commute.

Let $D =A\cap B$. Then we can decompose B into cosets relative to D $B =Db_1\cup Db_2\cup...\cup Db_n$ where $n =|B|/|D|$ (and all cosets are distinct). Then left multiplying by A gives $A B=ADb_1\cup ADb_2\cup...\cup ADb_n$ We have D ⊂A , thus $A D=A$ and hence $A B=Ab_1\cup Ab_2\cup...\cup Ab_n$ Note if $A b_i$ and $A b_j$ have an element in common, then we must have $a_1 b_i=a_2b_j$ for some a 1 ,a 2∈A from which it follows $a_2^{-1} a_1=b_jb_i^{-1}$ which then is contained in D , the intersection of A and B .

But then $D (b_jb_i^{-1})=D$, that is, $D b_j=Db_i$, implying $i =j$. Thus the sets $A b_i$ are disjoint so $A B$ contains exactly $n |A|=|B||A|/|D|$ elements.

Now suppose $A B$ is a group. Then let a ∈A,b∈B . Then (a - 1b - 1) - 1=ba∈AB thus B A⊂AB . But from above, $B A$ and $A B$ both contain exactly $|A||B|/|A\cap B|$ elements thus $A B=BA$. Alternatively, by symmetry we have A B⊂BA .

Conversely, if A ,B commute then (AB) 2=(AB)(AB)=A(BA)B=A(AB)B=A 2B 2=AB , hence A B is a group.

Theorem: [Frobenius] Let A ,B be subgroups of a group G . Then G admits a decomposition into disjoint sets: G =Ag 1B+Ag 2B+...+Ag rB where g i ∈G . We have | Ag iB|=|A||B|/|g i - 1Ag i| .

Proof: Suppose A g 1B,Ag 2B have an element in common, that is, we have a 1 g 1b 1=a 2g 2b 2 for some a 1 ,a 2∈A,b 1,b 2∈B . Then A g 1B=Aa 1g 1b 1B=Aa 2g 2b 2B=Ag 2B Note | g i - 1Ag iB|=|Ag iB| . Since g i - 1 Ag i≅A , the result follows after applying the product theorem.

Corollary: Using the same notation, | G|=∑ i =1 r|A||B|/|g i - 1Ag i|

Permutations

The set of all permutations of n objects forms a group S n of order n ! . It is called the n th **symmetric group**.

A permutation that interchanges m objects cyclically is called **circular permutation** or a **cycle** of degree m . Denote the object by the positive integers. Then the cycle that moves 1 to 2, 2 to 3, . ..,m-1 to m and m to 1 is written (12...m) .

Every permutation can be unique represented into cycles operating on disjoint sets.

Example: (123456) 2=(135)(246)

So we may write a given permutation P =C 1...C r where the C i are cycles. Since cycles on disjoint sets commute, we have P m =C 1 m...C r m , and we see that the order of a permutation is the lowest common multiple of the orders of its component cycles. A permutation is **regular** if all of its cycle are of the same degree.

Two permutations a ,b∈S n are **conjugate** or **similar** if there exists t ∈S n with b =t - 1at . Let a =C 1...C r where the C i are cycles. Then the cycle decomposition of b is obtained by applying t to the elements inside the brackets of the strings representing each cycle, that is, if C i =(a 1a 2...a m) then t - 1 C it=(t(a 1)t(a 2)...t(a m)) where t (a i) represents the element t maps a i to.

Let a ∈S n , and write a =C 1...C r such that the cycles are arranged in non-decreasing order, that is, if we write μ i for the cycle length of C i , then 1 ≤μ 1≤...≤μ r , and μ 1 +...+μ r=n . Thus every permutation is associated with a partition of n into positive integers. Two permutations that belong to the same partition are said to belong to the same **class** of S n .

It is clear that two permuations of S n are conjugate if and only if they belong to the same class.

Now let us count how many partitions belong to a given class. Say a permutation has α_i cycles of degree i, so that $\alpha_1+2\alpha_2+\dots+n\alpha_n=n$. Then a set of nonnegative integers $\{\alpha_1,\dots,\alpha_n\}$ determines a class which we shall denote α. When writing down the cycles, we need to use up n numbers, and there are $n!$ ways to do this. But since for any i, we may permute the i-cycles amongst themselves, we must divide by $\alpha_1!\dots\alpha_n!$ times. Lastly, a cycle of length i can be written in i different ways, so if h_α denotes the number of permutations in the class α, we have $h_\alpha=\frac{n!}{1^{\alpha_1}\alpha_1!\dots n^{\alpha_n}\alpha_n!}$ [Cauchy].

A 2-cycle is called a **transposition**.

Let $x_1,\dots,x_n$ be indeterminates and consider the **product of differences** $\Delta=\prod_{i<j}(x_i-x_j)$ Then applying a permutation $\pi\in S_n$ to the variables will either preserve this value or negate it. We write $\Delta(\pi(x_1,\dots,x_n))=\zeta(\pi)\Delta(x_1,\dots,x_n)$ A permutation π is said to be **even** if $\zeta(\pi)=1$, and **odd** otherwise, that is, if $\zeta(\pi)=-1$. The function ζ is called the **alternating character** of S_n.

Theorem: Let $a,b\in S_n$. Then $\zeta(ab)=\zeta(a)\zeta(b)$.

Proof: Write Δ_π for $\Delta(\pi(x_1,\dots,x_n))$. $\zeta(ab)\Delta=\Delta_{ab}=\zeta(a)\Delta_b=\zeta(a)\zeta(b)\Delta$

Note all permutations of the same class have the same alternating character: by the theorem we have $\zeta(b)\zeta(b^{-1})=\zeta(1)=1$, and $\zeta(b^{-1}ab)=\zeta(a)$ after applying the theorem again.

Theorem: All transpositions are odd permutations.

Proof: The permutation (12) negates the factor (x_1-x_2) in Δ but leaves the other factors unchanged, thus we have $\zeta((12))=-1$. Then the results follows after using the identities $(1a)=(2a)(12)(2a)^{-1},(ab)=(1b)(1a)(1b)^{-1}$

Every permutation π can be written as a product of transpositions, because a cycle $(a_1\dots a_m)$ can be written as $(a_1a_2)(a_1a_3)\dots(a_1a_m)$. By the above theorem, the number of transpositions in such a representation is odd or even depending on whether π is odd or even.

Note S_n can be generated by the $n-1$ transpositions $(12),(13),\dots,(1n)$.

Theorem: In any group of permutations G, either all or exactly half the elements are even. The even permutations of G form a subgroup.

Proof: It is clear that the even permutations form a subgroup.

If G contains no odd permutations, there is nothing to prove. Otherwise let $q\in G$ be an odd permutation, so that $\zeta(q)=-1$. Then as $qG=G$, we have $\sum_{g\in G}\zeta(g)=\sum_{g\in G}\zeta(qg)$ Also, since ζ is multiplicative we have $\sum\zeta(qg)=\sum\zeta(q)\zeta(g)=-\sum\zeta(g)$ hence $\zeta(g)=0$, proving the result.

The set of all even permutation of degree n forms a group A_n of order $\frac{1}{2}n!$, called the **alternating group** of degree n .

Since (1i)(1j)=(1ij) for distinct 1 ,i,j , and since (1ij)=(12j)(12i)(12j) we see that A n may be generated from the n -2 3-cycles (123)(124)...(12n)

Cayley's Theorem: Let G ={g 1,...,g | G|} be any group. Each g i ∈G can be associated with the permutation of S n that takes g j to g j g i . The set of these permutations forms a subgroup G ' of S n , and G '≅G .

The permutation group G ' associated with a group G is called the **regular representation** of G . In general, if an abstract group G is isomorphic to some concrete mathematical group (e.g. permutations, matrices) then we say we have a **faithful representation** of G .

A group of permutations G ⊂S n is said to be **transitive** if for every α ,β∈{1,...,n} there exists g ∈G with g (α)=β , that is, for any two objects, there exists a permutation that maps one to the other. Otherwise the group is **intransitive**.

Example: { (1),(12),(34),(12)(34)} is intransitive because no permutations takes 1 to 3. It is isomorphic to the transitive group { (1),(12)(34),(13)(24),(14)(23)} .

Write G α for the subgroup of permutations of G that fix α .

Theorem: A group of permutations G ⊂S n is transitive if and only if the subgroup G 1 is of index n relative to G .

Proof: If G is transitive, then there exists element g 1 2 ,g 1 3,...,g 1 n∈G that map 1 to 2 ,3,...,n respectively. Consider the sets G 1 g 1 2,G 1g 1 3,...,G 1g 1 n The sets are disjoint because each acts differently on the element 1. Futhermore, any q ∈G transforms 1 to k , say, hence q ∈G 1g 1 k because q g 1 k leaves 1 unchanged so must lie in G 1 . So these disjoint cosets partition G , showing that G 1 has index n in G .

Conversely, if G 1 has index n , decompose G into cosets G 1 g 1,...,G 1g n . Then if g i ,g j transform 1 to the same object α , we have that g i g j -1∈G 1 , implying that G 1 g i=G 1g j and hence i =j . Thus we may label the g i such that g i (1)=i .

Lastly, if α ,β∈{1,...,n} then g α - 1 g β transforms α into β .

Corollary: The order of a transitive groups of permuations of degree n is divisible by n .

A group of permutations G is said to be **k -ply transitive** if for any sets of size k { α 1,...,α k},{β 1,...,β k}⊂{1,...,n} there exists g ∈G with g (α i)=β i for all i .

The number of distinct subsets of size k in a set of size n is given by n (n-1)...

$(n-k+1)$. Thus we have:

Theorem: The order of a k -ply transitive group of degree n is divisible by $n(n-1)...(n-k+1)$.

Theorem: The group G is k -ply transitive if G is simply transitive and G_1 is $(k-1)$ -ply transitive with respect to $\{2,3,...,n\}$.

Let G be a transitive group in S_n . Suppose it is possible to place $1,...,n$ in an $r \times s$ matrix where $rs=n, r,s>1$ such that the permutations of G either permute the objects of any one row amongst themselves or else interchange objects of one row with another. In other words, two objects that start in the same row are never transformed to objects in different rows, and vice versa. Then G is said to be **imprimitive**, and the rows are called **imprimitive systems**. Otherwise G is said to be primitive. Note all doubly-transitive groups are primitive, and in particular, S_n is primitive.

Geometry and Groups

The Dihedral Group: Consider a regular n -gon. Then rotating it by a multiple of $2\pi/n$ leaves it unchaged, as does a reflection through any one of its axes of symmetry. Thus if a represents rotation by $2\pi/n$ and c represents reflection through one of its axes of symmetry, then all the symmetry-preserving rotations and reflections (alternatively, reflections can be replaced by rotations in 3D) can be generated using a, c , with defining relations $a^n=c^2=(ac)^2=1$. The last relation can be seen by realizing $ac=ca^{-1}$. This group is called the **dihedral group** of order $2n$.

The Tetrahedral Group: Consider a tetradhedron that is free to rotate about its center. Any one of the four vertices can be brought to the position of any other, and then there are three configurations the other vertices can take. Thus there are $4\times 3=12$ operations. Note if one vertex is fixed, the other three can only be rotated cyclically, thus the tetrahedral group contains all possible 3-cycles, hence it contains A_4 . But since its order is the same as that of A_4 , the tetradhedral group must be A_4 .

The Octahedral/Hexahedral Group: Note the centers of the faces of an octahedron can be thought of as the vertices of a cube, and conversely.

For a cube, we may rotate any given vertex to the position of any of the eight vertices, and then choose one of three rotations (the edges that the given vertex belong to can take one of three positions), hence there are 24 operations in all. Now consider the four diagonals of the cube, which are permuted amongst themselves. Note that two distinct rotations of the octahedral group correspond to two distinct permutations of the four diagonals because no rotation except the identiy can map all four diagonals into themselves, thus the octahedral group is precisely S_n .

The Icosahedral/Dodecahedral Group: Again, the centers of the faces of one of these solids can be viewed as the vertices of the other.

Given a dodecahedron, we can rotate any one of its vertices to the position of any one of the twenty vertices, and once there, we can choose among three rotations, so there are 60 distinct rotations.

In Euclid's Elements (Book XIII, Proposition 17) a dodecahedron is derived from a cube such that each of the twelve edges of the cube is a diagonal in one of the faces of the dodecahedron. Conversely, starting with a given diagonal of a dodecahedron, a unique cube can be constructed with its edges being the diagonals of the dodecahedron, with one of the edges being the chosen diagonal. Each face has five diagonals, so there are exactly five cubes that can be constructed in this manner. Now two distinct permutations of these five cubes correspond to distinct rotations, because a little thought shows that only the identity will leave the five cubes in place, thus the dodecahedral group is isomorphic to some subgroup of S_5 . But we shall see the only subgroup of S_5 of order 60 is A_5 , so this must be what the dodecahedral group is.

Normal Subgroups

Two elements a ,b in a group G are said to be **conjugate** if $t^{-1}at=b$ for some t ∈G . The elements t is called a **transforming element**. Note conjugacy is an equivalence relation. Also note that conjugate elements have the same order. The set of all elements conjugate to a is called the **class** of a .

Theorem: The elements of G that commute with a given element a form a subgroup N , called the **normalizer** of a . Given a decomposition of G into cosets $Ng_1,...,Ng_h$, where $h=|G|/|N|$, the elements of the class of a can be written $g_1^{-1}ag_1,...,g_h^{-1}ag_h$.

Proof: That the normalizer is indeed a subgroup is easily verified. If we take any ng_i∈Ng_i where n ∈N then we have $(ng_i)^{-1}a(ng_i)=g_i^{-1}n^{-1}ang_i=g_i^{-1}ag_i$ Also, if we have $g_i^{-1}ag_i=g_j^{-1}ag_j$ then $g_ig_j^{-1}$ also commutes with a , thus also belongs to N , implying that $Ng_i=Ng_j$.

Note an element a forms a class by itself if and only if a commutes with all of G . Such an element is called an **invariant** or **self-conjugate** element of G . In every group, the identity is invariant. In an abelian group every element is invariant.

Classes of conjugates are disjoint, for if $g^{-1}ag=h^{-1}bh$ then $x^{-1}ax=(gh^{-1}x)^{-1}b(gh^{-1}x)$ for any x ∈G , implying that every element in the class of a also belongs to the class of b . Thus we may decompose G into disjoint classes of conjugates, and if there are k classes, we have $|G|=h_1+...+h_k$ where h_i is the size of the i th class. Note each h_i divides $|G|$ and $h_i=1$ if and only if a_i is self-conjugate.

Theorem: If a group G has order p^m for some prime p , then the number of self-conjugate elements is a positive multiple of p .

Proof: Consider the decomposition of G . Using the above notation, each h_i must be some nonnegative power of p . Then suppose z of the h_i are equal to one (so z is the number of self-conjugates). Then we have $p^m=z+p^{a_1}+p^{a_2}$

$+\dots$ where $0 < a_1 \le a_2 \le \dots$. We see z must be a multiple of p , but since $z \ge 1$ because 1 is always invariant, z must be a positive multiple of p .

We may generalize some of these concepts as follows: If K is a subset of some group G then any subset of the form $g^{-1}Kg$ is said to be **conjugate** with K . The elements of G which commute with K form a group N which is the **normalizer** of K . In a similar manner to above we can show:

Theorem: The number of sets conjugate to K is the index of its normalizer N .

A set H that commutes with every element of G is called **invariant** or **self-conjugate**. In particular, if H is some subgroup of G , then we call H a **normal** or **invariant** or **self-conjugate subgroup** of G . In general, if A is some subgroup of G then groups of the form $g^{-1}Ag$ are called the **conjugate subgroups** of A . Write $H \triangleleft G$ to express that H is a normal subgroup of G . Note that the intersection of normal subgroups is also a normal subgroup, and that subgroups generated by invariant sets are normal subgroups.

Theorem: A subgroup of index 2 is always normal.

Proof: Suppose H is a subgroup of G of index 2. Then there are only two cosets of G relative to H . Let $s \in G \setminus H$. Then G can be decomposed into the cosets H, sH or H, Hs , implying H commutes with s . Since $Hh = hH$ for any $h \in H$ we see that H commutes with every element of G and hence is normal.

Example: In the dihedral group $D_{2n} : \{a, c \mid a^n = c^2 = (ac)^2 = 1\}$ the cyclic subgroup $\langle a \rangle$ is normal.

Example: The alternating group A_n is normal in S_n .

Note if a is an element of a normal subgroup H of a group G , then the class of a is contained in H , so that a normal subgroup can be viewed as the union of classes of G , and conversely, any union of classes of G satisfying the group axioms form a normal subgroup of G .

Example: The classes of S_4 are $K_0 = \{1\}$ $K_1 = \{(12),(13),(14),(23),(24),(34)\}$ $K_2 = \{(123),(124),(132),(134),(142),(143),(234),(243)\}$ $K_3 = \{(12)(34),(13)(24),(14)(23)\}$ $K_4 = \{(1234),(1243),(1324),(1342),(1423),(1432)\}$ It can be verified that $V = K_0 \cup K_3$ forms a subgroup thus is normal.

Quotient Groups

Let H be a normal subgroup of G . Then it can be verified that the cosets of G relative to H form a group. This group is called the **quotient group** or **factor group** of G relative to H and is denoted G/H .

It can be verified that the set of self-conjugate elements of G forms an abelian group Z which is called the **center** of G . Note the center consists of the elements of G that commute with all the elements of G . Clearly the center is always a normal subgroup.

Theorem: A group G of order p 2 where p is prime is always abelian.

Proof: From a previous theorem, the number of invariant elements is a positive multiple of p , so the center has order p or p 2 . The latter case implies G is abelian, so consider the case | Z|=p . Then | G/Z|=p so G /Z is cyclic, thus we may decompose G into the cosets Z ,Zg,...,Zg p -1 for some g ∈G . The product of any two elements z 1 g λ,z 2g μ is z 1 z 2g λ +μ=z 2g μ z 1g λ , thus G is abelian and | Z|=p 2 in fact.

Define the **commutator** of two elements g ,h of a group G by u =g - 1h - 1gh . We have u =1 if and only if g h=hg . In an abelian group, all commutators are equal to the identity. Consider the set of all commutators { u 1,...,u m} as g ,h run through all the elements of G . This set is not necessarily closed under the group operation. We define the **commutator group** U to be the group generated by this set. If U =G we say G is a **perfect group**.

Theorem: The commutator group U of a group G is normal. G /U is abelian. U is contained in every normal subgroup that has an abelian quotient group.

Proof: Let x ∈G . Then x - 1 g - 1h - 1ghx=a - 1b - 1ab where a =x - 1gx,b=x - 1hx , thus U is normal.

Consider the commutator of two cosets U x,Uy . We have (Ux - 1)(Uy - 1)(Ux)(Uy)=Ux - 1y - 1xy=U since x - 1 y - 1xy∈U , hence G /U is abelian.

Lastly if R is any normal subgroup of G with an abelian quotient group, then for any x ,y∈G we have R x - 1y - 1xy=R since all commutators of G /R must be equal to the identity, thus R contains x - 1 y - 1xy hence R ⊃U .

Theorem: If A ,B are normal subgroups of G with only the identity element in common then every element of A commutes with every element of B .

Proof: Consider u =a - 1b - 1ab=(a - 1b - 1a)b=a - 1(b - 1ab) where a ∈A,b∈B . Then since A ,B are normal, a - 1 ba∈B and b - 1 ab∈A , thus u ∈A∩B={1} , hence a ,b commute.

The Isomorphism Theorems

Let G be a group. Let H ◃G . Then a **natural homomorphism** exists from G to G /H , given by g ↦Hg .

First Isomorphism Theorem: Let φ :G→G' be a group homomorphism. Let E be the subset of G that is mapped to the identity of G ' . E is called the **kernel** of the map φ . Then E ◃G and G /E≅im ϕ .

An **automorphism** is an isomorphism from a group G to itself. Let g ∈G . Then the map that sends a ∈G to g - 1 ag is an automorphism. Automorphisms of this form are called **inner** automorphisms, otherwise they are called **outer** automorphisms. Note that all inner automorphisms of an abelian group reduce to the identity map.

Second Isomorphism Theorem: Let G be a group. Let H ◃G . If A is any subgroup of G , then H ∩A is normal and A /(H∩A)≅HA/H

Proof: Let A ={1,a 1,a 2,..} . Then the image of A under the natural map from G to G /H is H A=H∪Ha 1∪Ha 2∪... Now H A is a subgroup by the Product Theorem because H A=AH since H is normal, and H is normal in H A , thus H A/H={H,Ha 1,Ha 2,...} Lastly, the kernel of the natural map from G to G /H when restricted to A is clearly H ∩A , and applying the first isomorphism theorem proves the result.

Theorem: If H ◃G and A is some subgroup satisfying H ⊂A⊂G then A /H is a subgroup of G /H . Conversely, every subgroup of G /H is of the form A /H for some H ⊂A⊂G .

Proof: H is normal in G , so H must also be normal in A . Let A ={1,a 1,a 2...} . Then A /H={H,Ha 1,Ha 2,...} must be some subgroup of G /H . Conversely, suppose A '={H,Ha 1,Ha 2,...} is some subgroup of G /H . Then the set A =H∪Ha 1∪Ha 2∪... is a subgroup of G since for any h 1 ,h 2∈H we have h 1 a ih 2a j=h 3a k where a k =a ia j and for some h 3 ∈H , since A ' is a group. Thus A '=A/H .

Third Isomorphism Theorem: If H ◃G and H ◃A◃G then A /H◃G/H and G /HA /H ≅G/A . Conversely, every normal subgroup of G /H is of the form A /H for some H ◃A◃G .

Proof: Consider the map from G /H→G/A that sends H x to A x . The map is well-defined because H x=Hy implies x y - 1∈H⊂A whence A x=Ay . This map is homomorphic because H xHy=Hxy is mapped to A xy=AxAy . The kernel of the map consists of all elements of G /H that get mapped to A , in other words, elements of the form H x with A x=A . This happens if and only if x ∈A , thus the the kernel consists of the cosets of the form H a for a ∈A . That is, the kernel is precisely A /H . By the first isomorphism theorem, A /H is therefore normal in G /H and we have G /HA / H ≅G/A .

Conversely, suppose A '={H,Ha 1,Ha 2,...} is a normal subgroup of G /H . Then we know that A =H∪Ha 1∪Ha 2∪... is a subgroup of G , and it remains to show A is normal. Since A ' is normal, we have for all x ∈G,a∈A , H xHaHx - 1=Ha' for some a '∈A . In particular, by picking the identity for the first and third occurences of H in the equation, x Hax - 1⊂Ha' for some a '∈A , and hence x Ax - 1⊂H∪Ha 1∪Ha 2∪...⊂A . Swapping x with its inverse gives the reverse inclusion x Ax - 1⊃A , thus A =x - 1Ax , that is, A is normal.

ordan-Holder Decomposition

A group which has no proper normal subgroups is called a **simple** group.

Example: Cyclic groups of prime order are simple. Simple groups of composite order are "rare" according to the book.

A proper normal subgroup A is called a **maximum normal subgroup** of G if A ◃H◃G implies H =G or H =A . Note A is a maximum invariant normal subgroup if and only if G /A is a simple group, because H /A is a normal subgroup of G /A .

If G is not simple, let A a maximum normal subgroup in G . Now if A is not simple, let A 1 be a maximum normal subgroup. Continuing in this fashion we can construct a sequence, called a **composition series** as follows. G ▹A▹A 1▹...▹A r▹{1} where G /A,A/A 1,A 1/A 2,...,A r are all simple nontrivial groups, which are called the **composition quotient groups**. The orders of the composition quotient groups are called the **composition indices**.

Jordan-Holder Theorem: In any two composition series for a group G , the composition quotient groups are isomorphic in pairs, though may occur in different orders in the sequences.

Proof: Trivially the theorem is true if | G|=2 . Next assume the theorem has been proved for groups of order less than | G| . If G is simple then the theorem is again trivially true, otherwise let two composition series be G ▹A▹A 1▹...▹A r▹{1} and G ▹B▹B 1▹...▹B s▹{1}

Then if A =B , by inductive assumption the composition quotient groups A /A 1,A 1/A 2,...,A r and G /B,B/B 1,B 1/B 2,...,B s are isomorphic in pairs, and we have G /A=G/B hence the theorem is true in this case.

Otherwise A ≠B . Consider the group A B . This contains A and B which are distinct and maximal in G , thus we must have A B=G . Let D =A∩B . By the first isomorphism theorem we have G /A≅B/D and G /B≅A/D . Note G /A,G/B are simple, hence B /D , A /D are also simple which implies D is in fact a maximum normal subgroup in A and B .

Now let D ▹D 1▹...▹D t▹{1} be a composition series for D .

Consider the quotient groups G /A,A/D,D/D 1,...,D t,{1} and G /A,A/A 1,...,A r, {1} By inductive assumption, the theorem is true for the group A and hence the above sequences are isomorphic in pairs, and in fact t =r .

Similarly G /B,B/D,D/D 1,...,D t,{1} is isomorphic in pairs to the sequence G / B,B/B 1,,...,B s,{1} (and s =r).

But since the sequences $G/A, A/D, D/D_1, \dots, D_t, \{1\}$ and $G/B, B/D, D/D_1, \dots, D_t, \{1\}$ are clearly isomorphic in pairs, we have proved the theorem.

Example: The alternating group A_n is a maximum normal subgroup of S_n. We have already seen A_n is normal in S_n since it is of index 2. But the fact that it is of index 2 implies S_n/A_n is simple and hence A_n is maximal.

For $n = 3$, we have the composition series $S_3 \triangleright A_3 \triangleright \{1\}$ since the composition indices are the primes $2, 3$.

For $n = 4$, recall that the group $V = \{1, (12)(34), (13)(24), (14)(23)\}$ is normal in A_4, and note every element in V besides the identity generates a group of order 2 of index 2 (implying it is normal in V) thus we have the the composition series $S_4 \triangleright A_4 \triangleright V \triangleright \langle (12)(34) \rangle \triangleright \{1\}$ with composition indices $2, 3, 2, 2$.

Example: Consider the cyclic group of order 6, and let a be a generator. Then we have the composition series $\langle a \rangle \triangleright \langle a^2 \rangle \triangleright \{1\}$ with composition indices $2, 3$. Note the composition quotient groups are isomorphic to those of S_3, hence knowing the composition quotient groups is not enough to reconstruct the original group.

A group G is said to be **soluble** if all the composition indices of G are prime. For instance, all the groups in the above examples are soluble. Note a group G is soluble if it contains a normal subgroup H with both $G/H, H$ soluble. This is because given the series $H \triangleright H_1 \triangleright \dots \triangleright H_r \triangleright \{1\}$ and $G/H \triangleright G_1/H \triangleright \dots \triangleright G_s/H \triangleright \{1\}$ with prime composition indices, we have $G_{i-1}/H G_i/H \cong G_{i-1}/G_i$ (where we set $G_0 = G$ by applying the third isomorphism theorem.

Hence we can construct the series with prime composition indices $G \triangleright G_1 \triangleright \dots \triangleright G_s \triangleright H \triangleright H_1 \triangleright \dots \triangleright H_r \triangleright \{1\}$

Lemma: If a normal subgroup H of A_n for $n \ge 3$ contains a cycle of degree 3 then $H = A_n$.

Proof: Without loss of generality let $(123) \in H$. For $n = 3$, (123) generates A_3 and there is nothing to prove. For $n > 3$, since H is normal, it must also contain $s^{-1}(123)s$ for any even permutation s. Set $s = (32k)$ for $k > 3$. Then we have that H contains $(1k2)$, and hence also its square which is $(12k)$. Recall these cycles generate A_n.

Theorem: A_n is simple for $n > 4$.

Proof: Suppose H is a normal subgroup of A_n. Suppose $h \in H$ is a permutation of the form $(a_1 a_2 \dots a_m)h'$ where $m > 3$ and h' does not act on $a_1, \dots, a_m$. Then the permutation $s = (a_1 a_2 a_3)$ commutes with all the cycles of h except the first, Now s is even hence $h_1 = s^{-1}hs = (s^{-1}(a_1 \dots a_m)sh') \in H$, thus $h_1 h^{-1} = (s^{-1}as)a^{-1} = (a_2 a_3 a_1 a_4 \dots a_m)(a_m a_{m-1} \dots a_1) = (a_1 a_3 a_m) \in H$ is contained in H. Since this is a cycle of degree 3, by the above lemma we have H =A n . So if H is to be a proper subgroup, its elements cannot contain cycles longer than 3.

Now suppose H contains an element containing two 3-cycles. Without loss of generality, suppose (123)(456)h'∈H where h ' does not act on 1 , 2,3,4,5,6 . Set s =(234) , so that it is an even permutation commuting with h ' . Then set h 1 =s - 1hs=(134)(256)h'∈H , which gives h 1 h - 1=(134)(256)(321)(654)=(12436)∈H which is a cycle of length greater than 3.

Now suppose H contains an element containing exactly one 3-cycle, say h = (123)h' , and h ' consists of 2-cycles implying h ' 2=1 . Then h 2 =(132) , so by the above lemma H =A n .

Lastly suppose H consists only of permutations that are products of disjoint transpositions. For n =4 this leads to the four-group V in the above example. For n >4 , suppose h =(12)(34)h'∈H . Then set s =(234) , and we have h 1 =s - 1hs=(13)(42)h'∈H thus h 2 =h 1h - 1=(13)(42)(12)(34) ∈H Now take t =(145) , and we have h 3 =t - 1h 2t=(45)(23) ∈H We conclude that h 3 h 2 - 1=(45)(23)(14)(23)=(45)(14)=(145) ∈H , hence H =A n by the lemma.

Corollary: A n is the only subgroup of order 1 2 n! in S n when n >4 .

Proof: Any subgroup H of index 2 is necessarily normal in S n , thus D =A n∩H is normal in A n . By the Theorem we have D ={1} or D ={A n} . Since H contains more than one even permutation (because either half or all of a group of permutations are even) we must have D =A n , implying H =A n .

It can be easily verified that the statement of the corollary is also true for n ≤4

Corollary: S n is not soluble for n >4 .

Proof: By the theorem, the composition series for S n is S n ▹A n▹{1} and its composition indices are 2 ,1 2 n! , the latter of which is not prime.

Sylow Groups

Lemma: Let A be an abelian group. If p is a prime factor of | A| then A contains at least one element of order p

Proof: The lemma is trivial when | A|=p , which we shall use to start an induction. Assume | A| is composite. Then A contains a proper subgroup. Choose a proper subgroup H of maximum order. If p ||H| then by induction H contains an element of order p , so assume (|H|,p)=1 . Then take some element g ∈A∖H . Let t be the order of g . Consider the group A '=H⟨g⟩ . Since A is abelian, we have H ⟨g⟩=⟨g⟩H thus A ' is a group. But since it strictly contains H, we have $A' = A$ by maximality of H.

Now $H\langle g\rangle$ contains $|H|t/d$ elements where $d = |H \cap \langle g\rangle|$. Thus $|A|d = |H|t$. Since the p divides the left-hand side, and $(|H|, p) = 1$, we must have $p | t$, and $g^{t/p}$ is an element of order p.

If the order of a group G is divisible by p^m but by no higher power of p for some prime p then any subgroup of G of order p^m is called a **Sylow group** corresponding to p.

Theorem: Every group G possesses at least one Sylow group corresponding to each prime factor of $|G|$.

Proof: The theorem is immediate when $|G| = 2$, which we shall use to start an induction. Write $|G| = p^m r$ where $(r, p) = 1$. Decompose G into classes of conjugate elements, and pick elements $a_1, ..., a_k$ from each class. Recall if h_i denotes the size of the class containing a_i we have $|G| = h_1 + ... + h_k$. Also recall the normalizer N_i of a_i satisfies $|N_i| = |G|/h_i$. We have two cases:

Case 1: Suppose there exists h_i with $h_i > 1$ and $(h_i, p) = 1$. Then $|N_i|$ is less than $|G|$ and divisible by p^m. By inductive hypthoesis, N_i possesses a subgroup of order p^m which is the Sylow group corresponding to p.

Case 2: For all i, we have $h_i = 1$ or $p | h_i$. We have $h_i = 1$ for self-conjugate elements, and we must have at least one of these since 1 is self-conjugate. Let z be the number of self-conjugate elements. Then $p^m r = z + xp$ for some integer x, hence $p | z$. Thus the order of the center is divisible by p. Since it is abelian, by the lemma it contains at least one element g that commutes with all elements and has order p. Then $P = \langle g\rangle$ is a normal subgroup of G and G/P has order $p^{m-1} r$. By the inductive hypothesis G/P contains a Sylow group of order p^{m-1}, which we write H/P where H is a subgroup of G. Then $p^{m-1} = |H|/p$, thus $|H| = p^m$ and H is a Sylow group of G corresponding to p.

Theorem: [Cauchy] Let G be a group. If p is a prime factor of $|G|$ then G contains at least one element of order p

Proof: Let H be a Sylow group of G of order p^m. If $1 \neq h \in H$ then the order of h is p^μ for some $\mu > 0$. Then $h^{p^{\mu - 1}}$ has order p.

All subgroups conjugate to a Sylow group are themselves Sylow groups. It turns out the converse is true.

Theorem: All Sylow groups belonging to the same prime are conjugates.

Proof: Let A, B be subgroups of G of order p^m. Recall we can decompose G relative to A and B: $G = Ag_1B \cup ... \cup Ag_rB$ and $|G| = |A||B|/d_1 + ... + |A||B|/d_r$ where d_i is the size of $D_i = g_i^{-1}Ag_i \cap B$. We have $|A| = |B| = p^m$ and $|G| = p^m r$ where $(r, p) = 1$. Thus dividing by p^m gives $r = \frac{p^m}{d_1} + ... \frac{p^m}{d_r}$ Now D_i is a subgroup of B, hence d_i is some nonnegative power of p and is at most p^m. Since $(r, p) = 1$, we must have $p^m/d_l = 1$ for some l, in other words $d_l = p^m$.

Then D l has the same order as B and is contained in B , thus D l =B and similarly D l =g l - 1Ag l . Hence B =g l - 1Ag l implying that A ,B are conjugate.

Corollary: A Sylow group is unique if and only if it is a normal subgroup.

Theorem: If there are exactly k Sylow groups of a group G corresponding to a prime p then k =1modp and k divides | G| .

Proof: We know that the number of distinct Sylow groups is equal to the number k of distinct conjugates. Let A be some Sylow group corresponding to p and let N be the normalizer of A . Recall | G|=|N|k thus k divides | G| .

Every a ∈A satisfies a - 1 Aa=A thus a ∈N , Hence A ◃N . Thus | N|=p mn' where (n',p)=1 .

Decompose G as the disjoint sets G =Ag 1N∪...∪Ag rN Then | G|=| N|p md 1 +...+| N|p md r where d i is the order of the group D i =g i - 1Ag i∩N . Without loss of generality assume g 1 =1 , hence A g 1N=AN=N . Now dividing by n gives k =1+p m d 2 +...+p m d r Now suppose d i =p m for some i . Then D i =g i - 1Ag i , implying g i - 1 Ag i⊂N . Now N possesses a Sylow group of order p m , and we have already found two: A ,g i - 1Ag i . But A is normal in N thus must be the unique Sylow group, hence A =g i - 1Ag i . Since N is the normalizer of A we must have g i ∈N and hence A g iN=AN=N , which is impossible unless i =1 .

Thus all terms in the above summation are divisble by p except for the first term which is equal to one.

Theorem: Any group G of order p q for primes p ,q satisfying p ≠1(modq) and q ≠1(modp) is abelian.

Proof: We have already shown this for p =q so assume (p,q)=1 . Let P =⟨a⟩ be a Sylow group of G corresponding to p . The number of such subgroups is a divisor of p q and also equal to 1 modulo p . Also q ≠1modp . Then since the number of such subgroups cannot be equal to p ,q,pq , it must be equal to one. By the above corollary we have that P is normal in G of order p . Similarly we can find a group Q =⟨b⟩ normal in G of order q .

Then P Q=QP , which by the product theorem is a subgroup order p q/|P∩Q| . But since (p,q)=1 they only have the identity element in common thus G =PQ . Also, recall these conditions also imply every element of P commutes with every element of Q . Then every element of G has the form a α b β=b βa α and is clearly abelian

A **prime power group** is a group whose order is a power of a prime. [It seems that nowadays they are referred to as p -groups.] All Sylow groups are prime power groups. Recall that a group G of order p m for a prime p has at least one nontrivial self-conjugate element, thus we can find a self-conjugate element of order p . Let a be such an element. Then x - 1 ax for any x ∈G , and

⟨ a⟩ is a normal subgroup of order p . In general:

Theorem: A group of order p m for a prime p contains at least one normal subgroup of order p μ for any 0 <μ<m .

Proof: The theorem is true for m =2 because in this case the group is abelian. We shall use this case to base an induction.

Suppose G is a group of order p m for m >2 . Then let P be a normal subgroup of G of order p . Then G /P has order p m -1 which by inductive assumption has an invariant subgroup of order p μ -1 which has the form A /P for some normal subgroup A in G with order p μ .

Corollary: All prime power groups are soluble.

Proof: A group G of order p m has a normal subgroup A 1 of order p m -1 which in turn contains a normal subgroup of order p m -2 , and so on. Thus we can construct the composition series G ▹A 1▹A 2▹...▹A m -1▹{1}

Example: There is no simple group of order 200. For let G be a group with order 200. Then since 200 =5 2×8 , G contains k Sylow groups of order 25 where k =1mod5 and k |200 . Thus k |8 which is impossible unless k =1 . Thus there exists a unique normal Sylow group of order 25, and hence the group is not stimple.

Example: There is no simple group of order 30. Suppose there is such a group. Then none of its Sylow groups are unique, implying it has 1 +5=6 Sylow groups of order 5, hence there are 6 ×4=24 elements of order 5 , and similarly we must have 1 +3×3=10 Sylow groups of order 3, thus the total number of elements is greater than 30, a contradiction.

We can now supply an alternative proof that A n is simple for n ≥5 :

Proposition: If | G|=60 and G has more than one Sylow 5-subgroup then G is simple.

Proof: Suppose | G|=60 and contains more than one Sylow 5-subgroup, but there exists a proper normal subgroup. Then note we must have exactly 6 Sylow 5-subgroups. Let P be such a group. Then the normalizer of P has order 10 since its index is 6 .

If 5 ||H| then H contains a Sylow 5 -subgroup of G and since H is normal it contains all 6 conjugates of this subgroup, hence | H|≥1+6·4=25 hence we must have | H|=30 . But by the previous example, | G| must have a unique Sylow 5-subgroup, a contradiction, thus 5 does not divide | H| .

If | H| is 6 or 12 then H has a normal Sylow subgroup of order 2,3, or 4, which is also normal in G , and we may replace H by this. Hence | G/H|=30,20 or 15 . Then by previous results, G /H has a normal subgroup of order 5 . Its preimage under the natural map is a normal subgroup whose order is a multiple of 5, which we have previously shown to be a contradiction.

Corollary: A_5 is simple.

Proof: The subgroups ⟨ (12345)⟩ and ⟨ (13245)⟩ are distinct Sylow 5-subgroups.

Theorem: A_n is simple for all $n \geq 5$.

TODO: proof

Abelian Groups

We no longer assume that the groups we study are finite.

With abelian groups, additive notation is often used instead of multiplicative notation. In other words the identity is represented by 0 , and $a+b$ represents the element obtained from applying the group operation to a and b .

A group G is the **direct sum** of two subgroups U ,V if every element x ∈G can be written in the form $x=u+v$ where u ∈U,v∈V , and $u+v=0$ implies $u=v=0$. We write $G=U\oplus V$.

Note that U ,V cannot have a nonzero element w in common, otherwise $w+(-w)=0$ is a nontrivial decomposition of zero. Also u ,v are uniquely determined by x for if $u_1+v_1=u_2+v_2$ implies $u_1-u_2=v_2-v_1$∈$U\cap V$.

More generally we have $G=U_1\oplus\dots\oplus U_r$, if every x ∈G can be written in the form $x=u_1+\dots+u_r$ and also if $0=u_1+\dots+u_r$ implies $0=u_1=\dots=u_r$. Clearly if G is finite we have $|G|=|U_1|\dots|U_r|$.

An abelian group A is a **free abelian** group of **rank** r if there exist $u_1,\dots,u_r$∈A such that $A=$⟨$u_1,\dots,.u_r$⟩ and $a_1u_1+\dots+a_ru_r$ implies $a_1=\dots=a_r=0$. Alternatively we may require every x ∈A can be uniquely written in the form $x=a_1u_1+\dots+a_ru_r$. The set $\{u_1,\dots,u_r\}$ is a set of **free generators** of A . The trivial group is viewed as a free abelian group of rank zero, and viewed as been generated by the empty set.

Generators need not be unique. However it is easy to see that two sets of free generators are related by a unimodular (determinant of absolute value one) matrix transformation.

Theorem: [Dedekind] Let F be a free abelian group of rank r and let G be a nonzero subgroup of F . Then G is a free abelian group of rank s with $s\leq r$. Furthermore, F has a set of free generators $\{u_1,\dots,u_r\}$ such that G is generated by $v_1=a_{11}u_1+a_{12}u_2+\dots+a_{1r}u_r$ $v_2=a_{22}u_2+\dots+a_{2r}u_r$ ⋮ $v_s=a_{ss}u_s+\dots+a_{sr}u_r$ for some a_{ij} with $a_{11},a_{22},\dots,a_{ss}$ positive.

Proof: Let $\{u_1,\ldots,u_r\}$ be free generators for F. Then take any nonzero element $b = b_1 u_1 + \ldots + b_r u_r$ of G. After permuting the u_i's if necessary, assume $b_1 \neq 0$. Then since G is closed under inverses, we may take $b_1 > 0$.

Enumerate all elements $x_1 u_1 + \ldots + x_r u_r$ of G and consider the set of possible positive integer values for x_1. We know this set is nonempty since b_1 is a possible value. Then call the smallest integer in this set a_{11} and take any element $v_1 = a_{11} u_1 + \ldots + a_{1r} u_r \in G$ for which this minimum is attained.

Then every element $x_1 u_1 + \ldots + x_r u_r \in G$ must satisfy $a_{11} | x_1$, since we have $x_1 = a_{11} q + b$ for integers q, b with $0 \le b < a_{11}$ (which implies $x_1 = b$ for some element of G), and we have chosen a_{11} to be minimal.

Thus for all $x \in G$, for some integer q we have $x - q v_1 = b_2 u_2 + \ldots + b_r u_r$ for some $b_2, \ldots, b_r$. If $r = 1$ then we are done since we have $F = \langle u_1 \rangle$, $G = \langle a_{11} u_1 \rangle$.

We use induction. Suppose $r > 1$. Let $F_1 = \langle u_2, \ldots, u_r \rangle, G_1 = G \cap G_1$. Then G_1 is a subgroup of F_1 and by inductive hypothesis $G_1 = \langle v_2, \ldots, v_s \rangle$ where $s \le r$ and

$$\begin{aligned} v_2 &= a_{22} u_2 + a_{23} u_2 + \ldots + a_{2r} u_r \\ v_3 &= a_{33} u_3 + \ldots + a_{3r} u_r \\ &\vdots \\ v_s &= a_{ss} u_s + \ldots + a_{sr} u_r \end{aligned}$$

with $a_{22}, \ldots, a_{ss}$ positive. We claim $v_1, \ldots, v_s$ generate G. We have already seen that for any $x \in G$, there exists some integer q such that $x - q v_1 \in F_1$. Then $x - q v_1 \in G_1$, hence $G = \langle v_1, \ldots, v_s \rangle$.

It remains to show that $v_1, \ldots, v_s$ are independent. Suppose not, that is, there exists a nontrivial relation $c_1 v_1 + \ldots + c_s v_s = 0$. We must have $c_1 \neq 0$ because by induction we cannot have a nontrivial relation between $v_2, \ldots, v_s$. Expressing the v_i's in terms of the u_i's, we arrive at a nontrivial relation between the u_i's since the coeffecient of u_1 is $c_1 a_{11} \neq 0$, a contradiction since the u_i's are independent. ▪

Now let $F = \langle u_1, \ldots, u_r \rangle$ be an abelian free group of rank r. Recall any set of generators of F is related to the u_i's via a unimodular matrix transformation, hence such a generator $b_1 u_1 + \ldots + b_r u_r$ must have $\gcd(b_1, \ldots, b_r) = 1$. The converse is also true:

Lemma: Let $F = \langle u_1, \ldots, u_r \rangle$. Let $v = b_1 u_1 + \ldots + b_r u_r$ with $\gcd(b_1, \ldots, b_r) = 1$. Then there exist $v_2, \ldots, v_r \in F$ with $F = \langle v, v_2, \ldots, v_r \rangle$.

Proof: Set $s = |b_1| + \ldots + |b_r|$. If $s = 1$ then the result is trivial, since we have $v = \pm u_i$ for some i. We shall induct on s.

If $s > 1$ then at least two of the b_i's are nonzero, and without loss of generality assume $b_1 \ge b_2 > 0$. Then set $u'_1 = u_1, u'_2 = u_1 + u_2, u'_j = u_j$ for $j \ge 3$. Clearly $F = \langle u'_1, \ldots, u'_r \rangle$, and we have $v = (b_1 - b_2) u'_1 + b_2 u'_2 + \ldots + b_r u'_r$ Furthermore $\gcd(b_1 - b_2, b_2, \ldots, b_r) = 1$ and $|b_1 - b_2| + |b_2| + \ldots + |b_r| < s$ so by inductive hypothesis the result follows. ▪

Theorem: Let F be a finitely generated free abelian group of rank r and let G be a subgroup of F of rank s with 0 <s≤r . Then there exist generators for F v 1 ,...,v r such that G =⟨h 1v 1,...,h sv s⟩ where h 1 ,...,h s are positive integers satisfying h i |h i +1 for i =1,...,s-1 .

Proof: Let u 1 ,...,u r be a set of generators for F . Take any x ∈G . Write x =x 1u 1+...+x ru r . Define δ (x)=gcd(x 1,...,x r) . We claim that δ (x) is independent of the choice of generators of F .

This is easily seen because if u ' 1,...,u' r are another set of generators, we can write the u i 's in terms of the u ' i 's showing that gcd (x 1,...x r)|gcd(x' 1,...,x' r) where x =x' 1u' 1+...+x' ru' r . By symmetry we must have equality.

Now take any nonzero y 1 ∈G such that δ (y 1) is minimal. Set h 1 =δ (y 1) . Then y 1 can be written y 1 =h 1(z 1u 1+...+z ru r) for some integers z i satisfying gcd (z 1,...,z r)=1 . By the lemma, there exist elements v ' 2,...v' r which together with v 1 generate F .

Hence an element y ∈G can be written y =w 1v 1+w' 2v' 2+...+w' rv' r Now h 1 must divide w 1 , since we have w 1 =qh 1+m for some 0 le0<h 1 and h 1 is minimal. (Consider δ (y-qy 1) .) Thus y -qy 1=t 2v' 2+...+t 2v' r If r =1 we are done, for we have s =1,F=⟨v 1⟩,G=⟨h 1v 1⟩ . We induct on r , so suppose r >1 .

Let F 1 =⟨v 1,v' 2,...,v' r⟩ and G 1 =F 1∩G . Then G 1 is a subgroup of F 1 whose rank we shall denote by t -1 where 0 <t≤r . If t =1 then G 1 =0 and since G =⟨hv 1⟩ we are done. Otherwise t <1 , and by inductive hypothesis there exist free generators v 2 ,...,v r of F 1 such that G 1 =⟨h 2v 2,...,h tv t⟩ where h i |h i +1 for i =2,..,t-1 . Now F =⟨v 1,...,v r⟩ and any y ∈G can be written y =q 1h 1v 1+g 1 for some g 1 ∈G 1 . Thus h 1 v 1,...,h tv t generate G . They must also be independent, becuause a nontrival relation between them imply a nontrivial relation between the generators v 1 ,...,v r of F .

Thus G =⟨h 1v 1,...,h tv t⟩ and t =s . It remains to show h 1 |h 2 . Write h 2 =ah 1+b where 0 ≤b<h 1 . Then consider y 0 =h 1v 1+h 2v 2∈G . We have 𝛿 (y 0)=gcd(h 1,h 2)=gcd(h 1,b) . By minimality of h 1 we must have b =0 . ▪

Finitely Generated Abelian Groups

Consider an abelian group A generated by m elements A =⟨a 1,...,a m⟩ Then the free abelian group of rank m F =⟨u 1,...,u m⟩ maps homomorphically onto A via the map that sends u i to a i . By the first isomorphism theorem we have A ≅F/R for some subgroup R of F . Pick a basis v 1 ,...,v m of F such that R =⟨h 1v 1,...,h qv q⟩ where h i |h i +1 , h i ≥1 , q ≤m .

Consider the case where m =1 . There are three possibilities. (1) R =⟨v⟩ , so F /R is the trivial group, (2) R =⟨hv⟩ , in which case F /R=ℤ h , and (3) R ={0} and we have F /R=F .

More generally, we have:

Theorem: Every finitely generated abelian group can be expressed as the direct sum of cyclic groups A =ℤ n⊕ℤ h 1 ⊕...⊕ℤ h n where h i |h i +1 .

Corollary: A finitely generated abelian group is free if and only if it is **torsion-free**, that is, it contains no element of finite order other than the identity.

The number r is called the **rank** of A . The orders of the cyclic groups h 1 ,...,h n are called the **invariants** of A . Note A is finite if and only if its rank is zero.

Theorem: Suppose A is a finitely generated abelian group with decompositions A =ℤ r⊕ℤ e 1 ⊕...⊕ℤ e n A =ℤ s⊕ℤ d 1 ⊕...⊕ℤ d m satifying e i |e i +1,d i|d i +1 . Then r =s,n=m,e i=d i .

Proof: Let T be the set of elements of A of finite order. Clearly if g ,h have finite order then ord (g)ord(h)(h-k)=0 hence h -k also has finite order hence T is a subgroup of A . It is called the **torsion group** of A .

A little thought shows that we must have T =ℤ e 1 ⊕...⊕ℤ e n T =ℤ d 1 ⊕...⊕ℤ d m Consider the map that projects A onto ℤ r . By the first isomorphism theorem we have that A /T≅ℤ r . Similarly we have A /T≅ℤ s hence r =s .

Now conisder T . Let p be a prime, and let P be the set of elements whose order is a power of P . Then P is a group. We first need the following:

Theorem: Let G be a finite abelian group of order p 1 a 1 p 2 a 2 ... where the p i 's are distinct primes. Then G =P 1⊕P 2⊕... where P i is the subgroup of elements whose orders are powers of p i .

Proof: Let x ∈G be an element of order p 1 α f 1 where f 1 ,p 1 are coprime. Then we may write x =a 1+x 1 where a 1 has order p 1 α and x 1 has order f 1 . (Simply take a 1 =uf 1x,x 1=vp 1 α x where u f 1+vp 1 α =1 .)

Iterating this procedure gives a decomposition x =a 1+a 2+... with a i ∈P i . We claim this decomposition is unique. Suppose 0 =b 1+b 2+... where b i ∈P i . Then for all i , subtracting b i from both sides shows that the order of b i is coprime to p i . But it must also be a power of p i which is only possible if b i =0 .

It is clear that the groups P i are uniquely determined. In fact, they are the Sylow groups since G is abelian. ▪

In particular, if x is an element of order n =p 1 a 1 p 2 a 2 ... then we have ⟨ x⟩=⟨(n/p 1 a 1)x⟩⊕⟨(n/p 2 a 2)

$x\rangle \oplus \dots$

Now let $e_1 = p_1^{a_1} p_2^{a_2} \dots, e_2 = p_1^{b_1} p_2^{b_2} \dots, \dots$ where $a_i \le b_i \le \dots$ for all i since $e_i | e_{i+1}$. Then we have $T = P_1 \oplus P_2 \oplus \dots \oplus Q_1 \oplus Q_2 \oplus \dots$ where $P_1, P_2, \dots, Q_1, Q_2, \dots$ are cyclic groups of order $p_1^{a_1}, p_1^{b_1}, \dots, p_2^{a_2}, p_2^{b_2}, \dots$. We see that the Sylow groups of T are $P = P_1 \oplus P_2 \oplus \dots, Q = Q_1 \oplus Q_2 \oplus \dots$. Now we need the following:

Lemma: Let G be any group. Suppose $x, y \in G$ commute and have relatively prime orders m, n. Then $\langle x, y \rangle = \langle xy \rangle$ is cyclic of order mn.

Proof: We know the order is at most mn since each element must be of the form $x^a y^b$ for $a = 0, \dots, m-1, b = 0, \dots, n-1$. Now suppose $(xy)^t = 1$. Then $1 = (xy)^{tm} = y^{tm}$ implying that $n | tm$. Since m, n is coprime we have $n | t$. Similarly $m | t$, thus the group order must be exactly mn. ■

Thus given $T = P_1 \oplus P_2 \oplus \dots \oplus Q_1 \oplus Q_2 \oplus \dots$ we deduce that $T = \mathbb{Z}_{e_1} \oplus \dots \oplus \mathbb{Z}_{e_n}$ so that one decomposition implies the other. We are done as soon as we show that the Sylow groups have a unique decomposition:

Theorem: Let A be an abelian group of order p^a where p is prime. Suppose $A = \langle u_1 \rangle \oplus \dots \oplus \langle u_k \rangle$ $A = \langle v_1 \rangle \oplus \dots \oplus \langle v_l \rangle$ where $u_1, \dots, u_k$ have orders $p^{f_1} \ge \dots \ge p^{f_k} > 1$, and $v_1, \dots, v_v$ have orders $p^{g_1} \ge \dots \ge p^{g_l} > 1$. Then $k = l$ and $f_i = g_i$ for $i = 1, \dots, k$.

Proof: Note we must have $a = f_1 + \dots + f_k = g_1 + \dots + g_l$. The theorem is trivial when $a = 1$, which we use to start an induction.

Let A_p be the set of elements $x \in A$ with $px = 0$. Then A_p is a subgroup. We have $A_p = \langle p^{f_1 - 1} u_1 \rangle \oplus \dots \oplus \langle p^{f_k - 1} u_k \rangle$ $A_p = \langle p^{g_1 - 1} v_1 \rangle \oplus \dots \oplus \langle p^{g_l - 1} v_l \rangle$ Hence $A_p = \mathbb{Z}_p^k = \mathbb{Z}_p^l$ implying that $k = l$.

Now consider the set A^p of elements px for all $x \in A$ (the multiples of p). Then A^p is a subgroup, and is generated by $pu_1, \dots, pu_k$ and also by $pv_1, \dots, pv_k$. But in general these are not bases for A^p since we might have $pu_i = 0$ for example. So find κ such that $f_1, \dots, f_\kappa \ge 2$ and $f_{\kappa+1} = \dots = f_k = 1$, and similarly find λ with $g_1, \dots, g_\lambda \ge 2$ and $g_{\lambda+1} = \dots = g_k = 1$.

This yields the decompositions $A^p = \langle pu_1 \rangle + \dots + \langle pu_\kappa \rangle = \langle pv_1 \rangle + \dots + \langle pv_\lambda \rangle$ By inductive hypothesis we have $\kappa = \lambda$ and $f_i - 1 = g_i - 1$ for all $i = 1, \dots, \kappa$. ■

We have now proved the main theorem. ■

In the last proof, the numbers $p^{f_1},\ldots,p^{f_k}$ are called the **elementary divisors** of A corresponding to p. A is said to be of **type** $(f_1,\ldots,f_k)$.

Example: Suppose an abelian group A is generated by a,b subject to the relations $30a=12b=0$. Then define the free abelian groups $F=\langle x,y\rangle$ and $R=\langle 30x,12y\rangle$. Note we have $A\cong F/R=\mathbb{Z}_{30}\oplus\mathbb{Z}_{12}$. Then we have $A\cong\mathbb{Z}_2\oplus\mathbb{Z}_3\oplus\mathbb{Z}_5\oplus\mathbb{Z}_4\oplus\mathbb{Z}_3\cong(\mathbb{Z}_4\oplus\mathbb{Z}_2)\oplus(\mathbb{Z}_3\oplus\mathbb{Z}_3)\oplus\mathbb{Z}_5$ Thus the elementary divisors for $2,3,5$ are $(4,2),(3,3),5$. Rearranging gives $A\cong\mathbb{Z}_{60}\oplus\mathbb{Z}_6$, so the invariants are $60,6$.

Example: Suppose an abelian group A is generated by a,b,c,d and the relations $3a+9b-3c=0, 4a+2b-2d=0$. Then define the free abelian groups $F=\langle x,y,z,t\rangle$ and $R=\langle 3u,2v\rangle$ where $u=x+3y-z, v=2x+y-t$. Note x,y,u,v is also a basis of F. Thus $A\cong F/R\cong\mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z}_3\oplus\mathbb{Z}_2\cong\mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z}_6$

Generators and Relations

Suppose we have a set of symbols $\{x_1,\ldots,x_n\}$. Consider the **words** we may form from them, that is, formal products of the form $x_{i_1}^{a_1}\ldots x_{i_k}^{a_k}$ where the exponents are integers (and may be negative). The **empty word** is denoted by 1. A word is **reduced** if it is empty or no two consecutive x's have the same subscript. Define multiplication on words by concatenation. We may reduce a word by using the rules $x^a x^b=x^{a+b}$ and $x^0=1$.

It can be shown that we have constructed a **free group** in this manner. The only nontrivial fact to verify is that concatenation is indeed associative, which is tedious and will be omitted.

Now consider a group G that is generated by n elements $g_1,\ldots,g_n$. Then consider the map from the free group F generated by n elements that sends x_i to g_i. The kernel of this map R consists precisely of nontrivial relations $r(x_1,\ldots,x_n)$ such that $r(g_1,\ldots,g_n)=1$. Summarizing:

Theorem: Every group G which can be generated by n elements can be represented as the homomorphic image of the free group F on n generators. The kernel of this map consists of elements of F that correspond to relations in G.

The groups F,R are said to form a **presentation** of G. Conversely given any normal subgroup R of a free group F, we may form a group F/R.

Now suppose we are given m relations $r_1,\ldots,r_m$ on n elements $x_1,\ldots,x_n$. The group consisting of the smallest normal subgroup of F that contain all m relations is denoted by $R=\{r_1,\ldots,r_m\}^F$ and is called the **normal closure** of $r_1,\ldots,r_m$ and may be called the **relation group** of $G=F/R$.

Now suppose H is another group with generators $g_1,\ldots,g_n$ that satisfies all the relations that G does, but in addition also satisfies relations $t_1,\ldots,t_p$. Then consider S ={r 1,...,r m,t 1,...,t p} F . We have H =F/S . Since S ⊃R as in the third isomorphism theorem we may view A =S/R as a normal subgroup of F / R , and we have H ≅G/A , thus:

Theorem: If new relations are added to a group G , the resulting group is a homomorphic image of G .

Hence F /R is the freest group with n generators satisfying given relations r 1 ,...,r m .

As an application, we can make a group G abelian by considering G /G' where G ' is the normal closure of relations of the form g i - 1 g j - 1g ig j for all i ,j .

Example: Let G be the quarternion group ⟨ a,b|a 4=1,a 2=b 2,ba=a 3b⟩ . Then G /G' is generated by u =aG',v=bG' . In additive notation we have 4 u=0,2u=2v,v+u=3u+v , thus 2 u=2v=0 and we find G /G'=ℤ 2×ℤ 2 .

If the free group on x 1 ,...,x n is made abelian then we obtain the free abelian group on x 1 ,...,x n . This implies that free groups on different numbers of generators cannot be isomorphic, otherwise we would have their abelian counterparts isomorphic, a contradiction by a previous result.

Fact: A subgroup of a free group that contains more than one element is a free group.