GROUPS

SECOLINSKY

We define the concept of a group. Let G be a nonempty set equiped with a binary operation $*$. We say G is a group whenever all the following properties hold:

(i) Associativity: For any three elements a, b, c in G, $(ab)c = a(bc)$.
(ii) Identity: There is an element $e \in G$ such that for any element $a \in G$, $ae = ea = a$.
(iii) Inverses: For every element $a \in G$, there is an element $b \in G$ such that $ab = ba = e$.

A subgroup H of G is just a subset of G equipped with the same three properties with respect to the operation $*$. So We'll denote a group as $< G, * >$. This object of a group has a structure which needs to be examined to understand algebraic systems. So we begin the journey.

Statement 1. *Consider* $< G, * >$ *where* $a, b, c \in G$. *Then* $ab = ac \Rightarrow b = c$.

Proof. Using the proerties of a group, first observe that $a^{-1}(ab) = a^{-1}(ac)$. The left side of the equation simplifies to $a^{-1}(ab) = (a^{-1}a)b = e(b) = b$ and the right side of the equation simplifies to $a^{-1}(ac) = (a^{-1}a)(c) = ec = c$. Thus $b = c$. □

A binary operation on a set G takes two of its elements and yields some element in G. If this is not the case, then we don't have a binary operation and hence no group.

Example 1. $\mathbb{Z}_6/\{0\}$ *is not a group under modular multiplication since* $4\ 3 = 0 \notin \mathbb{Z}_6/\{0\}$.

Intuition of groups naturally come from our experience in arithmetic. The next group introduced will show that there are groups whose elements do not have to commute.

A permutation on a set S of n positive integers is a bijection on S. The collection of all such bijections is a group under the operation of function composition and is known as the symmetric group. It is denoted as S_n. Elements of S_n are written in cycle notation where they are read from right to left.

Example 2. *The permutation on the set* $\{1, 2, 3, 4, 5\}$ *which maps* 2 *to* 3, 3 *to* 5, 5 *to* 2 *and all others to themselves is expressed as* $(2\ 3)(3\ 5) = (3\ 5\ 2)$.

There is much to be said about cycle notation and the group S_n. Statements like the following:

Statement 2. *Consider the 5-cycle* $(3\ 5\ 7\ 8\ 6) = (3\ 6)(3\ 8)(3\ 7)(3\ 5)$. *The above example suggests the following relationship for a k-cycle:* $(a_1\ a_2\ ...\ a_k) = (a_1\ a_k)(a_1\ a_{k-1})...(a_1\ a_2)$.

The purpose now is not to manipulate the elements of S_n with its operation , but to just show the following fact that there are groups whose elements may not commute. Groups that do have the property of all elements commuting with each other are said to be Abelian.

Statement 3. *The symmetric group* S_5 *is not Abelian since* $(2\ 3)(3\ 5) = (3\ 5\ 2) \neq (3\ 2\ 5) = (3\ 5)(2\ 3)$

So what groups are Abelian? How about those that are generated by at least one of its elements, the cyclic groups. Give a little thought, and it'll be clear that they are Abelian.

Definition 1. $< G, * >$ *is cyclic if there is an element* $a \in G$ *such that* G *is equal to* $< a >= \{x \in G : x = a^n$ *for some nonnegative integer* $\}$.

All subgroups of $\mathbb{Z}$ are Abelian since they are cyclic and every cyclic group is Abelian. For $\mathbb{Z}$ we have 1 as the generator, i.e., $\mathbb{Z} =< 1 >$. But why all subgroups? It follows from the fact that all subroups of a cyclic group are cyclic. We present the result as a theorem whose proof is omitted.

Theorem (Fundamental Theorem of Cyclic Groups)**.** *Let* G *be a group and* H *be a subgroup of* G*. Then* G *is cyclic implies that* H *is cyclic.*

The group of units modulo n, denoted as $U(n)$, is defined as the set of positive integers relatively prime to n equiped with the operation of multiplaction modulo n. All group of units modulo n are Abelian. Not all are cyclic.

Now consider the group $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$. All the cyclic subgroups of $U(15)$ have an order which divides 8: $< 1 >= \{1\}$, $< 4 >= \{1, 4\}$, $< 11 >= \{1, 11\}$, $< 14 >= \{1, 14\}$, $< 2 >=< 8 >= \{1, 2, 4, 8\}$ and $< 7 >=< 13 >= \{1, 4, 7, 13\}$. Since all these cyclic subgroups have size less than eight, we know none can be $U(15)$ and thus $U(15)$ can't be cyclic. This establishes a counterexample to the converse of the statement "If a group is cyclic, then it is Abelian".

But what if obtaining all cyclic subgroups is a formidable task not worth taking. Then we are better off with the approach of using the contrapositive of the Fundamental Theorem of Cyclic Groups. That is, to find a non-cyclic subgroup H which would then yield the result of G being non-cyclic.

$U(15)$ is non-cyclic because there is a proper subgroup of $U(15)$ which is non-cyclic. Namely, $\{1, 4, 11, 14\} \subset U(15)$. To see that this set is indeed a subgroup, observe the following Cayley table:

$*$	1	4	11	14
1	1	4	11	14
4	4	1	14	11
11	11	14	1	4
14	14	11	4	1

Given a group, we can easily have a subgroup. Take a subset of a group G whose elements are those which commute with all elements of the group. This subset is named the center and is expressed as $\{g \in G : (\forall h \in G)(\ gh = hg\ )\}$. In general, to establish that a subset is a subgroup it is enough to show that it is nonempyt and that it is closed under both the group operation and from taking inverses. This method of proof is named the two-step subgroup test. It'll be used to prove that the center $Z(G)$ is a subgroup.

Statement 4. *The center of* G *is a subgroup.*

Proof. First note that $Z(G) \neq \emptyset$ since $e \in Z(G)$. So let $a, b \in Z(G)$ and $h \in G$ and note that $(ab)h = a(bh) = a(hb) = (ah)b = (ha)b = h(ab)$. Thus $ab \in Z(G)$. Finally we'll

show closure under inverse. Since $(ah) = (ha)$, $a^{-1}(ah)a^{-1} = a^{-1}(ha)a^{-1}$. The left side of the equation simplifies to $a^{-1}(ah)a^{-1} = (a^{-1}a)ha^{-1} = eha^{-1} = ha^{-1}$ and the right side simplifies to $a^{-1}(ha)a^{-1} = a^{-1}h(aa^{-1}) = a^{-1}h$. Thus $a^{-1}h = ha^{-1}$. Now since closure under inverses and closure under the operation have both been shown, we can conclude that $Z(G)$ is a subgroup of G. □

There are phrases and conventional ways of writing mathematics that may throw off many readers. One is the phrase about a condition being "necessary and sufficient". To explain these terms, let us say that P and Q are some statements. "If P, then Q" is equivalent to saying that P implies Q and is written in symbols as $P \Rightarrow Q$. In this context it is said that Q is the necessary condition and that P is the sufficient condition.

Here is a statement which gives a sufficient condition for a group to be cyclic.

Statement 5. *Let G be a group and $\mathcal{A}$ be the collection of all subgroups of G. $\mathcal{A} = \{\{e\}, G\} \Rightarrow G$ is cyclic.*

Proof. Assume that the only subgroups of G are $\{e\}$ and the set itself and consider $e \neq a \in G$. Note that $< a > \neq \{e\}$ and is a subgroup of G. Therefore $< a >$ must be equal to G. □

More can be said about such a group G. Assume that $|G| < \infty$. It then follows that $|G| \mid |G|$ and $1 = |\{e\}| \mid |G|$ are the only divisors of $|G|$. Therefore, the order of G must be prime.

Here is another common notation. A proper subroup H of G will be denoted in symbols as $H < G$. To continue with the general treatment of groups, we ask how to have more subgroups of G given that we know of one already. The following two Statements 6, 7 show us how.

Statement 6. *Let G be a group, $H \leq G$ and $x \in G$. Then*

(i) $xHx^{-1} \leq G$;
(ii) *H is cyclic* $\Rightarrow xHx^{-1}$ *is cyclic; and*
(iii) *H is Abelian* $\Rightarrow xHx^{-1}$ *is Abelian.*

The subgroup xHx^{-1} is referred to as a conjugate of H. Conjugation preserves structure.

Proof. We first show that xHx^{-1} is a subgroup of G. So note that $e = xex^{-1} \in xHx^{-1}$. Now let $a, b \in xHx^{-1}$ so that $a = xh_1x^{-1}$ and $b = xh_2x^{-1}$. So $ab^{-1} = xh_1x^{-1}(xh_2x^{-1})^{-1} = xh_1x^{-1}xh_2^{-1}x^{-1} = xh_1h_2^{-1}x^{-1} \in xHx^{-1}$. Thus $xHx^{-1} \leq G$.

To show the second part, let $H = \langle a \rangle$ so that $xHx^{-1} = x\langle a \rangle x^{-1} = \{xa^nx^{-1} : n \in \mathbb{Z}\} = \{(xax^{-1})^n : n \in \mathbb{Z}\} = \langle xax^{-1} \rangle$. Thus xHx^{-1} is cyclic.

Finally, assume H is Abelian so that $ab = xh_1x^{-1}xh_2x^{-1} = xh_1h_2x^{-1} = xh_2h_1x^{-1} = xh_2x^{-1}xh_1x^{-1} = ba$. Thus xHx^{-1} is Abelian. □

Statement 7. *Let G be a group, $H \leq G$, and $N(H)$ be the set of all elements in G whose conjugates of H are equal to itslef. Then $N(H) \leq G$.*

Proof. We have that $N(H) = \{x \in G : xHx^{-1} = H\}$ so first note that $H = eHe^{-1}$ implies $N(H) \neq \emptyset$. Now let $a, b \in N(H)$ so that $aHa^{-1} = H$ and $b^{-1}Hb = H$. So $ab^{-1} \in N(H)$ since $H = aHa^{-1} = a(b^{-1}Hb)a^{-1} = ab^{-1}H(ab^{-1})^{-1}$. Thus $N(H) \leq G$. This completes the proof. The group $N(H)$ is called the normalizer of H in G. □

Just as we have a subgroup of G for granted, i.e. the center, we also have a partition of G we can take for granted.

Statement 8. *Let G be a group, $cl(a) = \{xax^{-1} : x \in G\}$ be called the conjugacy class of $a \in G$, and $\mathcal{A}$ be the set of all conjugacy classes. Then $\mathcal{A}$ is a partition of G.*

Proof. We have that $\mathcal{A} = \{cl(a) : a \in G\}$. First note that $a \in cl(a)$ since $a = eae^{-1}$, and so it is clear that $G = \bigcup_{A \in \mathcal{A}} A$. We'll now show that for all $A, B \in \mathcal{A}$, if $A \cap B \neq \emptyset$, then $A = B$. So let $y \in cl(a) \cap cl(b) \neq \emptyset$. So for some $x_1, x_2 \in G$, $y = x_1 a x_1^{-1} = x_2 b x_2^{-1}$, and so $b = x_2^{-1} x_1 a x_1^{-1} x_2$. Now let $u \in G$ so that $ubu^{-1} \in cl(b)$. So $ubu^{-1} = (ux_2^{-1}x_1)a(x_1^{-1}x_2u^{-1}) \in cl(a)$. Thus $cl(b) \subset cl(a)$. By parallel argument, $cl(a) \subset cl(b)$. So we have shown that for all $A, B \in \mathcal{A}$, $A \cap B \neq \emptyset$ implies $A = B$. Therefore $\mathcal{A}$ is a partition of G. □

Is it possible for a group to be expressed as the union of two proper subgroups? The proof of an answer will be left as a good exercise. We continue with statements about subgroups as we present the next definition.

Definition 2. *Let G be a group. A subgroup H of G is normal when for all $a \in G$, $aH = Ha$. This is equivalent to $G = N(H)$. The relation is denoted as $H \lhd G$. If the only normal subgroups of G are $\{e\}$ and itself, then we say it is simple.*

Statement 9. *A group is a normal subgroup of itself.*

Proof. First note that $G \leq G$. Now let $a \in G$. We then have that $aG = G = Ga$ which completes the proof that $G \lhd G$. □

Give a little thought and it'll be clear that another normal subgroup of G is its center $Z(G)$.

What else can help us discover more about a group. Similar to the result that any subgroup of a cycic group is cyclic, we will show using the next two statements that any subgroup of an Abelian group is normal. It is worth noting that both these results allow us to know something about all subgroups from just knowing that it holds for the group. What now follows are the tools used for discovery.

Statement 10. *H is a normal subgroup of G is equivalent to $aHa^{-1} \subset H$ for all $a \in G$.*

Proof. Assume $H \lhd G$ and let $a \in G$ so that $aHa^{-1} = H$. Obviously $aHa^{-1} \subset H$. Now to prove the converse consider the subgroups aHa^{-1} and $a^{-1}Ha$. We'll first show that $aHa^{-1} \subset H$ implies $aH \subset Ha$. So let $x \in aH$ so that $x = ah_1$. Then $xa^{-1} = ah_1a^{-1} \in aHa^{-1} \subset H$ and thus $xa^{-1} \in H$. We then have that $x = (xa^{-1})a \in Ha$. By parallel argument, $a^{-1}Ha \subset H$ implies $aH \supset Ha$ and thus $aH = Ha$. □

Statement 11. *Let H be a subgroup. Then $aH \subset Ha \Leftrightarrow aHa^{-1} \subset H$.*

Proof. Let $x \in aHa^{-1}$ so that for some $h_1 \in H$, $x = ah_1a^{-1}$. Since then $xa = ah_1 \in aH$, $xa \in Ha$ and thus $xa = h_2a$ where $h_2 \in H$. Hence $x = (xa)a^{-1} = (h_2a)a^{-1} = h_2 \in H$. Therefore, $aHa^{-1} \subset H$. Now to prove the converse. Let $x \in aH$ so that $x = ah_1$. It then follows that $xa^{-1} = ah_1a^{-1} \in aHa^{-1}$ which implies that $xa^{-1} \in H$. Thus $xa^{-1} = h_2$ and the result follows from $x = (xa^{-1})a = h_2a \in Ha$. □

Note that the variables h_1, h_2 of the first part of the proof of Statement 11 were not the same as the second part when we proved the converse.

Statement 12. *If G is Abelian then all of its subgroups are normal.*

Proof. Let $H \leq G$, $a \in G$, and $x \in aH$ so that for some $h_1 \in H$, $x = ah_1 = h_1a \in Ha$. Thus $aH \subset Ha$. □

A corrollary to Statement 12 is that an Abelian group with more than two subgroups isn't simple.

Consider the sets $SL(2,\mathbb{R})$ and $GL(2,\mathbb{R})$ of all 2 x 2 real matrices whose determinants are 1 and non-zero, respectively. Each is a group under matrix multiplication and they are related in the sense that $SL(2,\mathbb{R}) \leq GL(2,\mathbb{R})$. They are called the standard and genereal linear group.

The proof of the following statement uses the fact from linear algebra that the determinant of a product of matrices is the product of the determinants of each.

Statement 13. $SL(2,\mathbb{R}) \lhd GL(2,\mathbb{R})$

Proof. Let $A \in GL(2,\mathbb{R})$. To show that $SL(2,\mathbb{R})$ is a normal subgroup of $GL(2,\mathbb{R})$, consider $M \in A[SL(2,\mathbb{R})]A^{-1}$ so that $M = ABA^{-1}$ for some $B \in SL(2,\mathbb{R})$. Since $det(M) = det(ABA^{-1}) = \frac{det(A)det(B)}{det(A)} = det(B) = 1$, $M \in SL(2,\mathbb{R})$. Thus $A[SL(2,\mathbb{R})]A \subset SL(2,\mathbb{R})$ which finishes the proof that $SL(2,\mathbb{R})$ is a normal subgroup of $GL(2,\mathbb{R})$. □

One of the first few big theorems learned in group theory is Lagrange's theorem. It is a statement about finite groups and their subgroups. In the context of this theorem, order is used to refer to the size of the finite group, i.e. its cardinality.

Theorem (Lagrange's Theorem)**.** *Let G be finite. Then the order of any subgroup divides the order of the group.*

Left and right cosets are aH and Ha, where H is a subgroup of G. The proof of Lagrange's theorem uses the fact that distinct left cosets partition G. From such a proof we observe the number of distinct left cosets of H in G to be the order of G divided by the order of H. No need trying to prove it since the properties of cosets used to derive the partition fact haven't been treated properly.

The theme of how to obtain a new group from knowing very little about a group is continued in the following definition.

Definition 3. *Let $H \lhd G$. Then $\{aH : a \in G\}$ is a group with the operation defined as $(aH)(bH) = (ab)H$ and is called a factor group, quotient group, or G mod H. It is denoted as G/H.*

The proof that G/H is indeed a group will be left as an exercise. From the definition it then follows that for when G is finite, $|G/H| = \frac{|G|}{|H|} = |G : H|$ where $|G : H|$ is refferred to as the index of H in G. We have, from Lagrange's theorem, the index of H in G to be the number of distinct left cosets of H in G.

The proof of what follows next will have us revisit familiar concepts. Here is our first statement involving a factor group. It will then be applied to say something about the center when knowing something about the group.

Statement 14. *Let G be a group. Then the quotient group $G/Z(G)$ being cyclic implies G is Abelian.*

Proof. Let $a, b \in G$. Since $G/Z(G) =< gZ(g) >$ for some $g \in G$ and $G/Z(G)$ partitions G, $a \in g^m Z(G)$ and $b \in g^j Z(G)$ for some $m, j \in \mathbb{Z}$. So $a = g^m h_1$ and $b = g^j h_2$ for some $h_1, h_2 \in Z(G)$. Thus $ab = g^m(h_1 g^j)h_2 = g^m g^j h_1 h_2 = g^j g^m h_1 h_2 = g^j h_2 g^m h_1 = ba$. □

To prepare for the proof of the next statement about the center, try proving that a group of prime order is cyclic. This exercise will involve taking a cyclic subgroup of an element of G not equal to the identity and applying Lagrange's theorem.

Statement 15. *Let p and q be prime and G be a group whose size is pq. Then G is non-Abelian implies that $Z(G) = \{e\}$.*

Proof. Assume to the contrary that $Z(G) \neq \{e\}$. Since G is non-abelian, $G \neq Z(G)$ and hence, by Lagrange's theorem and the fact that p and q are prime, $|Z(G)| = p$ or q. Thus $|G/Z(G)| = p$ or q and so $G/Z(G)$ is cyclic. Hence G is Abelian, a contradiction. □

So far we have seen a few ways how groups can be created and related. Functions provide another way. A homomorphism $\phi : G \to \overline{G}$ is an example which relates two groups in the following sense: for every two elements x, y in G, $\phi(xy) = \phi(x)\phi(y)$.

Before discussing more about these functions relating groups, we make just one simple statement about functions. It serves to build our confidence and comfort with the concept.

Statement 16. *Let S be a finite set and $\phi : S \to S$. Then ϕ is injective is equivalent to it being surjective.*

Proof. Let $|S| = n$ and assume to the contrary that ϕ is injective and not surjective. This results in there being a $z \in S$ such that for all $x \in S$, $\phi(x) \neq z$. It then follows that $|\phi(S)| < n$ and so there must be $m, p \in S$ such that both $m \neq p$ and $\phi(m) = \phi(p)$, a contradiction.

To show the converse, assume again to the contrary that ϕ is surjective and not injective. Since ϕ isn't injective, there are $x, y \in S$ such that $x \neq y$ and $\phi(x) = \phi(y)$. Therefore $|\phi(S)| < n$. Thus there is a $z \in S$ such that for all $x \in S$, $\phi(x) \neq z$, a contradiction. □

Similar to our treatment of cosets, the properties of homomorphisms used to derive the results which follow will not be treated properly, but be taken for granted. The next few statements use the fact of a homomorphism that $\phi(x^n) = \phi(x)^n$ for any integer n.

Statement 17. *Let $\phi : G \to \overline{G}$ be a homomorphism and $\{x \in G : \phi(x) = \overline{e}\}$ be the kernel of ϕ denoted as $\ker \phi$. Then ϕ is injective is equivalent to $\ker \phi = \{e\}$.*

Proof. Assume ϕ is injective and let $x \in \ker \phi$. Because $\phi(x) = \overline{e}$, $x = e$. Now to prove the converse, assume $\ker \phi = \{e\}$ and that $\phi(x) = \phi(y)$. It then follows that $\overline{e} = [\phi(x)]^{-1}\phi(x) = \phi(x^{-1})\phi(x) = \phi(x^{-1})\phi(y) = \phi(x^{-1}y)$. Since $x^{-1}y \in \ker \phi = \{e\}$, $x = y$. Thus ϕ is injective. □

Statement 18. *Let $\phi : G \to \overline{G}$ be a homomorphism. Then $\ker \phi$ is a subgroup of G.*

Proof. Since $e \in \ker \phi$, $\ker \phi \neq \emptyset$. Now let $x, y \in \ker \phi$ so that $\overline{e} = \phi(x)^{-1}\phi(x) = \phi(x^{-1})\phi(y) = \phi(x^{-1}y)$. Thus $x^{-1}y \in \ker \phi$. Therefore $\ker \phi$ is a subgroup of G. □

Statement 19. *Let $\phi : G \to \overline{G}$ be a homomorphism. Then $\ker \phi$ is a normal subroup of G.*

Proof. Let $a \in G$ and $x \in a(\ker \phi)a^{-1}$ so that there's a $h_1 \in \ker \phi$ such that $x = ah_1a^{-1}$. Because $\phi(x) = \phi(a)\phi(h_1)\phi(a)^{-1} = \overline{e}$, $x \in \ker \phi$. Thus $a(\ker \phi)a^{-1} \subset \ker \phi$. It has thus been shown that $\ker \phi \lhd G$. □

Statement 20. *Let G be a group, $N \lhd G$, and $\phi : G \to G/N$ where $\phi(g) = gN$. Then ϕ is a homomorphism and $N = \ker \phi$.*

Proof. Let $a, b \in G$ so that $\phi(ab) = abN = aNbN = \phi(a)\phi(b)$. Thus ϕ is a homomorphism. Now $\ker \phi = \{g \in G : \phi(g) = N\} = N$. □

When two groups are the same in structure, what does it mean and how do we express it? The detailed description of sameness isn't unfamiliar. An isomorphism is just a bijective homomorphism. When such a function exists between two groups, we say they are isomorphic and denote it with the $\cong$ symbol. Here is a general example. It is constructed from first knowing a homomorphism and its kernel.

Statement 21. *Let $\phi : G \to \overline{G}$ be a homomorphism. Then $\phi(G)$ is isomorphic to $G/\ker\phi$.*

Proof. Let $\rho : G/\ker\phi \to \phi(G)$ where $\rho(a\ker\phi) = \phi(a)$. We have that ρ is a well defined map. To see this, let $a\ker\phi = b\ker\phi$ so that $a^{-1}b \in \ker\phi$. Since ϕ is a homomorphism, $\overline{e} = \phi(a^{-1}b) = \phi(a)^{-1}\phi(b)$ and thus $\phi(b) = \phi(a)$. Now to show that ρ is bijective.

Let $\phi(a) = \rho(a\ker\phi) = \rho(b\ker\phi) = \phi(b)$ so that $\overline{e} = \phi(a^{-1})\phi(b)$, i.e., $a^{-1}b \in \ker\phi$. Thus $a\ker\phi = b\ker\phi$ and so ρ is injective. Now to prove that it is surjective.

Let $y \in \phi(G)$ so that for some $g \in G$, $y = \phi(g) = \rho(g\ker\phi)$. Hence ρ is surjective. Finally, we show ρ to preserve operation with the chain of relations $\rho(a\ker\phi b\ker\phi) = \rho(ab\ker\phi) = \phi(ab) = \phi(a)\phi(b) = \rho(a\ker\phi)\rho(b\ker\phi)$. Therefore, $\phi(G) \cong G/\ker\phi$. $\square$