

1.

This semester we studied group theory in some depth. Write an essay that describes the different types of groups and subgroups we encountered and why each type is important. Your discussion should include relevant definitions, relationships between the different types of groups, examples and non-examples to explain the relationships, and various methods for constructing new groups from old. You do NOT need to include any proofs in this essay. Your essay will be graded on how complete and through it is.

We will first go over the basics of what a group is and some subgroups that occur in all groups. A group is a set G on which one binary operation, denoted \cdot , is defined such that the following axioms hold true. The set G is closed under its operation, the operation \cdot is associative in G , the set G contains an identity element, and the set G contains an inverse for each of its elements. In addition, a group is Abelian if the operation is commutative in G .

One of the first classes of groups that we mentioned in class was the dihedral groups. A dihedral group is denoted D_n where n is some positive integer greater than or equal to three. A dihedral group is made up of all of the symmetries of a normal n -gon with composition as its operation. For example, D_3 would be the set of all the symmetries of an equilateral triangle. Another group that we talked about latter in the semester is the group of permutations, denoted S_n . This group contains all of the symmetries of the group D_n , but also contains some permutations that are not symmetries. In fact, D_n is a subgroup of S_n . Another interesting result is Cayley's Theorem which states that every group is a subgroup of a group of permutations. This is interesting, because it means that all group theory can be reduced to the study of permutations.

In order to better understand a group it can be useful to study the subgroup of a group. A subset H of a group G is a subgroup if H is a group using the same operation as in G . One of the first subgroups that we mentioned in class was the center of a group. The center of a group is the set of all elements that commute in this group. If a group is Abelian, then the center of this group is simply the group itself. One reason that the center of a group is useful is that it is always normal which we will talk about latter.

Another example of a subgroup is the cyclic subgroup. A cyclic subgroup of G is the smallest subgroup containing some element in G and is denoted $\langle a \rangle$ where $a \in G$. A group G is cyclic if it contains a generator a such that $G = \langle a \rangle$. A unique trait of cyclic groups is that every subgroup of a cyclic group is cyclic. At this point it may be useful to introduce presentations. Presentations are made up of a set contains generators of a group G and relations that define the group. A cyclic group G with order n and generator a has the presentation $\langle a | a^n = 1 \rangle$. The dihedral group D_n has the presentation $\{r, R | r^2 = 1, R^n = 1, rR = R^{-1}r\}$.

Finally, we have the normal subgroups. These subgroups are important, because they allow us to break a group down into simpler quotient groups. Many theorems rely on normal subgroups and their quotients. Normal subgroups can be used to break groups up into two parts, trivial and nontrivial groups. A trivial group is a group in which the only normal subgroups are itself and a subgroup containing the identity. A nontrivial group is simply a group that is not trivial. Mathematicians have been able to classify all of the finite simple groups into either an infinite family where there is an established pattern or in one of the sporadic groups. A group N is a normal subgroup of G , denoted $N \triangleleft G$, if for all $a \in G$, $aN = Na$. In other words if all left and right cosets are equal, a subgroup is normal. A left coset being the set $aN = \{an : n \in N\}$ for some a in G . When $N \triangleleft G$ we can create the following group $G/N = \{aN : a \in G\}$ with the operation with the operation $(aN)(bN) = (ab)N$ for all $a, b \in G$. This group is referred to as the quotient group of G by N . A quotient group can tell us some important things about the original group. For example, if G is a group and $G/Z(G)$ is cyclic, then G is Abelian.

Two ways of constructing new groups from old are with internal and external direct products. The external direct product of the groups G and H , denoted $G \oplus H$, is the set of their Cartesian product with the operation $(g_1, h_1)(g_2, h_2) = (g_1 \cdot_G g_2, h_1 \cdot_H h_2)$. The internal direct product of the normal subgroups K and N of G such that $K \cap N = \{e_G\}$ is denoted $G \times H$ and should not to be confused with the Cartesian product. It consists of the set $\{kn : k \in K, n \in N\}$ with the operation \cdot_G .

2.

(a) The operation table for U_{44} is given in Table 1. Explain why $U_{44} = \langle [3] \rangle \times \langle [21] \rangle$, the internal direct product of the subgroups $\langle [3] \rangle$ and $\langle [21] \rangle$.

First of all, $\langle [3] \rangle = \{[1], [3], [9], [15], [23], [25], [27], [31], [37]\}$ and $\langle [21] \rangle = \{[1], [21]\}$. From this we see that the intersection of $\langle [3] \rangle$ and $\langle [21] \rangle$ contains only $[1]$. From Theorem 26.6 (2) we can conclude that each element in $\langle [3] \rangle \times \langle [21] \rangle$ has a unique representation kn where $k \in \langle [3] \rangle$ and $n \in \langle [21] \rangle$. And so, $|\langle [3] \rangle \times \langle [21] \rangle| = |\langle [3] \rangle| \cdot |\langle [21] \rangle| = 10 \cdot 2 = 20$. From the closure property of the group G and the fact that $\langle [3] \rangle$ and $\langle [21] \rangle$ are subgroups of G we know that each element in $\langle [3] \rangle \times \langle [21] \rangle$ is also in G . From this fact and the fact that $\langle [3] \rangle \times \langle [21] \rangle$ and G have the same order, it must be the case that $G = \langle [3] \rangle \times \langle [21] \rangle$.

(b) When we decompose a group as an internal direct product, it is convenient for classification purposes to identify that internal direct product with an external direct product. Let G be an arbitrary group with identity element e and let K and N be normal subgroups of G with $K \cap N = \{e\}$. Prove that

$$K \times N \cong (K \oplus N).$$

Proof. We will prove that $\phi : K \oplus N \rightarrow K \times N$ such that $\phi((k, n)) = kn$ for all $k \in K$ and for all $n \in N$ is an isomorphism. In doing so we will have proven that $K \oplus N$ and $K \times N$ are isomorphic and therefore $(K \oplus N) \cong (K \times N)$.

First we will show that the ϕ is in fact a function. This means that it is well-defined. Let $(k, n) = (k', n') \in K \oplus N$. We will prove that $\phi((k, n)) = \phi((k', n'))$. We see that

$$\phi((k, n)) = kn = k'n' = \phi((k', n'))$$

and therefore ϕ is a function.

Next we will show that ϕ preserves structure and therefore is a homomorphism. Let $(k, n), (k', n') \in K \oplus N$. First we see that

$$\phi((k, n)(k', n')) = \phi((kk', nn')) = (kk')(nn').$$

From Theorem 26.6 (1) we know that $k'n = nk'$. Therefore,

$$\phi((k, n)(k', n')) = (kk')(nn') = k(k'n)n' = k(nk')n' = (kn)(k'n') = \phi((k, n))\phi((k', n'))$$

and ϕ preserves the operation in G .

Finally, we will show that ϕ is both injective and surjective. Let $\phi((k, n)) = \phi((k', n'))$. First we note that

$$kn = \phi((k, n)) = \phi((k', n')) = k'n'$$

and so $kn = k'n'$. From Theorem 26.6 (2) we know that kn is a unique representation of an element in $K \times N$, which means that k must be equal to k' and n must be equal to n' . Therefore, $(k, n) = (k', n')$ and ϕ is injective.

Let $kn \in K \times N$. The element $(k, n) \in K \oplus N$ is such that $\phi((k, n)) = kn$ and so ϕ is surjective. \square

Explain why $U_{44} \cong (\mathbb{Z}_{10} \oplus \mathbb{Z}_2)$.

Because $\mathbb{Z}_{10} \cap \mathbb{Z}_2 = [1]$, it follows that $\mathbb{Z}_{10} \times \mathbb{Z}_2 = U_{44}$ in a similar manner to part (a). Also from part (b) we know that $U_{44} = \mathbb{Z}_{10} \times \mathbb{Z}_2 \cong \mathbb{Z}_{10} \oplus \mathbb{Z}_2$. Therefore, $U_{44} \cong (\mathbb{Z}_{10} \oplus \mathbb{Z}_2)$.

3.

(a) Let $G = U_{44}$. Let $N = \langle [3] \rangle$ and let $K = \langle [9] \rangle$. The operation table for U_{44} is shown in Table 1. Find G/K , G/N , N/K , and $(G/K)/(N/K)$. Explain why $(G/K)/(N/K) \cong G/N$. First of all,

$$G/K = \{K, [3]K, [7]K, [13]K\},$$

$$G/N = \{N, [7]N\},$$

$$N/K = \{K, [3]K\},$$

and

$$(G/K)/(N/K) = \{N/K, ([7]K)(N/K)\}.$$

The groups $(G/K)/(N/K)$ and G/N both have only two elements and therefore are both isomorphic with \mathbb{Z}_2 . And so, $(G/K)/(N/K) \cong G/N$.

(b) Prove the Third isomorphism theorem as stated below.

Theorem (The Third Isomorphism Theorem). *Let G be a group, K and N normal subgroups of G with $K \subseteq N$. Then $(G/K)/(N/K) \cong G/N$.*

Proof. Let G be a group, K and N normal subgroups of G with $K \subseteq N$. Let $\phi : G/K \rightarrow G/N$ such that $\phi(gK) = gN$. First we need to make sure that ϕ is well-defined. Let $xK = yK$. In other words, $y^{-1}x \in K$. Because K is a subset of N we know that $y^{-1}x \in N$. And so, $xN = yN$. Therefore, $\phi(xK) = \phi(yK)$ and ϕ is well-defined.

Next let $xK, yK \in G/K$. We see that

$$\begin{aligned} \phi(xK)\phi(yK) &= (xN)(yN) \\ &= (xy)N \\ &= \phi((xy)K). \end{aligned}$$

Therefore, ϕ preserves structure and is a homomorphism.

Next we note that,

$$\begin{aligned} \text{Ker}(\phi) &= \{gK \in G/K : \phi(gK) = e_{G/N}\} \\ &= \{gK \in G/K : gN = N\} \\ &= \{gK \in G/K : g \in N\} \\ &= N/K. \end{aligned}$$

Finally, we will show that $\text{Im}(\phi) = G/N$ and apply The First Isomorphism Theorem to obtain $(G/K)/(N/K) \cong G/N$. Let $aN \in G/N$. The element $aK \in G/K$ is such that $\phi(aK) = aN$ and so ϕ is surjective. Because ϕ is surjective, the image of ϕ contains the entire codomain. In other words $\text{Im}(\phi) = G/N$. Applying The First Isomorphism Theorem we obtain

$$(G/K)/(N/K) = (G/K)/\text{Ker}(\phi) \cong \text{Im}(\phi) = G/N.$$

In other words, $(G/K)/(N/K) \cong G/N$.

□

EXTRA CREDIT We showed that if N is a normal subgroup of a group G , then the operation

$$(aN)(bN) = (ab)N \tag{1}$$

on G/N (the collection of left cosets of N in G) is well-defined. Is the converse true? That is, if G is a group and N is a subgroup of G so that (1) is well-defined, must N be a normal subgroup of G ? Prove your answer.

Conjecture. If G is a group and N is a subgroup of G such that the operation $(aN)(bN) = (ab)N$ is well-defined, then N

Proof. Let G be group with identity e and let N be a subgroup of G such that the operation $(aN)(bN) = (ab)N$ is well-defined. Let $n \in N$. We know that $nN = eN$ from the definition of a coset. Let $g \in G$. We know that $(eN)(gN) = (eg)N = gN$, because the operation $(aN)(bN) = (ab)N$ is well-defined. Also, because $nN = eN$ we see that

$$gN = (eN)(gN) = (nN)(gN) = (ng)N.$$

And so, $gN = (ng)N$. Multiplying the inverse of g on the left we obtain $N = (g^{-1}ng)N$. From the definition of a coset we now know that $g^{-1}ng \in N$. Finally, from this we can conclude that $g^{-1}Ng \subseteq N$, which makes N a normal subgroup of G . \square