Math 110B Homework 2

Thomas Slavonia

April 18, 2024

1.

a.

Proof. Let H and K be subgroups of G. Since $e \in H$ and $e \in K$, then $e \in H \cap K$. Take $a \in H \cap K$. Then, $a \in H$ and $a \in K$. Since H and K are subgroups we have $a^{-1} \in H$ and $a^{-1} \in K$ and thus $a^{-1} \in H \cap K$. Take $a, b \in H \cap K$. Then, $a, b \in H$ and $a, b \in K$. Note that H and K are subgroups, so $ab \in H$ and $ab \in K$, and therefore $ab \in H \cap K$. Thus, by Theorem 7.11 in the book these are the only axioms we needed to satisfy for $H \cap K$ to be a subgroup, thus $H \cap K$ is a subgroup. □

b.

Proof. Let $\{H_i\}$ be a collection of subgroups of G. Take $a \in \cap H_i$. Then, we have that $a \in H_i$ for any i. Since H_i is a subgroup we know that $a^{-1} \in H_i$ for every i and thus we can conclude that $a^{-1} \in \cap H_i$. Take $a, b \in \cap H_i$. Hence, we have that $a, b \in H_i$ for every i. Since H_i is a subgroup, we know that $ab \in H_i$ for every i and thus we can conclude that $ab \in \cap H_i$. Thus, by Theorem 7.11 in the book these are the only axioms we needed to satisfy for $\cap H_i$ to be a subgroup, thus $\cap H_i$ is a subgroup. □

2.

Proof. Let H be a subgroup of G. Note, that the normalizer of H is defined as $N(H) = \{x \in G : xHx^{-1} = H\}$. Now, take $a \in N(H)$. Therefore

$$aHa^{-1} = H$$

but, if we multiply by a^{-1} on the left and a on the right that

$$a^{-1}aHa^{-1}a = H = a^{-1}Ha$$

and thus $a^{-1} \in N(H)$. Take $a, b \in N(H)$. Then,

$$aHa^{-1} = H, \text{ and } bHb^{-1} = H.$$

Then using the proven fact (Corollary 7.6 in the book) that $(ab)^{-1} = b^{-1}a^{-1}$ we get the result

$$abH(ab)^{-1} = abHb^{-1}a^{-1} = aHa^{-1} = H.$$

Thus, $ab \in N(H)$ and by Theorem 7.11 showing that a subset is closed and under operation and inverses is necessary to prove that a subset of a group is a subgroup. Let $a \in H$. Then,

$$aHa^{-1} = aH = H$$

and so $a \in N(H)$ and therefore $H \subset N(H)$. □

3.

Proof. Let G be an abelian group of order mn where $(m,n) = 1$ with an element a of order m and an element b of order n. Look at the subgroup $\langle ab \rangle$. Then, $(ab)^k = a^k b^k$ as the group is abelian. Sicne we can choose any $k \in \mathbb{Z}$ we could choose $k = 0$, so $\exists k \in \mathbb{Z}$ such that $(ab)^k = a^k b^k = e$ and thus $a^k = b^{-k}$. Take each side to the power of n to get

$$\left(a^k\right)^n = \left(b^{-k}\right)^n$$

$$a^{kn} = b^{-kn}.$$

b is order n, so $b^{-kn} = e$ and so $a^{kn} = e$. a is of order m, and therefore $m|kn$. Since $(m,n) = 1$, then $\exists c, d \in \mathbb{Z}$ such that $mc + nd = 1$. Let $kn = mq$ for $q \in \mathbb{Z}$ as $m|kn$. Then, multiplying by k we get $mkc + knd = k$ and so $mkc + mqd = m(kc + qd) = k$. Therefore, as $(m,n) = 1$ we have that $m|k$ since $m|kn$. Thus, $a^k = e$. By our earlier equation we have

$$(a^k)^m = (b^{-k})^m$$

$$a^{km} = b^{-km}.$$

a is of order m, so $b^{-km} = e$. b is of order n, and thus $n|km$ but since $(m,n) = 1$, using the previous argument we can say that $n|k$ also. Since $(m,n) = 1$ we have previously shown in algebra that if $n|k$ and $m|k$ and n, m are coprime, then $nm|k$. Thus, $(ab)^{nm} = e$, so ab has order nm. But, the order of G is also nm and thus it must be that $G = \langle ab \rangle$. □

4.

a.

Proof. Let $f : G \to H$ be a group homomorphism and $a \in G$ has finite order k. Then,

$$f(a)^k = \underbrace{f(a) \cdot f(a) \cdots f(a)}_{k\text{-times}} \overset{(a)}{=} f(\underbrace{a \cdot a \cdots a}_{k\text{-times}}) = f(a^k) \overset{(b)}{=} f(e_G) \overset{(c)}{=} e_H$$

with steps $(a) - (c)$ justified:

(a) f is a group homomophism

(b) a has order k in G

(c) by theorem in book, identity element maps to identity element.

□

b.

Proof. We know that $f(a)^k = e_H$. Therefore, k is either the order of $f(a)$, or the order of $f(a)$ divides k, and either way we get the result that $|f(a)| \le |a|$. $\square$

5.

Proof. Let $f : G \to H$ be a group homomorphism and $K_f = \{a \in G : f(a) = e_H\}$ be the kernel of the homomorphism. For $e_G \in G$ we know that $f(e_G) = e_H$ by a theorem in the book. Take $a \in K_f$, then the same theorem also gives us that $f(a^{-1}) = f(a)^{-1}$. Hence

$$f(a^{-1}) = f(a)^{-1} = e_H^{-1} = e_H$$

which gives us that $f(a^{-1}) \in K_f$. Take $a, b \in K_f$. Then,

$$f(ab) = f(a)f(b) = e_H e_H = e_H.$$

Thus, we have that $ab \in K_f$. These properties give us that K_f is subgroup. $\square$

6.

Proof. Note that $\mathbb{Z}/n\mathbb{Z}$ is a cyclic group as $[1]$ will always be a generator as $(1,n) = 1$ always. Let $[a] \in \mathbb{Z}/n\mathbb{Z}$ be a generator for the group. Let $f \in \text{Aut } \mathbb{Z}/n\mathbb{Z}$. Then, $f([a]) = [ba]$ for $[b] \in \mathbb{Z}/n\mathbb{Z}$. If generators don't map to generators under an isomorphism, then the group structure is no longer maintained, thus $[ba]$ must be a generator of $\mathbb{Z}/n\mathbb{Z}$. So, $(ba,n) = 1$ and $(a,n) = 1$ and so

$$bac + nd = 1 \text{ and } ax + ny = 1$$

for some $c, d, x, y \in \mathbb{Z}$. Therefore,

$$(bac + nd)(ax + ny) = bacax + bacny + ndax + ndny = b(acax + acny) + n(dax + dny) = 1$$

so $(b,n) = 1$. So, $[a], [b] \in U_n$. Note that for $\mathbb{Z}/n\mathbb{Z}$ we have that 1 is always a generator, as $(1,n) = 1$ is always true. Look at the map $f : \text{Aut } \mathbb{Z}/n\mathbb{Z} \to U_n$ where for $\rho \in \text{Aut } \mathbb{Z}/n\mathbb{Z}$, $f(\rho) = [b]$ where we consider b to be the integer that 1 is shifted by. The map is well defined as if $\rho = \phi$, then $f(\rho) = [b] = f(\phi)$. Suppose $f(\rho) = f(\phi)$, then they both map to $[b]$, implying the $\rho = \phi$ as they both map $[1]$ to the same value and that will determine where all other values are mapped to since $[1]$ is a generator and thus $[b]$ will be a generator. Thus, the function is injective. Let $[b] \in U_n$. Then $[b]$ is a generator, so there exists an automorphism that maps $[1]$ by that generator as generators must map to generators in automorphisms. Thus, the function is surjective. Hence f is an isomorphism and $\text{Aut } \mathbb{Z}/n\mathbb{Z} \cong U_n$. $\square$