Problem Set 4
Abstract Algebra I

Bennett Rennier
barennier@gmail.com

January 15, 2018

Section 3.1

Ex 9 Define $\varphi : \mathbb{C}^\times \to \mathbb{R}^\times$ by $\varphi(a+bi) = a^2+b^2$. Prove that φ is a homomorphism and find the image of φ. Describe the kernel and the fibers of φ geometrically (as subsets of the plane).

Proof. We see that for all $a, b \in \mathbb{C}^\times$. Notice that $\varphi(a) = |a|^2$. Thus, $\varphi(ab) = |ab|^2 = (|a||b|)^2 = |a|^2|b|^2 = \varphi(a)\varphi(b)$. The image of φ is $\mathbb{R}_{\geq 0}$ since $a^2+b^2 \geq 0$ and for any $r \geq 0$, we see that $0+\sqrt{r}i \mapsto 0^2+\sqrt{r}^2 = r$. The fibers of φ are concentric circles around the origin of the complex plane, with the kernel being the the origin itself. □

Ex 22 a) Prove that if H and K are normal subgroups of a group G then their intersection $H \cap K$ is also a normal subgroup of G.

b) Prove that the intersection of an arbitrary nonempty collection of normal subgroups of a group is a normal subgroup (do not assume the collection is countable).

Proof. a) Use part (b) for the special case of just two normal subgroups.

b) Let H_i be a nonempty collection of normal subgroups, possibly not countable. We see that $\cap_i H_i$ is nonempty, as $1 \in H_i$ for all such i's. We also see that if $g, h \in \cap_i H_i$, then $g, h \in H_i$, which means that $gh^{-1} \in H_i$ for every such i, and thus $gh^{-1} \in \cap_i H_i$. This proves that $\cap_i H_i$ is a subgroup. Let $H = \cap_i H_i$. Let $h \in H$. This means that $h \in H_i$ for every such i. Since H_i is normal, this shows that $ghg^{-1} \in H_i$ for all $g \in G$. Since $ghg^{-1} \in H_i$ for all i's, this shows that $ghg^{-1} \in H$ for all $g \in G$. This proves that H is normal.

□

Ex 38 Let A be an abelian group and let D be the subgroup $\{(a,a) \mid a \in A\}$ of $A \times A$. Prove that D is a normal subgroup of $A \times A$ and $(A \times A)/D \simeq A$.

Proof. Let $\varphi : A \times A \to A$ where $\varphi((a,b)) = ab^{-1}$. Let $(a,b),(c,d) \in A \times A$. We see that $\varphi((a,b))\varphi((c,d)) = ab^{-1}cd^{-1} = acb^{-1}d^{-1} = ac(bd)^{-1} = \varphi((ac,bd)) = \varphi((a,b)(c,d))$, since A is abelian. Thus φ is a homomorphism. We see that $\ker\varphi$ is all $(a,b) \in A \times A$ such that $\varphi((a,b)) = ab^{-1} = 1$. This means that $a = b$. This is exactly D. Thus, $\ker\varphi = D$. This proves that D is a normal subgroup of $A \times A$. Let $a \in A$. we see that since $1 \in A$, that $\varphi((a,1)) = a1^{-1} = a$. This proves that φ is surjective. By the first isomorphism theorem, this means that $(A \times A)/D \simeq A$. □

Ex 42 Assume both H and K are normal subgroups of G with $H \cap K = 1$. Prove that $xy = yx$ for all $x \in H$ and $y \in K$. [Show $x^{-1}y^{-1}xy \in H \cap K$.]

Proof. Let $x \in H$ and $y \in K$. Since $x \in H$ and $y \in K \subseteq G$ and H is normal, we see that $y^{-1}xy \in H$. Since $x \in H$, multiplying on the left by $x^{-1} \in H$ still leaves us in H. Thus, $x^{-1}y^{-1}xy \in H$. We see that since $y \in K$ then $y^{-1}K$. Since $y^{-1} \in K$ and $x \in H \subseteq G$, then $x^{-1}y^{-1}x \in K$. Since $y \in K$, we can multiply by y on the right and still be in K. Thus, $x^{-1}y^{-1}xy \in K$. Thus, $x^{-1}y^{-1}xy \in H \cap K$. But $H \cap K = 1$, which means that $x^{-1}y^{-1}xy = 1$. Multiplying on the left by yx, we see that $xy = yx$. □

Section 3.2

Ex 4 Show that if $|G| = pq$ for some primes p and q, then either G is abelian or $Z(G) = 1$.

Proof. Recall that $Z(G) \leq G$. This means that $|Z(G)| \mid |G|$. Since $|G| = pq$, this means that $|Z(G)| = 1, p, q$ or pq. If $|Z(G)| = 1$, then $Z(G) = 1$, which is one of the results. If $|Z(G)| = pq$, then $Z(G) = G$, which means that G is a abelian. Now the only cases left are $|Z(G)| = p$ or q.

Suppose $|Z(G)| = p$. Since p is prime, this means that $Z(G)$ is cyclic and abelian, and thus normal. Consider $G/Z(G)$. Since $|Z(G)| = p$, this means that $|G/G(Z)| = q$, which is also prime. Thus, $G/G(Z)$ is cyclic and abelian as well. Let $gZ(G)$ be the generator of $G/G(Z)$. Let $x, y \in G$. Then $xZ(G), yZ(G) \in G/Z(G)$. This means that $xZ(G) = (gZ(G))^i$ and $yZ(G) = (gZ(G))^j$ for some integers i, j. This means that $x \in xZ(G) = g^iZ(G)$. Thus, $x = g^iz_1$ for some $z_iZ(G)$. Similarly, $y = g^jz_2$ for some $z_2 \in Z(G)$. This means that $xy = g^iz_1g^jz_2 = g^ig^jz_1z_2 = g^jg^iz_2z_1 = g^jz_2g^iz_1 = yx$, since $z_1, z_2 \in Z(G)$. This proves that G is abelian. A similar argument follows for when $|Z(G)| = q$. Thus, G is abelian if $|Z(G)| = p$ or q. This proves the statement. □

Ex 6 Let $H \leq G$ and let $g \in G$. Prove that if the right coset Hg equals some left coset of H in G, then it equals the left coset gH and g must be in $N_G(H)$.

Proof. Suppose that $Hg = g'H$. Since $1 \in H$, this means that for some $h \in H$, $1g = g'h$. Thus, $g'^{-1}g = h$ for some $h \in H$. This means that $g'^{-1}g \in H$. This proves that $g'H = gH$. Thus, $Hg = g'H = gH$. Multiplying by g^{-1} on the right, we get that $Hgg^{-1} = gHg^{-1}$. This means that $gHg^{-1} = H$. This proves that $g \in N_G(H)$. □

Ex 8 Prove that if H and K are finite subgroups of G whose orders are relatively prime then $H \cap K = 1$.

Proof. Since H and K are subgroups of G, then $H \cap K$ is a subgroup of G. Also, since $H \cap K \subseteq H$ then $H \cap K \leq H$. Similarly, $H \cap K \leq K$. This means that $|H \cap K|$ divides both $|H|$ and $|K|$. Since these numbers are relatievly prime, this means that $|H \cap K| = 1$. This proves that $H \cap K = 1$. □

Ex 10 Suppose H and K are subgroups of finite index in the group G with $|G : H| = m$ and $|G : K| = n$. Prove that $\text{lcm}\,(m, n) \leq |G : H \cap K| \leq mn$. Deduce that if m and n are relatively prime then $|G : H \cap K| = |G : H| \cdot |G : K|$.

Proof. Recall that the number of cosets of $H \cap K$ is equal to $|G : H \cap K|$. We see that the cosets are of the form $x\,(H \cap K)$. We see that since $x\,(H \cap K) \subseteq xH$, as $H \cap K \subseteq H$, and similarly, $x\,(H \cap K) \subseteq xK$. This means that $x\,(H \cap K) \subseteq xH \cap xK$. We see that the number of cosets of H is equal to $|G : H| = m$ and also that the number of cosets of K is equal to $|G : K| = n$. Thus, there are mn possible combinations of the two cosets. Since the the number of cosets of $H \cap K$ is a subset of $aH \cap bK$ and there are mn possibilities of aH and bK, this proves that the number of cosets of $H \cap K$ is less than or equal to mn.

We see that $H \cap K \leq H$ and that $H \cap K \leq K$. This means that $|H \cap K|$ divides both $|K|$ and $|H|$. We see that $|H \cap K||G : H \cap K| = |G| = |H||G : H|$. Cross multiplying, we get that $\frac{|G:H\cap K|}{|G:H|} = \frac{|H|}{|H\cap K|}$. Since $|H \cap K|$ divides $|H|$, this means that the right hand side is an integer. This means that $\frac{|G:H\cap K|}{|G:H|}$ is an integer, and thus that $|G : H| = m$ divides $|G : H \cap K|$. By a similar argument, $|G : K| = n$ divides $|G : H \cap K|$. Since both m and n divide $|G : H \cap K|$ this means that $|G : H \cap K|$ is at least as big as $\text{lcm}\,(m, n)$. Thus, $\text{lcm}\,(m, n) \leq |G : H \cap K| \leq mn$. □

Ex 16 Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ to prove Fermat's Little Theorem: if p is prime then $a^p = a \pmod p$ for all $a \in \mathbb{Z}$.

Proof. Look at the subgroup $\langle a \rangle \leq (\mathbb{Z}/p\mathbb{Z})^\times$. Since $|\,(\mathbb{Z}/p\mathbb{Z})^\times\,| = p - 1$, then this means that $|\langle a \rangle|$ divides $p - 1$. Since $|\langle a \rangle| = |a|$, this means that the order of a divides $p - 1$. Thus, $a^{p-1} = 1$. Multiplying by a, we get that $a^p = a$ for all $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. This means that $a^p = a \pmod p$ for all $a \in \mathbb{Z}$. □

Ex 18 Let G be a finite group, let H be a subgroup of G and let $N \trianglelefteq G$. Prove that if $|H|$ and $|G : N|$ are relatively prime then $H \leq N$.

Proof. Let $x \in K$, where $|x| = n$. We see that $n \mid |K|$. Look at xN. We see that $(xN)^n = x^nN = 1N = N$. Thus, $|xN| \mid n$. Since $n \mid |K|$, this means that $|xN| \mid |K|$. Since $xN \in G/N$, then $|xN| \mid |G/N| = |G : N|$. Since $|G : N|$ and $|K|$ are relatively prime, this means that $|xN| = 1$. Thus, $xN = N$. This proves that $x \in N$. Thus, $K \subseteq N$. □

Ex 19 Prove that if N is a normal subgroup of the finite group G and $(|N|, |G : N|) = 1$ then N is the unique subgroup of G of order $|N|$.

Proof. Let $H \leq G$ be a subgroup of order $|N|$. By the previous exercise, we see that $H \leq N$. Since $|H| = |N|$. This means that $H = N$. □

Ex 21 Prove that $\mathbb{Q}$ has no proper subgroups of finite index. Deduce that $\mathbb{Q}/\mathbb{Z}$ has no proper subgroups of finite index.

Proof. Let H be a proper subgroup of finite index of $\mathbb{Q}$. Let n be the finite index. Since $\mathbb{Q}$ is abelian, then H is normal, and thus $\mathbb{Q}/H$ exists. Since $|\mathbb{Q} : H| = n$, this means that $|\mathbb{Q}/H| = n$. Thus, if $gH \in \mathbb{Q}/H$, then $|gH| \mid |\mathbb{Q}/H| = n$. Thus, $n(gH) = H$. This means that $(ng)H = H$, which means that $ng \in H$ for all $g \in \mathbb{Q}$. However, $\frac{g}{n} \in \mathbb{Q}$ since $g \in \mathbb{Q}$ and $n \in \mathbb{N}$. This means that $n\frac{g}{n} \in H$. However, this just means that $g \in H$ for all $g \in \mathbb{Q}$. Thus, $H = \mathbb{Q}$. This is a contradiction, as H was assumed to be a proper subgroup.

Consider the canonical homomorphism $\varphi : \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$, where $\varphi(q) = q\mathbb{Z}$. Suppose H were a subgroup of $\mathbb{Q}/\mathbb{Z}$ of finite index. Then, $\varphi^{-1}(H)$ would be a subgroup of $\mathbb{Q}$ of finite index since $|\mathbb{Q} : \varphi^{-1}(H)| = |\mathbb{Q}/\mathbb{Z} : H|$. Thus, there is no proper subgroup of finite index of $\mathbb{Q}/\mathbb{Z}$. □

Section 3.3

Ex 4 Let C be a normal subgroup of the group A and let D be a normal subgroup of the group B. Prove that $(C \times D) \trianglelefteq (A \times B)$ and $(A \times B)/(C \times D) \simeq (A/C) \times (B/D)$.

Proof. Let $(c, d) \in C \times D$ and $(a, b) \in A \times B$. We then see that $(a, b)(c, d)(a, b)^{-1} = (ac, bd)(a^{-1}, b^{-1}) = (aca^{-1}, bdb^{-1})$. Since C and D are normal, we see that $aca^{-1} \in C$ and $bdb^{-1} \in D$. Thus, $(a, b)(c, d)(a, b)^{-1} \in C \times D$ for all $(a, b) \in A \times B$. This proves that $C \times D \trianglelefteq A \times B$.

Let $\varphi : A \times B \to (A/C) \times (B/D)$, where $\varphi((a, b)) = (aC, bD)$. We see that $\varphi((a_1, b_1)(a_2, b_2)) = \varphi((a_1a_2, b_1b_2)) = (a_1a_2C, b_1b_2D) = (a_1Ca_2C, b_1Db_2D) = (a_1C, b_1D)(a_2C, b_2D) = \varphi((a_1, b_1))\varphi((a_2, b_2))$. Thus φ is a homomorphism. For any $(aC, bD) \in C \times D$, we see that $\varphi((a, b)) = (aC, bD)$. Thus, φ is a surjection. The $\ker\varphi$ are the elements where $\varphi((a, b)) = (aC, bD) = (C, D)$. Thus, $a \in C$ and $b \in D$. This is exactly the group $C \times D$. Thus, by the first isomorphism theorem, $(A \times B)/(C \times D) \simeq (A/C) \times (B/D)$. □

Ex 8 Let p be a prime and let G be the group of p-power roots of 1 in $\mathbb{C}$. Prove that the map $z \mapsto z^p$ is a surjective homomorphism. Deduce that G is isomorphic to a proper quotient of itself.

Proof. Let φ be the described function. We see that $\varphi(zw) = (zw)^p = z^pw^p = \varphi(z)\varphi(w)$, since $\mathbb{C}$ is abelian and so G is abelian. Let $z \in G$. This means that $z^{p^n} = 1$ for some $n \in \mathbb{N}$. By the fundamental theorem of algebra, the polynomial $x^p - z$ has a root. Call this root w. We see that $(w^p)^{p^n} = w^{p^{n+1}} = 1$. Thus, $w \in G$. We see that $\varphi(w) = z$. This proves that φ is surjective.

We see that $\ker\varphi = \{z \in \mathbb{C} \mid z^p = 1\}$. By the fundamental theorem of algebra again, this is kernel nontrivial. By the first isomorphism theorem, $G/\ker\varphi \simeq G$. This proves the statement. □

Ex 9 Let p be a prime and let G be a group of order $p^a m$, where p does not divide m. Assume P is a subgroup of G of order p^a and N is a normal subgroup of G of order $p^b n$, where p does not divide n. Prove that $|P \cap N| = p^b$ and $|PN/N| = p^{a-b}$. (The subgroup P of G is called a Sylow p-subgroup of G. This exercise shows that the intersection of any Sylow p-subgroup of G with a normal subgroup N is a Sylow p-subgroup of N.)

Proof. By the second isomorphism theorem, we see that $PN \leq G$, $N \trianglelefteq PN$, $P \cap N \trianglelefteq P$, and $P/(P \cap N) \simeq PN/N$. We see that $|PN|$ divides $|G|$. Thus, $|PN| = p^k j$ for some k where p does not divide j and $j \mid m$. Because $P \leq PN$, we see that $k = a$ and because $N \leq PN$, then $n \mid j$. Thus $|PN/N| = p^{a-b}q$ where p does not divide q. Since $P \cap N \leq P$, we see that $|P/(P \cap N)| = |P : P \cap N|$ divides P, and thus $|P/(P \cap N)| = p^k$ for some k, and thus $p^k = p^{a-b}q$. This means that $q = 1$ and thus $|PN/N| = p^{a-b}$. At last, we see that $|P|/|P \cap N| = |\frac{P}{P \cap N}| = \frac{p^a}{p^b}$, which means that $|P \cap N| = p^b$. □

Additional Exercises

Ex A Let A be a group with $|A| = p^a m$ with $a > 0$ and m relatively prime to p. Let B be a group such that $|B| = p^b n$ with $a > b$ and n relatively prime to p. Prove that every group homomorphism $\varphi : A \to B$ has a nontrivial kernel.

Proof. We see that if $|B| < |A|$, then there is no injective function from $A \to B$, much less an injective homomorphism. We also see that $|B| \neq |A|$, because this would mean that $p^b n = p^a m$, which means that n would have a factor of p^{a-b}, which is a contradiction, as p and n are relatively prime. Thus $|A| < |B|$, which means that $p^a m < p^b n$.

Let φ be an homomorphism from A to B with a trivial kernel. This means that φ is injective. Then by the first isomorphism theorem $A/\ker\varphi = A/\{e\} \simeq A \simeq \operatorname{Im}\varphi$. Thus, $A \simeq \operatorname{Im}\varphi \leq B$. Since $|A| = p^a m$ and $|B| = p^b n$, this means that $p^a m \mid p^b n$. Since $p^a m < p^b n$, this means that either $p^a m \mid p^b$ or $p^a m \mid n$. However, since $p^a > p^b$, the first case is not possible. Thus, $p^a m \mid n$. This means that $n = p^a m k$ for some k. This means that $p \mid n$. This is a contradiction, as p and n are relatively prime. Thus, there is no such φ. □

Ex B Let G be an arbitrary group and, as usual, let's write $e \in G$ for the identity element. Please determine the quotient groups G/G and $G/\{e\}$.

Proof. We see that the elements of G/G are of the form gG for $g \in G$. However, $gG = G$ for all $g \in G$. This means that G is the only element, and thus G/G is the trivial group.

Let $\varphi : G \to G$ be the identity function, which is a bijection. We see that $\varphi(gh) = gh = \varphi(g)\varphi(h)$. Thus, φ is a isomorphism. Since φ is a isomorphism, $\ker\varphi = \{e\}$. Thus, by the first isomorphism theorem, $G/\{e\} \simeq G$. □