Math 561 H **Fall 2011**
Homework 3 Solutions **Drew Armstrong**

Group Problems.

1. Let G be a group. Given $a \in G$ define the centralizer $Z(a) := \{b \in G : ab = ba\}$. Prove that $Z(a) \leq G$. For which $a \in G$ is $Z(a) = G$?

Proof. To show closure, let $b, c \in Z(a)$. That is, suppose that $ba = ab$ and $ca = ac$. Then we have $(bc)a = bca = bac = abc = a(bc)$, hence $bc \in Z(a)$. Next, note that $1 \in Z(a)$ since $1a = a1 = a$. Finally, suppose $b \in Z(a)$, i.e. $ab = ba$. Multiplying by b^{-1} on both the left and the right gives $b^{-1}abb^{-1} = b^{-1}bab^{-1}$, or $b^{-1}a = ab^{-1}$. We conclude that $b^{-1} \in Z(a)$. □

2. We say $a, b \in G$ are conjugate if there exists $g \in G$ such that $a = gbg^{-1}$. Recall (HW2.8) that this is an equivalence relation. Let $C(a) := \{b \in G : \exists\, g \in G, a = gbg^{-1}\}$ denote the conjugacy class of $a \in G$. **Prove** that $|C(a)| = [G : Z(a)]$.

Proof. First note that every element of $C(a)$ looks like gag^{-1} for some $g \in G$. We claim that the map $gag^{-1} \mapsto gZ(a)$ is a **bijection** from $C(a)$ to the cosets of $Z(a)$. The map is clearly **surjective**. Then to see that the map is **well-defined** and **injective**, note that

$$\begin{aligned} gag^{-1} = hah^{-1} &\Leftrightarrow a(g^{-1}h) = (g^{-1}h)a \\ &\Leftrightarrow g^{-1}h \in Z(a) \\ &\Leftrightarrow gZ(a) = hZ(a). \end{aligned}$$

The direction $\Rightarrow$ shows well-definedness and the direction $\Leftarrow$ shows injectivity. □

3. On HW2 you proved that $\mathrm{Aut}(\mathbb{Z})$ is the group with two elements. Now **prove** that $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$. (Hint: An automorphism $\varphi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is determined by $\varphi(1)$. What are the possibilities?) Taking $n = 0$, we recover the fact that $\mathrm{Aut}(\mathbb{Z}) \approx \mathbb{Z}^\times = \{\pm 1\}$.

To save space we will just write a for the element $a + n\mathbb{Z}$ of $\mathbb{Z}/n\mathbb{Z}$. First we will prove a useful **Lemma:** The order of $a \in \mathbb{Z}/n\mathbb{Z}$ is $n/\gcd(a, n)$.

Proof. First note that $a(n/\gcd(a, n)) = n(a/\gcd(a, n)) = 0 \in \mathbb{Z}/n\mathbb{Z}$. Next suppose that $ak = 0 \in \mathbb{Z}/n\mathbb{Z}$ for some $k \geq 1$. We wish to show that $n/\gcd(a, n) \leq k$. Indeed since $ak = 0 \in \mathbb{Z}/n\mathbb{Z}$ we have $n|ak$, which implies that $(n/\gcd(a, n))|(a/\gcd(a, n))k$, and since $n/\gcd(a, n)$ and $a/\gcd(a, n)$ are **coprime**, this implies that $n/\gcd(a, n)|k$, hence $n/\gcd(a, n) \leq k$. □

Proof. Suppose that $\varphi; \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is an **automorphism** with $\varphi(1) = a$. By the **homomorphism** property we have $\varphi(x) = \varphi(1 + \cdots + 1) = \varphi(1) + \cdots + \varphi(1) = a + \cdots + a = ax$. Thus the **image** of φ is the (additive) cyclic subgroup $\langle a \rangle \leq \mathbb{Z}/n\mathbb{Z}$. Then since φ is **surjective** we must have $\langle a \rangle = \mathbb{Z}/n\mathbb{Z}$. By the Lemma, this happens if and only if a and n are coprime, i.e. $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, in which case the map $\varphi(x) = ax$ is also invertible with inverse $\varphi^{-1}(x) = a^{-1}x$.

In summary, there is a **bijection** between $(\mathbb{Z}/n\mathbb{Z})^\times$ and $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ given by sending $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ to the automorphism $\varphi_a(x) = ax$. Moreover, this bijection is a **group isomorphism** since for all $a, b \in (\mathbb{Z}/n\mathbb{Z})^\times$ and $x \in \mathbb{Z}/n\mathbb{Z}$ we have

$$\varphi_a \circ \varphi_b(x) = \varphi_a(\varphi_b(x)) = \varphi_a(bx) = a(bx) = (ab)x = \varphi_{ab}(x).$$

□

4. Let H, K be subgroups of G. **Prove that:**

(a) If $H \trianglelefteq G$ then $HK := \{hk \in G : h \in H, k \in K\}$ is a subgroup of G.

(b) Moreover, if $H \cap K = \{1\}$ and if $hk = kh$ for all $h \in H$, $k \in K$ then HK is isomorphic to the direct product group $H \times K := \{(h, k) : h \in H, k \in K\}$ with the componentwise product. (Hint: What could the isomorphism possibly be? Really?)

Proof. First we show (a). Given $H, K \leq G$ with $H \trianglelefteq G$, we will show that $HK \leq G$. To see that HK is closed, consider h_1k_1 and h_2k_2 in HK. Is $h_1k_1h_2k_2 \in HK$? Yes. Since $k_1h_2 \in k_1H = Hk_1$ there exists $h_3 \in H$ such that $k_1h_2 = h_3k_1$. Then $h_1h_2k_1k_2 = (h_1h_3)(k_1k_2) \in HK$. Next, observe that $1 \in H \cap K$ hence $1 = 1 \cdot 1 \in HK$. Finally, let $a = hk \in HK$ with $h \in H$ and $k \in K$. To see that $a^{-1} = k^{-1}h^{-1} \in HK$ note that $k^{-1}h^{-1} \in k^{-1}H = Hk^{-1}$, hence there exists $h' \in H$ such that $k^{-1}h^{-1} = h'k^{-1}$. That is, $a^{-1} = k^{-1}h^{-1} = h'k^{-1} \in HK$.

Next we show (b). Suppose that $H, K \leq G$ with $H \trianglelefteq G$, $H \cap K = \{1\}$ and with $hk = kh$ for all $h \in H, k \in K$. In this case we claim that the "multiplication" map $\mu((h, k)) := hk$ is a **group isomorphism** $\mu : H \times K \to HK$. First note that it is a **homomorphism** because

$$\mu((h_1, k_1)(h_2, k_2)) = \mu((h_1h_2, k_1k_2)) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \mu((h_1, k_1))\mu((h_2, k_2)).$$

Next, to show that μ is **injective**, suppose that $\mu((h_1, k_1) = h_1k_1 = h_2k_2 = \mu((h_2, k_2))$. Then $h_1k_1 = h_2k_2$ implies that $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K$. Since $H \cap K = \{1\}$, we get $h_2^{-1}h_1 = 1$ (or $h_1 = h_2$) and $k_2k_1^{-1} = 1$ (or $k_1 = k_2$), hence $(h_1, k_1) = (h_2, k_2)$. Finally, note that μ is **surjective** by definition. □

5. Let G be a cyclic group of order n. **Prove** that every subgroup of G is cyclic and has order d for some $d|n$. Conversely, **prove** that for every $d|n$ there exists a subgroup of order d. Bonus: Prove that there is **exactly one** subgroup of order $d|n$.

Proof. First we show that every subgroup of G is cyclic. To see this suppose $G = \langle g \rangle$ and consider the **surjecitve homomorphism** $\varphi : \mathbb{Z} \to G$ given by $\varphi(n) := g^n$. If $H \leq G$ is any subgroup, then $H' := \varphi^{-1}(H)$ is a subgroup of $\mathbb{Z}$. We know (Theorem 2.3.3) that any subgroup of $\mathbb{Z}$ is **cyclic**, hence $H' = a\mathbb{Z}$ for some $a \in \mathbb{Z}$. Then the **restricted homomorphism** $\varphi : H' \to H$ (which is **surjective** by definition) sends $ak \in a\mathbb{Z}$ to $g^{ak} = (g^a)^k$. Hence H **is equal to the image** $\langle g^a \rangle$, which is cyclic. Finally, by Lagrange's Theorem 2.8.9 we know that the size of H divides the size of G.

Conversely, suppose that $G = \langle g \rangle$ has size n and consider a divisor $d|n$. We claim that there exists a subgroup $H \leq G$ of size d. To see this consider the **surjective homomorphism** $\varphi : \mathbb{Z} \to G$ defined by $\varphi(a) := g^a$. The **kernel** is $n\mathbb{Z}$. Thus the Correspondence Theorem 2.10.5 says that the map $H \mapsto \varphi(H)$ is a bijection from subgroups $n\mathbb{Z} \leq H \leq \mathbb{Z}$ to subgroups $\varphi(H) \leq G$. In particular, let $dk = n$ and consider the subgroup $n\mathbb{Z} \leq k\mathbb{Z} \leq \mathbb{Z}$. Then $\varphi(k\mathbb{Z})$ is a subgroup of G (and is cyclic by part (a)). What is its order? Part of the Correspondence Theorem says that $k = [\mathbb{Z} : k\mathbb{Z}] = [G : \varphi(k\mathbb{Z})]$. Finally, Lagrange's Theorem 2.8.9 tells us that $|\varphi(k\mathbb{Z})| = |G|/k = n/k = dk/k = d$.

Bonus: Suppose we had two subgroups $H, K \leq G$ with $|H| = |K| = d$, where $dk = n$. Then the preimages $\varphi^{-1}(H)$ and $\varphi^{-1}(K)$ are both sugroups of index k in $\mathbb{Z}$. By Theorem 2.3.3 there is a **unique** such subgroup; namely $k\mathbb{Z}$. Hence $\varphi^{-1}(H) = k\mathbb{Z} = \varphi^{-1}(K)$. Applying φ then gives $H = \varphi(k\mathbb{Z}) = K$. □

Ring Problems.

A ring is a tuple $(R, +, \times, 0, 1)$ such that $(R, +, 0)$ is an abelian group, $(R, \times, 1)$ is a semigroup (associative with identity 1, maybe no inverses, maybe not abelian) and for all $a, b, c \in R$ we have $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

6. Let R and S be rings. What is the correct definition of a ring homomorphism $\varphi : R \to S$? Hint: You will need $\varphi(1_R) = 1_S$. Suppose that R and S are isomorphic *as rings*. **Prove** that the corresponding groups of units $R^\times$ and $S^\times$ are isomorphic *as groups*.

Proof. A ring homomorphism should preserve the operations $+, \times$. That is, we need $\varphi(a + b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$. We also want $\varphi(0_R) = 0_S$ and $\varphi(1_R) = 1_S$. The first of these follows from $\varphi(a + b) = \varphi(a) + \varphi(b)$ since a homomorphism of additive groups automatically preserves zero. However, $\varphi(1_R) = 1_S$ does **not** automatically follow from $\varphi(ab) = \varphi(a)\varphi(b)$ since the usual proof requires invertibility, which we don't have. Hence we define a **ring homomorphism** to satisfy:

- $\varphi(a + b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$,
- $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$,
- $\varphi(1_R) = 1_S$.

We say $R \approx S$ **as rings** if there exists a bijective ring homomorphism (i.e. a **ring isomorphism**) $\varphi : R \to S$. In this case we claim that $R^\times \approx S^\times$ **as groups**. To see this, restrict the map φ to $R^\times$ and note that for all $r \in R^\times$ we have $\varphi(r^{-1}) = \varphi(r)^{-1}$ by the usual proof. Hence $\varphi(r) \in S^\times$ and by the same logic we have $\varphi^{-1}(r) \in R^\times$ for all $S^\times$. Thus we have a **surjective homomorphism of multiplicative groups** $\varphi : R^\times \to S^\times$. Injectivity is inherited from $\varphi : R \to S$. $\square$

7. Let R be a (possibly non-commutative) ring. Prove that:

(a) For all $a \in R$ we have $0a = a0 = 0$.

(b) For all $a, b \in R$ we have $(-a)(-b) = ab$. (Hint: Think about $ab + a(-b)$. Think about $(-a)(-b) + a(-b)$. Now if a child asks you why negative $\times$ negative = positive, you will have an answer.)

Proof. First we show (a). Note that for all $a \in R$ we have $0 + 0a = 0a = (0 + 0)a = 0a + 0a$. Then we cancel $0a$ from both sides (which we can since $(R, +, 0)$ is a group) to get $0 = 0a$. The proof of $0 = a0$ is similar. Next we show (b). Note that $ab + a(-b) = a(b + (-b)) = a0 = 0$ and also that $(-a)(-b) + a(-b) = ((-a) + a)(-b) = 0(-b) = 0$. By transitivity we have $ab + a(-b) = (-a)(-b) + a(-b)$. Cancel $a(-b)$ from both sides to get $ab = (-a)(-b)$. $\square$

8. (Chinese Remainder Theorem) For all $a, b \in \mathbb{Z}$ define the notation $[a]_b = a + b\mathbb{Z}$. Now let $m, n \in \mathbb{Z}$ be coprime. Prove that the map $\varphi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ defined by $\varphi([a]_{mn}) := ([a]_m, [a]_n)$ is a **ring isomorphism**. (Hint: The hard part is to show surjectivity. Since m, n are coprime we can write $1 = xm + yn$. What does φ do to $bxm + ayn$?)

Proof. First we show that φ is **well-defined**. Indeed, if $[a]_{mn} = [b]_{mn}$ then $[a]_m = [b]_m$ and $[a]_n = [b]_n$, hence $([a]_m, [a]_n) = ([b]_m, [b]_n)$. The fact that φ is a **ring homomorphism** is straightforward. Finally, let us show that φ is a **bijection**. To see that it is an **injection**, suppose that $([a]_m, [a]_n) = ([b]_m, [b]_n)$, i.e $[a]_m = [b]_m$ and $[a]_n = [b]_n$. This means that $m|a - b$ and $n|a - b$. Since m, n are coprime this implies $mn|a - b$, hence $[a]_{mn} = [b]_{mn}$ as desired. To show **surjectivity**, consider an arbitrary element $([a]_m, [b]_n)$. Does it get hit by φ? Well, since m, n are coprime we can write $xm + yn = 1$. Then we claim that $\varphi([bxm + ayn]_{mn}) = ([a]_m, [b]_n)$. Indeed, we have $[bxm + ayn]_m = [ayn]_m$. Then note that $[yn]_m = [1]_m$, hence $[ayn]_m = [a]_m[1]_m = [a]_m$. The proof that $[bxm + ayn]_n = [b]_n$ is similar. $\square$

Let R be a ring. We say that R is an integral domain if it is commutative and if for all $a, b \in R$ we have $ab = 0$ implies $a = 0$ or $b = 0$ (i.e. R has no "zero divisors"). We say that R is a field if it is commutative and if every nonzero $a \in R$ has a multiplicative inverse.

9. Prove that a **finite** integral domain is a field. Give an example to show that an infinite integral domain need not be a field. (Hint: Given $a \in R$ consider the map $R \to R$ defined by $x \mapsto ax$. Is it injective? Surjective?)

Proof. Let R be a **finite integral domain** and fix $a \in R$ with $a \neq 0$. Then the map $x \mapsto ax$ is **injective** because $ax = ay \Rightarrow a(x - y) = 0 \Rightarrow x - y = 0 \Rightarrow x = y$. Since R is **finite**, the map is **also surjective**. It follows that there exists some $b \in R$ such that $1 = ab$. Hence a is invertible. Since the choice of $a \neq 0$ was arbitrary we conclude that R is a field.

The integers $\mathbb{Z}$ are an example of an (infinite) integral domain that is **not** a field. $\square$