Solutions to Some Review Problems for Exam 3

Recall that $\mathbb{R}^*$, the set of nonzero real numbers, is a group under multiplication, as is the set $\mathbb{R}^+$ of all positive real numbers.

1. Prove that the set $N$ of matrices $A \in \text{Gl}_n(\mathbb{R})$ with $\det(A)$ equal to 1 or $-1$ is a normal subgroup of $\text{Gl}_n(\mathbb{R})$. Show that the function $\varphi : \text{Gl}_n(\mathbb{R}) \to \mathbb{R}^+$ defined by $\varphi(A) = \deg(A)^2$ is a group homomorphism. Use the fundamental homomorphism theorem to show that $\text{Gl}_n(\mathbb{R})/N$ is isomorphic to $\mathbb{R}^+$.

**Solution.** Let $A, B \in \text{Gl}_n(\mathbb{R})$. Then

$$\varphi(AB) = \det(AB)^2 = (\det(A)\det(B))^2 = \det(A)^2\det(B)^2 = \varphi(A)\varphi(B)$$

by properties of determinants and exponents. Therefore, $\varphi$ is a group homomorphism. Its kernel is

$$\ker(\varphi) = \{A \in \text{Gl}_n(\mathbb{R}) : \varphi(A) = 1\} = \{A \in \text{Gl}_n(\mathbb{R}) : \det(A)^2 = 1\}$$

$$= \{A \in \text{Gl}_n(\mathbb{R}) : \det(A) = \pm 1\} = N.$$

This shows that $N$ is a normal subgroup of $\text{Gl}_n(\mathbb{R})$. Finally, we note that the image of $\varphi$ is all of $\mathbb{R}^+$ since if $a$ is a positive real, then the diagonal matrix

$$A = \begin{pmatrix} \sqrt{a} & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & & \ddots & \cdots \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

in $\text{Gl}_n(\mathbb{R})$ has determinant $\sqrt{a}$, and so $\varphi(A) = a$. Consequently, by the fundamental homomorphism theorem, $\text{Gl}_n(\mathbb{R})/N$ is isomorphic to $\mathbb{R}^+$.

2. Let $\varphi : G \to H$ be a group isomorphism. If $g \in G$ has finite order $n$, show that $\varphi(g) \in H$ also has order $n$.

**Solution.** Recall that the order of an element $a$, when finite, is the smallest positive integer $n$ satisfying $a^n = e$. First suppose that $n$ is the order of $g \in G$. Then $g^n = e$. Therefore, as $\varphi$ preserves the operation, $e = \varphi(g^n) = \varphi(g)^n$. Therefore, the order of $\varphi(g)$ divides $n$. Suppose that $m$ is the order of $\varphi(g)$. We’ve argued that $m$ divides $n$. Now, as $\varphi(g)^m = e$, we have $\varphi(g^m) = e$. Since $\varphi$ is an isomorphism, it is 1-1, and so $g^m = e$. This means $n$ divides $m$. Thus, $m = n$ as $m$ divides $n$ and vice-versa.

3. Let $G$ be a group and let $N$ be a normal subgroup of $G$. If $G$ is Abelian, prove that $G/N$ is Abelian.

**Solution.** Let $x, y \in G/N$. Then there are $a, b \in G$ with $x = Na$ and $y = Nb$. Then

$$xy = Nab = Nab = Nba = NbNa = yx$$
since $G$ is Abelian. Thus, $G/N$ is Abelian.
4. Let $G$ and $H$ be groups. Define $\pi : G \times H \to G$ by $\pi(g, h) = g$. Show that $\pi$ is a group homomorphism, that $\pi$ is onto, and that $\ker(\varphi) = \{(e, h) : h \in H\}$. Conclude that $(G \times H)/\ker(\varphi)$ is isomorphic to $G$.

**Solution.** Let $(g, h), (g', h') \in G \times H$. Then

$$\pi((g, h)(g', h')) = \pi((gg', hh')) = gg' = \pi(g, h)\pi(g', h'),$$

so $\pi$ is a group homomorphism. It is onto because if $g \in G$, then $(g, e) \in G \times H$ and $\pi(g, e) = g$. Finally, $\ker(\pi) = \{(g, h) : \pi(g, h) = e\} = \{(g, h) : g = e\}$.

5. Keep the notation of the previous problem. Show that the map $\varphi : H \to G \times H$ given by $\varphi(h) = (e, h)$ is a group homomorphism, and that $H$ and $\ker(\pi)$ are isomorphic.

**Solution.** Let $h, h' \in H$. Then $\varphi(hh') = (e, hh') = (e, h)(e, h') = \varphi(h)\varphi(h')$, so $\varphi$ is a group homomorphism. It is 1-1 since $\ker(\varphi) = \{h : \varphi(h) = (e, e)\} = \{h : (e, h) = (e, e)\} = \{e\}$. Finally, its image is exactly $\ker(\pi)$ from the previous problem. Therefore, $\varphi$ is a 1-1, onto group homomorphism from $H$ to $\ker(\pi)$, and so these two groups are isomorphic.

6. Define $\varphi : \mathbb{R}^* \to \mathbb{R}^+$ by $\varphi(a) = |a|$. Show that $\varphi$ is a group homomorphism. Determine the kernel $N$ of $\varphi$ and show that $\mathbb{R}^*/N \cong \mathbb{R}^+$.

**Solution.** Let $a, b \in \mathbb{R}^*$. Then $\varphi(ab) = |ab| = |a||b| = \varphi(a)\varphi(b)$ by properties of the absolute value function. Therefore, $\varphi$ is a group homomorphism. Its kernel is $N = \{a \in \mathbb{R}^* : |a| = 1\} = \{1, -1\}$. Moreover, as $|a| = a$ for each positive real, $\varphi$ is onto. Thus, by the fundamental homomorphism theorem, $\mathbb{R}^*/N \cong \mathbb{R}^+$.

7. Let $G$ be a group and $N$ a normal subgroup of $G$. Suppose that for each $a, b \in G$ we have $aba^{-1}b^{-1} \in N$. Prove that $G/N$ is Abelian.

**Solution.** Let $x, y \in G/N$. Then there are $a, b \in G$ with $x = Na$ and $y = Nb$. Consequently, $xy = NaNb = Nab$ and $yx = NbNa = Nba$. Now, $Nab = Nba$ if and only if $(ab)(ba)^{-1} \in N$. However, $(ab)(ba)^{-1} = aba^{-1}b^{-1}$. Since this is in $N$ by assumption, $xy = yx$ and, since this holds for all $x, y \in G/N$, we conclude that $G/N$ is Abelian.

8. Let $G$ be a finite group. Suppose that $H$ is a subgroup of $G$ with $|H| = n$ and such that $H$ is the only subgroup of $G$ of order $n$. Prove that $H$ is a normal subgroup of $G$.

**Solution.** Recall that $H$ is normal iff $Ha = H_a$ for all $a \in G$, iff $aHa^{-1} = H$ for all $a \in G$. The map $H \to aHa^{-1}$ sending $h$ to $aha^{-1}$ is a bijection; it is onto by definition of $aHa^{-1}$, and is 1-1 since if $aha^{-1} = aka^{-1}$, then cancellation shows $h = k$. Then
this will yield $|aHa^{-1}| = |H|$. Consequently, if $H$ is the only subgroup of $G$ of order $n$, we get $aHa^{-1} = H$ for all $a \in G$, and so $H$ is normal in $G$.

9. Prove that $\mathbb{R}^*$ is isomorphic to $\mathbb{R}^+ \times \{1, -1\}$ by defining an explicit function from one to the other, and showing that it is a group homomorphism, 1-1, and onto.

Solution. Define $\varphi : \mathbb{R}^* \to \mathbb{R}^+ \times \{1, -1\}$ by $\varphi(a) = (|a|, \text{sgn}(a))$, where $\text{sgn}$ is the sign function. That is, $\text{sgn}(a) = 1$ if $a > 0$ and $\text{sgn}(a) = -1$ if $a < 0$. Note that $\text{sgn}$ preserves multiplication. Therefore, if $a, b \in \mathbb{R}^*$, then

$$\varphi(ab) = (|ab|, \text{sgn}(ab)) = (|a||b|, \text{sgn}(a)\text{sgn}(b)) = (|a|, \text{sgn}(a))(|b|, \text{sgn}(b)) = \varphi(a)\varphi(b).$$

Therefore, $\varphi$ is a group homomorphism. Note that $a = \text{sgn}(a)|a|$ for each nonzero real number $a$. From this we see that if $\varphi(a) = \varphi(b)$, then $|a| = |b|$ and $\text{sgn}(a) = \text{sgn}(b)$, so $a = b$ from this formula. Finally, It is onto since if $(\alpha, s) \in \mathbb{R}^+ \times \{1, -1\}$, then $a = s\alpha$ maps to $(\alpha, s)$.

10. Find all solutions to the equation $x^2 - 3x + 2 = 0$ in $\mathbb{Z}_6$.

Solution. Note that this factors as $(x - 2)(x - 1)$. This implies that 1, 5 are solutions. However, if we plug in all six elements in, we’ll see that 5 is also a solution.

11. Find all solutions to $x^2 = x$ in $\mathbb{Z}_{15}$.

Solution. Note this question is asking for all the idempotents of $\mathbb{Z}_{15}$. Testing all elements shows that the idempotents are 0, 1, 6, 10.

12. Find all units in the ring $\mathbb{Z} \times \mathbb{Q}$.

Solution. Let $(n, q) \in \mathbb{Z} \times \mathbb{Q}$. If it has an inverse $(m, r)$, then $(n, q)(m, r) = (1, 1)$. This means $mn = 1 = qr$. Since $m, n \in \mathbb{Z}$, we see that $n = \pm 1$ and $m = n$. Since $q, r \in \mathbb{Q}$ and every nonzero element of $\mathbb{Q}$ has a multiplicative inverse in $\mathbb{Q}$, the only restriction is $q \neq 0$. Therefore, the set of units is

$$\{(n, q) : n = \pm 1, q \in \mathbb{Q} - \{0\}\}.$$

13. A subring $S$ of a ring $R$ is a nonempty subset of $R$ which is a ring under the induced operations of $R$. Show that a nonempty subset $S$ of a ring $R$ is a subring if $a, b \in S$ implies $a - b \in S$ and $a, b \in S$ implies $ab \in S$.

Solution. We need to know that $S$ is closed under addition, multiplication, and negation. All the other properties are inherited from $S$ being a subset of $R$ (that is, associativity of both operations, commutativity of addition, the distributive property). Note that 0 $\in S$ if $S$ is closed under addition and negation. So, we need to prove that if
$a, b \in S$ implies $a - b \in S$, then $S$ is closed under addition and negation. This is really a group theory argument. Let $a \in S$. Then with $b = a$, we see $a - a \in S$. Therefore, $0 \in S$. Next, with $a = 0$, for any $b \in S$ we have $-b = a - b \in S$. Therefore, $S$ is closed under negation. Finally, if $a, b \in S$, we have $a, -b \in S$ by the previous line. Therefore, $a - (-b) \in S$, so $a + b \in S$. This shows $S$ is closed under addition.

14. Let $R$ be a ring with unity $1$. If the order of $1$ in the group $(R, +)$ is finite, say $n$, show that each element of $(R, +)$ has finite order, and that the order of each element divides $n$.

**Solution.** Let $a \in R$. Then with $b = a$, we see $a - a \in S$. Therefore, $0 \in S$. Next, with $a = 0$, for any $b \in S$ we have $-b = a - b \in S$. Therefore, $S$ is closed under negation. Finally, if $a, b \in S$, we have $a, -b \in S$ by the previous line. Therefore, $a - (-b) \in S$, so $a + b \in S$. This shows $S$ is closed under addition.

15. Let $R = \mathbb{Z}_p[x]$, the ring of polynomials over $\mathbb{Z}_p$. Show that each nonzero element has order $p$ (in the additive group). Why is $R$ infinite?

**Solution.** This essentially follows from the previous problem, knowing that $1 \in \mathbb{Z}_p[x]$ is the same as $1 \in \mathbb{Z}_p$, which has order $p$. The previous problem shows that the order of anything divides $p$. Thus, the order is $1$ or $p$. The only element with order $1$ is $0$. Therefore, each nonzero element has order $p$. Note that $\mathbb{Z}_p[x]$ is infinite because there are infinitely many monomials $x^n$.

16. Let $R = \{a + bi : a, b \in \mathbb{Z}\}$. Show that $R$ is a subring of $\mathbb{C}$. Also, determine the units of $R$. Using complex conjugation is likely to help to determine the units.

**Solution.** We use the result of Problem 13 to simplify this. Let $x, y \in R$ and write $x = a + bi$ and $y = c + di$ for some $a, b, c, d \in \mathbb{Z}$. Then

$$x - y = (a + bi) - (c + di) = (a - c) + (b - d)i \in R$$

and

$$xy = (a + bi)(c + di) = (ac - bd) + (ad + bc)i \in R$$

since $\mathbb{Z}$ is closed under addition, subtraction, and multiplication. Thus, $R$ is a subring of $\mathbb{C}$. To determine the units, suppose that, with notation above, $xy = 1$. Then $\overline{xy} = 1$, and multiplying these equations together gives $(x\overline{x})(y\overline{y}) = 1$. We see that $\|x\|^2 = x\overline{x} = a^2 + b^2$. Since $a, b \in \mathbb{Z}$, the square $\|x\|^2$ of the norm is an integer. Then $\|x\|^2\|y\|^2 = 1$ means $\|x\|^2 = 1$. This says $a^2 + b^2 = 1$. Again, because $a, b$ are integers, we must have $a = 0$ and $b = \pm 1$ or $a = \pm 1$ and $b = 0$. This yields that the units of $R$ are $\{1, -1, i, -i\}$. 

4
17. Prove or disprove that $R = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{R}$.

**Solution.** This is not a subring, but the argument will use some things we haven’t seen. The easiest way to see it is to see that $R$ is not closed under multiplication. For, $x = \sqrt{2} \in R$ but $x^2 = \sqrt{4} \notin R$; to see that, if $x^2 \in R$, then $x^2 = a + bx$ for some $a, b \in \mathbb{Z}$. Then $x^2 - bx - a = 0$. This is a polynomial equation for which $x$ is a root. But $x^3 - 2 = 0$ is another such polynomial equation. If we take the greatest common divisor of these two polynomials, the result is another polynomial equation for $x$, but by applying the Euclidean algorithm for this, one sees that gcd is the constant polynomial 1. This cannot be a polynomial equation for $x$ since $x \neq 0$. This is a contradiction.