MATH 335 Final Exam 05/24/06 Solutions

(1) Viewing $\langle 3\rangle$ and $\langle 12\rangle$ as subgroups of $\mathbb{Z}$, prove that $\langle 3\rangle / \langle 12\rangle$ is isomorphic to $\mathbb{Z}_4$.

Solution 1: Compute the addition table for $\langle 3\rangle / \langle 12\rangle$ and compare it with that of $\mathbb{Z}_4$.

Solution 2: Let $\phi : \langle 3\rangle \to \mathbb{Z}_4$ be defined by $\phi(3k) = k \bmod 4$. This function is a homomorphism, since for any $3j, 3k \in \langle 3\rangle$, we have

$$\phi(3j + 3k) = \phi(3(j + k)) = (j + k) \bmod 4 = (j \bmod 4) + (k \bmod 4) = \phi(3j) + \phi(3k)\ .$$

Since $\phi(0) = 0$, $\phi(3) = 1$, $\phi(6) = 2$, and $\phi(9) = 3$, ϕ is onto.

Thus the isomorphism theorem gives $\langle 3\rangle / \ker\phi \simeq \mathbb{Z}_4$.

Finally, $\ker\phi$ consists of all numbers $3k$ for which $4|k$, whence $\ker\phi = \{12k : k \in \mathbb{Z}\} = \langle 12\rangle$.

(2) Fix an integer $n \geq 2$, and consider the map $\phi : S_n \to \mathbb{Z}_2$ given by

$$\phi(\alpha) = \begin{cases} 0 & \text{if } \alpha \text{ is even,} \\ 1 & \text{if } \alpha \text{ is odd.} \end{cases}$$

Show that ϕ is a homomorphism, determine its kernel, and conclude from this that A_n is a normal subgroup of S_n.

We proved in class that the product of two even permutations is even, as is the product of two odd permutations, and that the product of an even and an odd permutations is odd.

Suppose $\alpha, \beta \in S_n$. If α and β are even, then so is $\alpha \circ \beta$, whence

$$\phi(\alpha \circ \beta) = 0 = 0 + 0 = \phi(\alpha) + \phi(\beta)\ .$$

If α and β are odd, then $\alpha \circ \beta$ is even, whence

$$\phi(\alpha \circ \beta) = 0 = 1 + 1 = \phi(\alpha) + \phi(\beta)\ .$$

If one of α and β is even and the other one odd, say α is even and β odd, then $\alpha \circ \beta$ is odd, whence

$$\phi(\alpha \circ \beta) = 1 = 0 + 1 = \phi(\alpha) + \phi(\beta)\ .$$

This proves that ϕ is a homomorphism.

The kernel of ϕ consists of all even permutations, whence $\ker\phi = A_n$.

Since the kernel of a homomorphism $G \to H$ forms a normal subgroup of G, we conclude that A_n is normal in S_n.

(3) Let H be a subgroup of the group G. Let $N(H) = \{x \in G : xHx^{-1} = H\}$ (the *normalizer* of H) and $C(H) = \{x \in G : xhx^{-1} = h \text{ for all } h \in H\}$ (the *centralizer* of H). Prove that $N(H)$ and $C(H)$ are subgroups of G.

Suppose $x, y \in N(H)$. We will show that $x^{-1}y \in N(H)$, which proves that $N(H)$ is a subgroup of G. We are given that

$$xHx^{-1} = yHy^{-1} = H\ . \tag{1}$$

In particular, given $h_1 \in H$, there exists $h_2 \in H$ such that $xh_1x^{-1} = yh_2y^{-1}$. We multiply $xh_1x^{-1} = yh_2y^{-1}$ by x^{-1} on the left and x on the right to obtain

$$h_1 = x^{-1}yh_2y^{-1}x \ .$$

Since $\left(x^{-1}y\right)^{-1} = y^{-1}x$, this proves $H \subseteq \left(x^{-1}y\right) H \left(x^{-1}y\right)^{-1}$.

On the other hand, (1) also gives that, given $h_2 \in H$, there exists $h_1 \in H$ such that $xh_1x^{-1} = yh_2y^{-1}$. Now we can repeat the above argument to conclude $H \supseteq \left(x^{-1}y\right) H \left(x^{-1}y\right)^{-1}$.

In summary, we have proved that $H = \left(x^{-1}y\right) H \left(x^{-1}y\right)^{-1}$, whence $x^{-1}y \in N(H)$.

Now suppose $x, y \in C(H)$. Similarly to the above, we will show that $x^{-1}y \in C(H)$, which proves that $C(H)$ is a subgroup of G. We are given that $xhx^{-1} = yhx^{-1} = h$ for all $h \in H$. If we multiply $xhx^{-1} = yhy^{-1}$ by x^{-1} on the left and x on the right, we obtain

$$h = x^{-1}yhy^{-1}x \qquad \text{for all } h \in H \ .$$

Once more, since $\left(x^{-1}y\right)^{-1} = y^{-1}x$, we obtain $h = \left(x^{-1}y\right) h \left(x^{-1}y\right)^{-1}$ for all $h \in H$, which means that $x^{-1}y \in C(H)$.

(4) Prove that $\mathbb{Z}[i]/\langle 1-i \rangle$ is a field. Conclude that $\langle 1-i \rangle$ is a prime ideal in $\mathbb{Z}[i]$. (*Hint:* Start by showing that $2 \in \langle 1-i \rangle$.)

Let $I = \langle 1-i \rangle$ in $\mathbb{Z}[i]$. Since I is an ideal, $2 = (1-i)(1+i) \in I$.

Since $1 - i \in I$, we have $1 + I = i + I$, and so every element $a + bi + I \in \mathbb{Z}[i]/I$ can be written as $a + I$ for some $a \in \mathbb{Z}$.

Furthermore, since $2 \in I$, every element in $\mathbb{Z}[i]/I$ can be written as $a + I$, where $a = 0$ or 1.

Hence $\mathbb{Z}[i]/I$ consists of the two elements I and $1 + I$, and hence $\mathbb{Z}[i]/I$ is a field.

By a theorem proved in class, $\mathbb{Z}[i]/I$ being a field implies that I is maximal, which in turn implies that I is prime.

(5) Show that $3x + 1$ is a unit in $\mathbb{Z}_9[x]$, but not a unit in $\mathbb{Z}[x]$. Determine $U(\mathbb{Z}[x])$.

Since in $\mathbb{Z}_9[x]$, we have $(3x + 1)(-3x + 1) = 1$, we can conclude that $3x + 1 \in U\left(\mathbb{Z}_9[x]\right)$.

Since $\mathbb{Z}$ is an integral domain, the degree of a product of two polynomials equals the sum of the degrees, and so the degree of $(3x + 1)\, g(x)$ is at least one, for any nonzero $g(x) \in \mathbb{Z}[x]$. Since the constant polynomial 1 has degree zero, $3x + 1$ cannot be a unit in $\mathbb{Z}[x]$.

More generally, suppose $f(x), g(x) \in \mathbb{Z}[x]$ are units, i.e., $f(x)\, g(x) = 1$.

Since $\mathbb{Z}$ is an integral domain, we conclude that $\deg(f) + \deg(g) = 0$, which implies that f and g are both constants.

Hence $U(\mathbb{Z}[x])$ consists of the units in $\mathbb{Z}$, which are ± 1.