Math 581 Problem Set 3 Solutions

1. Prove that complex conjugation is a isomorphism from $\mathbb{C}$ to $\mathbb{C}$.

Proof: First we prove that it is a homomorphism. Define $\phi : \mathbb{C} \to \mathbb{C}$ by $\phi(z) = \overline{z}$. Note that $\phi(1) = 1$. The other properties of a homomorphism follow from properties of complex conjugation proved last term, namely, we have

$$\begin{aligned} \phi(z+w) &= \overline{z+w} \\ &= \overline{z} + \overline{w} \\ &= \phi(z) + \phi(w) \end{aligned}$$

and

$$\begin{aligned} \phi(zw) &= \overline{zw} \\ &= \overline{z} \cdot \overline{w} \\ &= \phi(z)\phi(w). \end{aligned}$$

Thus, ϕ is a homomorphism. To see ϕ is surjective, let $z \in \mathbb{C}$. Then $\phi(\overline{z}) = \overline{\overline{z}} = z$. The fact that ϕ is injective follows from the fact that $\overline{z} = 0$ if and only if $z = 0$. Thus, ϕ is an isomorphism. ■

2. Let $a, b \in R$ and suppose $\langle a \rangle = \langle b \rangle$. What can we conclude about a and b?

Note that since the ideals are equal, we have $a \in \langle b \rangle$ and $b \in \langle a \rangle$, i.e., $b|a$ and $a|b$. This is equivalent to the statement that there exists $k, l \in R$ so that $a = bk$ and $b = al$. Substituting, we have $a = alk$. Similarly, we have $b = bkl$. Thus we have $a(1_R - lk) = 0_R$ and $b(1_R - kl) = 0_R$. Thus, either a and b are zero divisors, or $kl = 1_R$. If $kl = 1_R$, then k and l are units and we can say a and b differ by a unit.

3. Find all ideals in the ring $\mathbb{Z}/12\mathbb{Z}$.

Note that in problem 6 we will show that $\mathbb{Z}/12\mathbb{Z}$ is a PID, so we only need to decide which of the principal ideals are equal. Recall that if $a \in \mathbb{Z}$ is relatively prime to 12 then $\overline{a}$ is a unit in $\mathbb{Z}/12\mathbb{Z}$. (You should be able to prove this fact!) We also have seen that if an ideal contains a unit, the ideal must be the entire ring. Therefore, the ideals $\langle \overline{1} \rangle$, $\langle \overline{5} \rangle$, $\langle \overline{7} \rangle$, and $\langle \overline{11} \rangle$ are all equal to $\mathbb{Z}/12\mathbb{Z}$. We also have the ideals:

$$\begin{aligned}
\langle\overline{2}\rangle &= \{\overline{0},\overline{2},\overline{4},\overline{6},\overline{8},\overline{10}\},\\
\langle\overline{3}\rangle &= \{\overline{0},\overline{3},\overline{6},\overline{9}\},\\
\langle\overline{4}\rangle &= \{\overline{0},\overline{4},\overline{8}\},\\
\langle\overline{6}\rangle &= \{\overline{0},\overline{6}\},\\
\langle\overline{8}\rangle &= \{\overline{0},\overline{4},\overline{8}\} = \langle\overline{4}\rangle,\\
\langle\overline{10}\rangle &= \{\overline{0},\overline{2},\overline{4},\overline{6},\overline{8},\overline{10}\} = \langle\overline{2}\rangle.
\end{aligned}$$

This is a complete list of the ideals.

4. Prove that the map $\phi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ defined by $\phi(x) = x^p$ is a ring homomorphism for p a prime. Find $\ker\phi$.

Proof: Note first that $\phi(\overline{1}) = \overline{1}$. We also have $\phi(xy) = (xy)^p = x^p y^p = \phi(x)\phi(y)$ where we have used that $\mathbb{Z}/p\mathbb{Z}$ is commutative. To see that ϕ respects addition, observe that $\phi(x+y) = (x+y)^p = x^p + y^p = \phi(x) + \phi(y)$ where we have used that p divides the binomial coefficients. Thus ϕ is a homomorphism. Let $x \in \ker\phi$. Then $x^p = \overline{0}$. However, $\mathbb{Z}/p\mathbb{Z}$ is a field, so there are no zero-divisors. Thus it must be that $x = \overline{0}$. One should also note that since these are finite sets with the same number of elements, an injective function must also be surjective. Thus, ϕ is actually an isomorphism! ■

5. Use the ring homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ for an appropriate value of m to prove that the equation $x^2 - 5y^2 = 2$ has no solution for $x, y \in \mathbb{Z}$.

Proof: Suppose that $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ is a solution to the equation. Applying ϕ to the equation $x^2 - 5y^2 = 2$ with $m = 5$ and using that ϕ is a homomorphism gives the equation $\phi(x)^2 = \phi(2) = \overline{2}$. However, it is easy to check that there is no element in $\mathbb{Z}/5\mathbb{Z}$ that squares to give $\overline{2}$. Thus, there can be no such (x, y). ■

6. Let R and S be commutative rings, and let $\phi : R \to S$ be a ring homomorphism.

(a) Give an ideal $J \subset S$, define

$$\phi^{-1}(J) = \{r \in R : \phi(r) \in J\} \subset R.$$

Prove that $\phi^{-1}(J)$ is an ideal.

Proof: Note that since ϕ is a homomorphism, $0_R \in \phi^{-1}(J)$ since O_S is necessarily in J. Let $a, b \in \phi^{-1}(J)$. Then we have $\phi(a), \phi(b) \in J$ by definition. Since J is an ideal, $\phi(a) + \phi(b) \in J$. But ϕ is a homomorphism, so $\phi(a+b) = \phi(a)+\phi(b) \in J$. Thus, $a+b \in \phi^{-1}(J)$. Let $r \in R$. Then since J is an ideal, $\phi(r)\phi(a) \in J$. Since ϕ is a homomorphism, $\phi(ra) = \phi(r)\phi(a) \in J$. Thus, $ra \in \phi^{-1}(J)$. Thus $\phi^{-1}(J)$ is an ideal. ■

(b) Given an ideal $I \subset R$, prove that

$$\phi(I) = \{\phi(r) : r \in I\} \subset S$$

is an ideal if ϕ is surjective.

Proof: Note that $O_S \in \phi(I)$ since ϕ is a homomorphism and $0_R \in I$ necessarily. Let $c, d \in \phi(I)$. By definition there exists $a, b \in I$ so that $\phi(a) = c$ and $\phi(b) = d$. Since I is an ideal, $a + b \in I$. Thus, $c + d = \phi(a) + \phi(b) = \phi(a + b) \in \phi(I)$. Now let $s \in S$. Since ϕ is surjective, there exists an $r \in R$ so that $\phi(r) = s$. Then one has $cs = \phi(a)\phi(r) = \phi(ar) \in \phi(I)$ since $ar \in I$ (I an ideal). Thus we have that $\phi(I)$ is an ideal.
If ϕ is not surjective this is not necessarily true. For example, consider the map $\phi : \mathbb{Z} \to \mathbb{Q}$ that is the identity, i.e., $\phi(n) = n$. Let $I = \langle 2 \rangle$. Then one has $\phi(I) = I$ in $\mathbb{Q}$. However, in $\mathbb{Q}$ this is no longer an ideal as $\frac{1}{2} \in \mathbb{Q}$ and $2 \in I$ but $1 \notin I$. ■

(c) Prove that every ideal in $\mathbb{Z}/m\mathbb{Z}$ is principal.

Proof: Let I be an ideal in $\mathbb{Z}/m\mathbb{Z}$. By part (a) we know that $\phi^{-1}(I)$ is an ideal in $\mathbb{Z}$. Since $\mathbb{Z}$ is a PID, there exists $n \in \mathbb{Z}$ so that $\phi^{-1}(I) = \langle n \rangle$. Let $a \in I$. Observe that there exists $b \in \phi^{-1}(I)$ so that $\phi(b) = a$. Since $b \in \phi^{-1}(I)$ we have $n|b$. Thus there exists $r \in \mathbb{Z}$ so that $rn = b$. Applying ϕ we have $\phi(r)\phi(n) = a$. This shows that any element of I is divisible by $\phi(n)$, i.e., $I = \langle \phi(n) \rangle$. One should also observe that this same proof works to show that if $\psi : R \to S$ is a ring homomorphism from a PID to a ring, then $\phi(R)$ is a PID as well. ■

7. If $\gcd(m, n) = 1$ in $\mathbb{Z}$, prove that $\langle m \rangle \cap \langle n \rangle$ is the ideal $\langle mn \rangle$.

Proof: Recall that $\langle a \rangle = \{ax : x \in \mathbb{Z}\}$. Let $mnx \in \langle mn \rangle$. Then $mnx \in \langle m \rangle$ and $mnx \in \langle n \rangle$ for all $x \in \mathbb{Z}$, so $\langle mn \rangle \subset \langle m \rangle \cap \langle n \rangle$. Now let $a \in \langle m \rangle \cap \langle n \rangle$, i.e., $a \in \langle m \rangle$ and $a \in \langle n \rangle$. Thus, $m|a$ and $n|a$. As we saw in a previous homework problem, since $\gcd(m,n) = 1$, we have $mn|a$. Thus, $a \in \langle mn \rangle$. Combining this with the above containment gives $\langle m \rangle \cap \langle n \rangle = \langle mn \rangle$, as claimed. ■

8. Let $\phi : R \to S$ be an isomorphism. Prove that:
(a) $\phi(u)$ is a unit if and only if u is a unit

Proof: Let $u \in R$ be a unit, i.e., there exists $t \in R$ so that $ut = 1_R = tu$. Applying ϕ we see this is equivalent to the statement that $\phi(ut) = 1_S = \phi(tu)$. Since ϕ is a homomorphism, we obtain $\phi(u)\phi(t) = 1_S = \phi(t)\phi(u)$. Thus, if u is a unit then $\phi(u)$ is a unit. Now suppose $\phi(u)$ is a unit, i.e., there exists an $s \in S$ so that $\phi(u)s = 1_S = s\phi(u)$. Here we use that ϕ is surjective to conclude that there exists a $t \in R$ so that $\phi(t) = s$. Thus, $\phi(ut) = 1_S = \phi(1_R)$. Now use that ϕ is injective to conclude that $ut = 1_R$ and similarly for tu. Thus, u is a unit. ■

(b) $\phi(b)$ is a zero-divisor if and only if b is a zero-divisor

Proof: Let $b \in R$ be a zero-divisor, i.e., there exists an $a \in R$ with $a \neq 0_R$ so that $ab = 0_R = ba$. As above, we apply ϕ to obtain $\phi(a)\phi(b) = 0_S = \phi(b)\phi(a)$. Here it is important to note that since ϕ is an isomorphism, it is injective so that $\phi(a) \neq 0_S$ and so $\phi(a)$ and $\phi(b)$ are zero-divisors. Now suppose that $\phi(b)$ is a zero-divisor, i.e., there exists a $0 \neq c \in S$ so that $\phi(b)c = 0_S = c\phi(b)$. Since ϕ is surjective, there exists $a \in R$ so that $\phi(a) = c$. Thus $\phi(ab) = \phi(ba) = 0_S$. Since ϕ is injective we have that $a \neq 0_R$ and $ab = 0_R = ba$. Thus, b is a zero-divisor. ■

9. Using the first isomorphism theorem, prove that $\mathbb{Q}[x]/\langle x^2+x+1 \rangle \cong \mathbb{Q}[\omega]$ where ω is a third root of unity.

Proof: Recall that $\mathbb{Q}[\omega] = \{f(\omega) : f(x) \in \mathbb{Q}[x]\}$. This leads one to define $\phi : \mathbb{Q}[x] \to \mathbb{Q}[\omega]$ by $\phi(f(x)) = f(\omega)$. Clearly ϕ is surjective. To see ϕ is a homomorphism, observe that

$$\begin{aligned} \phi(f(x)g(x)) &= f(\omega)g(\omega) \\ &= \phi(f(x))\phi(g(x)) \end{aligned}$$

and

$$\begin{aligned}\phi(f(x)+g(x)) &= f(\omega)+g(\omega)\\ &= \phi(f(x))+\phi(g(x)).\end{aligned}$$

It is also clear that $\phi(1) = 1$. Now we just need to prove that $\ker\phi = \langle x^2+x+1\rangle$. Since $\omega^2+\omega+1 = 0$, one sees that $\langle x^2+x+1\rangle \subset \ker\phi$. Since $\mathbb{Q}[x]$ is a PID and x^2+x+1 is irreducible (degree 2 polynomial with no rational roots!), we must have $\ker\phi = \langle x^2+x+1\rangle$. (See Corl 1.3!) Thus, by the 1^{st} isomorphism theorem we have that $\mathbb{Q}[x]/\langle x^2+x+1\rangle \cong \mathbb{Q}[\omega]$. ■

10. Is $(\mathbb{Z}/3\mathbb{Z})\times(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/9\mathbb{Z}$? Be sure to justify your answer.

Proof: Suppose these two rings are isomorphic. Then there exists an isomorphism $\phi : \mathbb{Z}/9\mathbb{Z} \to (\mathbb{Z}/3\mathbb{Z})\times(\mathbb{Z}/3\mathbb{Z})$. Since ϕ is an isomorphism, we know that $\phi(1) = (1,1)$. Thus, $\phi(2) = \phi(1+1) = \phi(1)+\phi(1) = (1,1)+(1,1) = (2,2)$. Similarly, $\phi(3) = \phi(2+1) = \phi(2)+\phi(1) = (2,2)+(1,1) = (3,3) = (0,0)$. This is a contradiction however as then $3 \in \ker\phi$, but ϕ being an isomorphism means that ϕ is injective and has trivial kernel. Thus there can be no such isomorphism. ■

11. Let p be a prime number.
(a) Prove that $\mathbb{Q}[\sqrt{p}] \cong \mathbb{Q}[x]/\langle x^2 - p\rangle$.

Proof: Define $\phi : \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{p}]$ by $\phi(f(x)) = f(\sqrt{p})$. Now one uses the first isomorphism theorem just as in problem 9. The only difference it concluding that $x^2 - p$ is irreducible by Eisenstein's criterion with p. ■

(b) Prove that

$$\mathbb{Q}[\sqrt{p}] \cong \left\{ \begin{pmatrix} a & pb \\ b & a \end{pmatrix} : a, b \in \mathbb{Q} \right\}.$$

Proof: Set $\mathcal{A} = \left\{ \begin{pmatrix} a & pb \\ b & a \end{pmatrix} : a, b \in \mathbb{Q} \right\}$. Define the map $\phi : \mathcal{A} \to \mathbb{Q}[\sqrt{p}]$ by

$\phi\left(\begin{pmatrix} a & pb \\ b & a \end{pmatrix}\right) = a + b\sqrt{p}$. Note that $\phi\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = 1$. We also have

$$\begin{aligned}
\phi\left(\begin{pmatrix} a & pb \\ b & a \end{pmatrix} + \begin{pmatrix} c & pd \\ d & c \end{pmatrix}\right) &= \phi\left(\begin{pmatrix} a+c & p(b+d) \\ b+d & a+c \end{pmatrix}\right) \\
&= (a+c) + (b+d)\sqrt{p} \\
&= (a + b\sqrt{p}) + (c + d\sqrt{p}) \\
&= \phi\left(\begin{pmatrix} a & pb \\ b & a \end{pmatrix}\right) + \phi\left(\begin{pmatrix} c & pd \\ d & c \end{pmatrix}\right).
\end{aligned}$$

and

$$\begin{aligned}
\phi\left(\begin{pmatrix} a & pb \\ b & a \end{pmatrix} \begin{pmatrix} c & pd \\ d & c \end{pmatrix}\right) &= \phi\left(\begin{pmatrix} ac+pbd & p(ad+bc) \\ ad+bc & ac+pbd \end{pmatrix}\right) \\
&= ac + pbd + (ad+bc)\sqrt{p} \\
&= (a + b\sqrt{p})(c + d\sqrt{p}) \\
&= \phi\left(\begin{pmatrix} a & pb \\ b & a \end{pmatrix}\right) \phi\left(\begin{pmatrix} c & pd \\ d & c \end{pmatrix}\right).
\end{aligned}$$

Thus we have that ϕ is a homomorphism. Now we just need to show ϕ is surjective and injective. Let $a + b\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$. To see ϕ is surjective, just observe that $\phi\left(\begin{pmatrix} a & pb \\ b & a \end{pmatrix}\right) = a + b\sqrt{p}$. To see ϕ is injective, suppose $\phi\left(\begin{pmatrix} a & pb \\ b & a \end{pmatrix}\right) = 0$. Then, $0 = a + b\sqrt{p}$ so $a = b = 0$ and thus $\begin{pmatrix} a & pb \\ b & a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ so so $\ker\phi = 0$. Thus, ϕ is an isomorphism. ■