MATH 3GR3 Assignment #6 Solutions
Due: Wednesday, December 6 by 11:59pm

1. Consider the ring $\mathbb{Z}_{20}$. List all of the ideals of this ring. List all of the units of this ring.

   Solution: All of the ideals of the ring $\mathbb{Z}_n$ are principal (Theorem 16.25 establishes this for $\mathbb{Z}$, the same holds for $\mathbb{Z}_n$), and so the ideals of $\mathbb{Z}_{20}$ are of the form $\langle a \rangle$ with $a \in \mathbb{Z}_{20}$. These are also equal to the subgroups of the group $\mathbb{Z}_{20}$, and so the following is a complete list of the ideals:

   $$\mathbb{Z}_{20}, \langle 2 \rangle, \langle 4 \rangle, \langle 5 \rangle, \langle 10 \rangle, \langle 0 \rangle.$$

   The units are just the members of $U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$.

2. For each pair of rings, determine if they are isomorphic.

   (a) $\mathbb{R}$ and $\mathbb{C}$.

   (b) $\mathbb{Z}$ and $\mathbb{Z}[i]$.

   Solution: For (a), the two rings are not isomorphic, since every element from $\mathbb{C}$ has a square root, but not every element from $\mathbb{R}$ does. So, if $\phi : \mathbb{C} \to \mathbb{R}$ is an isomorphism, there is some $c \in \mathbb{C}$ with $\phi(c) = -1$. If $d \in \mathbb{C}$ with $dd = c$, then $-1 = \phi(c) = \phi(dd) = \phi(d)\phi(d) = r^2$, where $r = \phi(d)$. This shows that in $\mathbb{R}$, the element -1 has a square root. Since it doesn't, then there can't be any such isomorphism.

   The argument for (b) is similar. We can see that the two rings are not isomorphic, since in $\mathbb{Z}[i]$, the element -1 has a square root, while in $\mathbb{Z}$ it doesn't. Any isomorphism ϕ from $\mathbb{Z}[i]$ to $\mathbb{Z}$ must map the identity element 1 to 1 and so must map -1 to -1. So $-1 = \phi(-1) = \phi(i^2) = (\phi(i))^2$, which implies that -1 has a square root in $\mathbb{Z}$, which it doesn't.

3. Show that the map $f : \mathbb{C} \to M_{2\times 2}(\mathbb{R})$ defined by

   $$f(a + bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

   is a one-to-one homomorphism from the ring of complex numbers to the ring of 2×2 matrices with real entries.

Solution: If $f(a+bi)$ equals the Zero matrix, then $a=b=0$ and so the kernel of f is $\{0\}$. From this it follows that f is one-to-one. Using the rules for matrix addition and multiplication we can see that f is a homomorphism

$$f((a+bi)+(c+di)) = f((a+c)+(b+d)i) = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix}$$

while

$$f(a+bi)+f(c+di) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix}.$$

Similarly,

$$f((a+bi)(c+di)) = f((ac-bd)+(ad+bc)i) = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}$$

while

$$f(a+bi)f(c+di) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}.$$

4. Let R be a commutative ring with identity and suppose that I and J are ideals of R. Show that $I \cap J$ is also an ideal of R. If I and J are prime ideals of R will $I \cap J$ always be a prime ideal of R?

   Solution: We need to show that $I \cap J$ is non-empty and if $a, b \in I \cap J$ and $r \in R$ then $a - b \in I \cap J$ and ra and $ar \in I \cap J$. Clearly $I \cap J$ is non-empty since 0 is a member of it. Since $a, b \in I$ and are in J then $a-b$, ra, and ar are in I and in J and so belong to $I \cap J$.

   If I and J are prime ideals of R, then $I \cap J$ need not be prime. For example, we know that the ideals $2\mathbb{Z}$ and $3\mathbb{Z}$ are prime ideals of $\mathbb{Z}$, but their intersection, $6\mathbb{Z}$, is not a prime ideal (since $6 = (2)(3) \in 6\mathbb{Z}$ but 2 and 3 are not).

5. Let

$$I = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{Z}[x] \mid a_0 \text{ is even}\}.]$$

   (a) Show that I is an ideal of $\mathbb{Z}[x]$.

(b) Show that $\mathbb{Z}[x]/I$ is isomorphic to $\mathbb{Z}_2$.

(c) Prove that I is a maximal ideal of $\mathbb{Z}[x]$.

Solution:

(a) Since $2 \in I$, I is nonempty. If $p(x), q(x) \in I$ and $r(x) \in R$, then p_0 and q_0 are even, so $p_0 + q_0$ and $r_0 p_0$ are even, which means $p(x) + q(x) \in I$ and $r(x)p(x) \in I$. Thus, by the proposition from question 3 and the fact that multiplication in $\mathbb{Z}[x]$ is commutative, I is an ideal.

(b) Define $\phi : \mathbb{Z}[x] \to \mathbb{Z}_2$ by $\phi(p(x)) = p_0 \bmod 2$. Since ϕ is a composition of the evaluation homomorphism $p(x) \mapsto p(0)$ and the quotient homomorphism $a \mapsto a \bmod 2$, ϕ is also a homomorphism. Clearly, ϕ is surjective ($\phi(0) = 0$ and $\phi(1) = 1$) and $\phi(p(x)) = 0$ if and only if p_0 is even. Thus, by the first isomorphism theorem,

$$\mathbb{Z}_2 = \phi(\mathbb{Z}[x]) \cong \mathbb{Z}[x]/\ker(\phi) = \mathbb{Z}[x]/I.$$

(c) By Theorem 16.35, I is maximal if and only if $\mathbb{Z}[x]/I$ is a field. But $\mathbb{Z}[x]/I \cong \mathbb{Z}_2$ is a field, and hence I is maximal.

6. Let $R = \mathbb{Z}[x]$ and let I be the set of polynomials of $\mathbb{Z}[x]$ whose terms have degree at least 2, plus the constant 0 polynomial. So, members of I are of the form $a_2x^2 + a_3x^3 + \cdots + a_nx^n$ for some $n \geq 2$ and integers a_i.

   (a) Show that I is an ideal of R. Hint: Show that $I = \langle x^2 \rangle$.

   (b) Show that the polynomials $3 + 5x + x^3 + x^5$ and $3 + 5x - x^4$ are in the same coset of I and give a general condition for when two polynomials $p(x)$ and $q(x)$ lie in the same coset of I.

   (c) Show that R/I consists of the elements $(a + bx) + I$ for a, $b \in \mathbb{Z}$.

   (d) Describe the addition and multiplication operations on R/I.

   (e) Is R/I an integral domain? (this is the same as asking if I is a prime ideal.)

Solution:

(a) We could prove that I is an ideal directly. Alternatively, notice that $f(x) \in I$ if and only if $x^2 \mid f(x)$, so $I = x^2\mathbb{Z}[x] = \langle x^2 \rangle$. This is clearly an ideal, since it is the ideal generated by x^2.

(b) By definition, two elements are in the same coset if their difference is in I. We have

$$(3 + 5x + x^3 + x^5) - (3 + 5x - x^4) = x^3 + x^4 + x^5 \in I$$

so these two polynomials are in the same coset. In general, let $p(x) = a + bx + x^2 r(x)$ and $q(x) = c + dx + x^2 s(x)$. Then

$$p(x) - q(x) = (a - c) + (b - d)x + x^2(r(x) - s(x))$$

so p and q are in the same coset if and only if $a = c$ and $b = d$.

(c) From part (b), $p(x)$ and $q(x)$ are in the same coset if and only if their constant and linear terms are equal. Thus, each coset contains precisely one element of the form $a + bx$ with $a, b \in \mathbb{Z}$, and so we can consider R/I as the set of such polynomials.

(d) Let $a + bx, c + dx \in R/I$. Then

$$(a + bx) + (c + dx) = (a + c) + (b + d)x$$

and

$$(a + bx)(c + dx) = ac + (ad + bc)x + bdx^2 = ac + (ad + bc)x.$$

(e) No, R/I is not an integral domain, since $x + I \neq 0 + I$, but $(x + I) \cdot (x + I) = x^2 + I = 0 + I$.

Bonus:

(a) Compute the remainder when the polynomial $8x^5 - 18x^4 + 20x^3 - 25x^2 + 20$ is divided by $4x^2 - x - 2$. Both polynomials are members of the polynomial ring $\mathbb{Q}[x]$.

Solution: $8x^5 - 18x^4 + 20x^3 - 25x^2 + 20$ is equal to $(2x^3 - 4x^2 + 5x - 7)(4x^2 - x - 2) + (3x + 6)$, so the remainder is $3x + 6$.

(b) Compute the remainder when the polynomial $3x^4 + x^3 + 2x^2 + 1$ is divided by $x^2 + 4x + 2$. Both polynomials are members of the polynomial ring $\mathbb{Z}_5[x]$.

Solution: $3x^4 + x^3 + 2x^2 + 1$ is equal to $(3x^3 - x)(x^2 + 4x + 2) + (2x + 1)$, so the remained is $2x + 1$.