Math 307 Abstract Algebra Homework 11 **Sample solution**

1. Find an multiplicative inverse of $2x+1$ in $\mathbb{Z}_4[x]$. Is the inverse unique?

   Solution. $(2x+1)(2x+1) = 4x^2+4x+1 = 1$. So, $(2x+1)$ is its own inverse.

   Note that in a ring with unity, if b, c are the inverses of a, then $b = b(ac) = (ab)c = c$. So, the inverse if always unique if it exists.

2. (a) Given an example to show that a factor ring of an integral domain may have zero-divisors.

   (b) Give an example to show that a factor ring of a ring with zero-divisors may be an integral domain.

   Solution. (a) Let $R = \mathbb{Z}$, $A = 4\mathbb{Z}$. Then $R/A \cong \mathbb{Z}_4$ has a zero divisor.

   (b) Let $R = \mathbb{Z}_4$ and $A = \langle 2 \rangle$. Then $R/A = \{0+A, 1+A\} \cong \mathbb{Z}_2$ has no zero divisors.

3. Let R_1 and R_2 be rings, and $\phi : R_1 \to R_2$ be a ring homomorphism.

   (a) Show that if A is an ideal of R_1, then $\phi(A)$ is an ideal of $\phi(R_1)$.

   (b) Give an example to show that $\phi(A)$ may not be an ideal of R_2.

   Solution. (a) Note that $\phi(A)$ is a subgroup of R_2 using the group theory result. So, it is a subgroup of $\phi(R_1)$. For any $b \in \phi(A)$ and $y \in \phi(R_1)$, there are $a \in A$, $x \in R_1$ such that $\phi(a) = b$ and $\phi(x) = y$. Because $ax, xa \in A$, we have $by = \phi(a)\phi(x) = \phi(ax) \in \phi(A)$ and $yb = \phi(x)\phi(a) = \phi(xa) \in \phi(A)$.

   (b) Suppose $A = R_1 = \mathbb{Z}$, $R_2 = \mathbb{Q}$, and $\phi(x) = x$. Then ϕ is a ring homomorphism, $\phi(A) = \phi(R_1) = \mathbb{Z}$ so that $\phi(A)$ is an ideal in $\phi(R_1)$. But $\phi(A) = \mathbb{Z}$ is not an ideal in $R_2 = \mathbb{Q}$, say, $1 \in \mathbb{Z}$, $1/2 \in \mathbb{Q}$ and $1 \cdot (1/2) \notin \mathbb{Z}$.

4. (8 points) Let $A = \langle x^2+x+1 \rangle = \{(x^2+x+1)f(x) : f(x) \in \mathbb{Z}_2[x]\} \subseteq \mathbb{Z}_2[x]$.

   (a) Show that $\mathbb{Z}_2[x]/A = \{a+bx+A : a, b \in \mathbb{Z}_2\}$ has 4 elements.

   Proof: Note that $\mathbb{Z}_2[x]/A = \{f(x)+A : f(x) \in \mathbb{Z}_2[x]\}$. Now for every $f(x) \in \mathbb{Z}_2[x]$, $f(x) = a+bx+(x^2+x+1)q(x)$ so that $f(x)+A = a+bx+(x^2+x+1)q(x)+A = a+bx+A$. Thus, $\mathbb{Z}_2[x]/A = \{a+bx+A : a, b \in \mathbb{Z}_2\} = \{A, 1+A, x+A, 1+x+A\}$ has four distinct elements.

   (b) Show that $(a+bx+A)(c+dx+A) = (ac+bd)+(ad+bc+bd)x+A$.

   Proof: $(a+bx+A)(c+dx+A) = ac+adx+bcx+bdx^2+A = ac+adx+bcx+bdx^2+bd+bd+bdx+bdx+A(ac+bd)+(ad+bc+bd)x+bd(x^2+x+1)A = (ac+bd)+(ad+bc+bd)xA$.

   (c) For each nonzero element $a+bx+A \in \mathbb{Z}_2[x]/A$, show that there is $c+dx+A \in \mathbb{Z}_2[x]/A$ such that $(a+bx+A)(c+dx+A) = 1+A$, and deduce that $\mathbb{F} = \mathbb{Z}_2[x]/A$ is a field.

   Proof: Because $\mathbb{Z}_2[x]/A$ is a commutative ring with unity, we only need to show that every nonzero element has an inverse. Then $\mathbb{Z}_2[x]/A$ is a field. Now, $(1+A)(1+A) = 1+A$ and $(x+A)(1+x+A) = 1+A$. The result follows.

   (d) Show that the nonzero elements in $\mathbb{F}$ form a cyclic group under multiplication.

   Proof: Note that $(x+A)^1 = x+A$, $(x+A)^2 = x^2+A = 1+x+A$, $(x+A)^3 = x^3+A = x(x^2+x+1)+(x^2+x+1)+1+A = 1+A$. The result follows.

5. (12 points) Let $A = \langle x^2+1\rangle = \{(x^2+1)f(x) : f(x) \in \mathbb{Z}_3[x]\} \subseteq \mathbb{Z}_3[x]$.

(a) Show that $\mathbb{Z}_3[x]/A = \{a+bx+A : a, b \in \mathbb{Z}_3\}$ has 9 elements.

Proof: For similar reason in previous problem, $\mathbb{Z}_3[x]/A = \{a+bx+A : a, b \in \mathbb{Z}_3\}$ has 9 elements.

(b) Show that $(a+bx+A)(c+dx+A) = (ac+2bd)+(ad+bc)x+A$.

Proof: $(a+bx+A)(c+dx+A) = ac+adx+bcx+bdx^2+A = ac+(ad+bc)x+bdx^2+bd-bd+A = ac+(ad+bc)x+bd(x^2+1)+-bd+A = ac+(ad+bc)x+bd(x^2+1)+2bd+A = (ac+2bd)+(ad+bc)x+A$

(c) For each nonzero element $a+bx+A \in \mathbb{Z}_3[x]/A$, show that there is $c+dx+A \in \mathbb{Z}_3[x]/A$ such that $(a+bx+A)(c+dx+A) = 1+A$, and deduce that $\mathbb{F} = \mathbb{Z}_3[x]/A$ is a field.

Proof: It suffices to show that every nonzero $(a+bx+A \in \mathbb{Z}_3[x]/A$ has an inverse, i.e., we want to find $(c+dx)$ so that $1 = (a+bx)(c+dx) = (ac+2bd)+(ad+bc)x$, i.e., $ac+2bd = 1, bc+ad = 0$. Solving the linear system with c, d as unknowns, we get $(c, d) = (a^2+b^2)^{-1}(a, 2b)$. Here note that $(a^2+b^2)^{-1} = (a^2+b^2) \in \{1, 2\}$ if $(a, b) \neq (0, 0)$. So, $(a+bx+A)^{-1} = (a^2+b^2)(a+2bx)+A$.

(d) Determine the multiplicative inverse of $1+2x+A \in \mathbb{F}$.

Proof: By (c), $(1+2x+A)^{-2} = 2(1+x+A) = 2+2x+A$.

(e) Show that the nonzero elements in $\mathbb{F} = \mathbb{Z}_3[x]/A$ form a cyclic group under multiplication.

Proof: Note that every element in $\mathbb{F}^*$ has order 2, 4, or 8 under multiplication. Consider$1+x+A$. Then $(1+x+A)^4 = [(1+x+A)^2]^2 = [1+2x+x^2+A]^2 = [2x+A]^2 = 4x^2+A = -1+A$. So, $1+x+A$ has order 8 and is a generator of $\mathbb{F}^*$ under multiplication.

(f) Show that $X = x+A$ is a zero of the polynomial $X^2+1 \in \mathbb{F}[X]$.

Proof: $X^2+1 = (x^2+A)+(1+A) = A$, so $X = x+A$ is a zero of the polynomial $X^2+1 \in \mathbb{F}[X]$.

6. Let $\mathbb{Z}[i] = \{a+ib : a, b \in \mathbb{Z}\}$ be the integral domain $\mathbb{D}$ of Gaussian integers. Let $\mathbb{F} = \{[(a, b)] : a \in \mathbb{D}, b \in \mathbb{D}^*\}$ be the field of quotients of $\mathbb{D}$, and $\mathbb{Q}[i] = \{x+iy : x, y \in \mathbb{Q}\}$.

(a) Show the if $[(a, b)] \in \mathbb{F}$ then $[(a, b)] = [(p+iq, m)]$ for some $p, q \in \mathbb{Z}, m \in \mathbb{N}$.

Proof: Let $[(a, b)] = [(a+ib), (c+id)]$. $\frac{a+ib}{c+id} = \frac{ac+bd+i(bc-ad)}{c^2+d^2}$. Since $a, b, c, d \in \mathbb{Z}$, $c+id \neq 0$, let $p = ac+bd$, $q = bc-ad$, $m = c^2+d^2$. Then $p, q \in \mathbb{Z}$ and $m \in \mathbb{N}$.

(b) Show that $\phi : \mathbb{F} \to \mathbb{Q}[i]$ defined by $\phi([(a+ib, c+id)]) = \frac{ac+bd}{c^2+d^2} + \frac{i(bc-ad)}{c^2+d^2}$ is an isomorphishm.

Proof: Let $A = [(a_1+ib_1, c_1+id_1)], B = [(a_2+ib_2, c_2+id_2)]$.

Well-defined: if $A = B$, then $\frac{a_1+ib_1}{c_1+id_1} = \frac{a_2+ib_2}{c_2+id_2}$, $(a_1c_2+b_1d_2)+i(a_1d_2-b_1c_2) = (a_2c_1+b_2d_1)+i(a_2d_1-b_2c_1)$. Then $a_1c_2+b_1d_2 = a_2c_1+b_2d_1$ and $a_1d_2-b_1c_2 = a_2d_1-b_2c_1$. $\phi(A) = \frac{(a_1c_1+b_1d_1)+i(b_1c_1-a_1d_1)}{c_1^2+d_1^2}$, $\phi(B) = \frac{(a_2c_2+b_2d_2)+i(b_2c_2-a_2d_2)}{c_2^2+d_2^2}$.

One-one: for $A, B \in \mathbb{F}$, if $\phi(A) = \phi(B)$, $\frac{a_1c_1+b_1d_1}{c_1^2+d_1^2} = \frac{a_2c_2+b_2d_2}{c_2^2+d_2^2}$ and $\frac{b_1c_1-a_1d_1}{c_1^2+d_1^2} = \frac{a_2c_2+b_2d_2}{c_2^2+d_2^2}$, so $A = B$.

Onto: for any $y = p+iq \in \mathbb{Q}[i]$, we may let $p = a/m$ and $q = b/m$. Then for $A = [(a+ib, m)]$ we have $\phi(A) = \frac{am}{m^2} + \frac{ibm}{m^2} = y$.

Isomorphism: For any $A, B \in \mathbb{F}$,

$$\begin{aligned}
\phi(A+B) &= \phi([(a_1+a_2)+i(b_1+b_2),(c_1+c_2)+i(d_1+d_2)]) \\
&= \frac{(a_1+a_2)(c_1+c_2)+(b_1+b_2)(d_1+d_2)+i(b_1+b_2)(c_1+c_2)-(a_1+a_2)(d_1+d_2)}{(c_1+c_2)^2+(d_1+d_2)^2} \\
&= \frac{(a_1c_1+b_1d_1)+i(b_1c_1-a_1d_1)}{c_1^2+d_1^2}+\frac{(a_2c_2+b_2d_2)+i(b_2c_2-a_2d_2)}{c_2^2+d_2^2} \\
&= \phi(A)+\phi(B)
\end{aligned}$$

Alternatively

First, note that $\mathbb{Q}[i] = \mathbb{F}_1 = \{(a+ib)/(c+id) : a+ib \in \mathbb{Z}[i], c+id \in \mathbb{Z}[i]^*\}$ under the map $\phi_1((a+ib)/(c+id)) = (ac+bd)/(c^2+d^2)+i(bc-ad)/(c^2+d^2)$, which is just the identity map on the subset $\mathbb{Q}[i] = \mathbb{F}_1$ in $\mathbb{C}$. In particular, ϕ_1 can be viewed as a field isomorphism.

Now, we show that $\mathbb{F}$ is isomorphic to $\mathbb{F}_1$ by the map $\phi_2([a+ib, c+id)]) = (a+ib)/(c+id)$.

Well-defined: Clearly, $[(x_1,y_1)] = [(x_2,y_2)]$ in $\mathbb{F}$ implies $x_1y_2 = x_2y_1$. Applying ϕ to both sides, we get x_1/y_1 and x_2/y_2, which are equal in $\mathbb{F}_1$.

One-one: If $x_1/y_1 = \phi([(x_1,y_1)]) = \phi([(x_2,y_2)]) = x_2/y_2$, then $x_1y_2 = x_2y_1$. So, $[(x_1,y_1)] = [(x_2,y_2)]$.

Onto: If $x/y \in \mathbb{F}_1$, then $f([(x,y)]) = x/y$.

Isomorphism: $\phi([(x_1,y_1)]+[(x_2,y_2)]) = \phi([(x_1y_2+x_2y_1, y_1y_2)]) = (x_1y_2+x_2y_1)/(y_1y_2) = x_1/y_1 + x_2/y_2 = \phi([(x_1,y_1])+\phi([(x_2,y_2)])$.

Also, $\phi([(x_1,y_1)][(x_2,y_2)]) = \phi([(x_1x_2,y_1y_2)]) = (x_1x_2)/(y_1y_2) = (x_1/y_1)(x_2/y_2)$

$= \phi([(x_1,y_1)])\phi([(x_2,y_2)])$.

It follows that $\phi = \phi_2 \circ \phi_1$ is an isomorphism between $\mathbb{F}$ and $\mathbb{Q}[i]$.

Extra credit problems

1. Find an example of a commutative ring R such that $a^2 \neq a$ for any nonzero elements.

   Answer. $R = 2\mathbb{Z}$.

2. Find an example of a non-commutative ring R such that $a^2 = 0$ for all $a \in R$.

   Answer: Unknown???