ASSIGNMENT 5

MATH 235

QUESTION 1

Part (1): Let $R := \mathbb{Z}[i]$ and $I \triangleleft R := 2\mathbb{Z}[i]$. Let $x \in \mathbb{Z}[i] = p + qi$, with $i^2 = -1$. We will consider the cosets $\overline{x} = \{p + qi + 2a + 2bi : a, b \in \mathbb{Z}\}$. For brevity, p, q are always **fixed** integers, and $a, b \in \mathbb{Z}$, $r, s \in \mathbb{Z}$ are **arbitrary**.

$p, q \equiv_2 0$ Let $\overline{x} = \{q + qi + 2a + 2bi : a, b \in \mathbb{Z}\}$. This is $\{2r + 2si : r, s \in \mathbb{Z}\}$, since $p, q \equiv_2 0$. Thus $\overline{x} \in I \implies \overline{x} = \overline{0}$.

$p, q \equiv_2 1$ $\overline{x} = \{p+qi+2a+2bi\} = \{p+2a+(q+2b)i\} = \{2r+1+(2s+1)i\} = \{1+i+2r+2si\}$. Thus, $\overline{x} = \overline{1+i}$

$p \equiv_2 1, q \equiv_2 0$ $\overline{x} = \{p + qi + 2a + 2bi\} = \{1 + 2r + 2si\} \implies \overline{x} = \overline{1}$

$p \equiv_2 0, q \equiv_2 1$ $\overline{x} = \{p+qi+2a+2bi\} = \{p+2a+(q+2b)i\} = \{2r+(2s+1)i\} = \{i+2r+2si\} \implies \overline{x} = \overline{i}$

Since all cases for p, q have been covered (odd/odd, etc.), the set $\{0, 1, i, 1 + i\}$ represents all cosets. If any two of these were equal, then their difference would have to be in $2\mathbb{Z}[i]$, i.e. be $\overline{0} = \overline{2r + 2si}$, which is not true. We conclude that the cosets represented by $\{0, 1, i, 1 + i\}$ are disjoint.

Checking, one sees that $\overline{0} - \overline{a}$ for $a \in \{1, i, 1 + i\}$ is $\not\equiv 0$. The remaning cases are: $\overline{1+i} - \overline{1} = \overline{i} \neq \overline{0}$, $\overline{1+i} - \overline{i} = \overline{1} \neq \overline{0}$, and $\overline{1} - \overline{i} = \overline{1-i} \neq \overline{0}$.

Part (2):

$+$	0	1	i	$1+i$
0	0	1	i	$1+i$
1	1	0	$1+i$	i
i	i	$1+i$	0	1
$1+i$	$1+i$	i	1	0

$\times$	0	1	i	$1+i$
0	0	0	0	0
1	0	1	i	$1+i$
i	0	i	1	$1+i$
$1+i$	0	$1+i$	$1+i$	0

Part (3): R/I is not a field. In order for this to be true, all non-zero elements must have a multiplicative inverse, but $1 + i$ has none (see chart). Furthermore, R/I is not isomorphic to $\mathbb{Z}/4\mathbb{Z}$. To see this, let $\varphi(r)$ be an isomorphism sending $\varphi : \mathbb{Z}[i]/2\mathbb{Z}[i] \to \mathbb{Z}/4\mathbb{Z}$. Then $\varphi(\overline{2r}) = \varphi(\overline{0}) = 0 \bmod 4$. However, $\varphi(\overline{2r}) = \varphi(\overline{r}) + \varphi(\overline{r})$. Since φ is bijective, $\varphi(\overline{r})$ maps to a unique $s \in \mathbb{Z}/4\mathbb{Z}$, and the entirety of $\mathbb{Z}/4\mathbb{Z}$ is mapped.

We then have that $2s = 0 \bmod 4$ $\forall s \in \mathbb{Z}/4\mathbb{Z}$, which is not true (take $s = 1$) $\lightning$

QUESTION 2

Part (1): Let $\mathbb{Q}[\sqrt{p}] := \{a + b\sqrt{p} : a, b \in \mathbb{Q}\}$, with p prime. Clearly $\mathbb{Q}[\sqrt{p}] \subseteq \mathbb{R}$. The remaining conditions are:

$\mathbb{0}, \mathbb{1}$ in set Let $a = 1, b = 0$. Then $1 \in \mathbb{Q}[\sqrt{p}]$. Similarly, letting $a, b = 0$, we see that $0 \in \mathbb{Q}[\sqrt{p}]$.

Closed under + Let $x, y \in \mathbb{Q}[\sqrt{p}]$ with $x = a + b\sqrt{p}$ and $y = c + d\sqrt{p}$. Then $x + y = (a + c) + (b + d)\sqrt{p}$. Since $\mathbb{Q}$ is a ring, $a + c, b + d \in \mathbb{Q}$, so $x + y \in \mathbb{Q}[\sqrt{p}]$.

Closed under × Using the definitions from above, $xy = (a + b\sqrt{p})(c + d\sqrt{p}) = ac + bdp + (bc + ad)\sqrt{p}$, so $xy \in \mathbb{Q}[\sqrt{p}]$.

Additive inverse For $x = a + b\sqrt{p}$, define $-x := -a - b\sqrt{p}$. Then $x + (-x) = a - a + (b - b)\sqrt{p} = 0$

$\mathbb{Q}[\sqrt{p}]$ is also a field. Let $x = a + b\sqrt{p}$, and define $x^{-1} := \frac{1}{a+b\sqrt{p}}$. Clearly, $xx^{-1} = 1$, but we need to show that x^{-1} can be written as $r + s\sqrt{p}$ for some $r, s \in \mathbb{Q}$:

$$\frac{1}{a + b\sqrt{p}} = \frac{a - b\sqrt{p}}{a^2 - b^2 p} = \frac{a}{a^2 - b^2 p} + \frac{b^2}{b^2 p - a^2}\sqrt{p} = r + s\sqrt{p}$$

since $\mathbb{Q}$ is closed under multiplication and addition.

Part (b): We'll use the first isomorphism theorem. Consider

$$\varphi : \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{p}] : q_n x^n + ... + q_1 x + q_0 \mapsto q_n \sqrt{p}^n + ... + q_1\sqrt{p} + q_0$$

It is not immediately obvious that $q_n\sqrt{p}^n + ... + q_0 \in \mathbb{Q}[\sqrt{p}]$. WLOG, assume that n is even. We can regroup as follows:

$$(q_n\sqrt{p}^n + q_{n-1}\sqrt{p}\sqrt{p}^{n-2}) + ... + (q_2\sqrt{p}^2 + q_1\sqrt{p}) + q_0$$

$\sqrt{p}^{i-2} = p^{\frac{i-2}{2}}$, where $\frac{i-2}{2}$ is a positive integer, as $i - 2$ is even.

For any $q_i\sqrt{p}^i + q_{i-1}\sqrt{p}\sqrt{p}^{i-2}$, we have that $\sqrt{p}^{i-2}$ is an integer. $\sqrt{p}^i$ is also an integer.

$\implies q_i\sqrt{p}^i + q_{i-1}\sqrt{p}\sqrt{p}^{i-2} \in \mathbb{Q}[\sqrt{p}]$, and since $\mathbb{Q}[\sqrt{p}]$ is closed under addition, the whole sum $\in \mathbb{Q}[\sqrt{p}]$.

If we had let n be odd, write $q_n\sqrt{p}^n = q_n\sqrt{p}\sqrt{p}^{n-1}$, where $\sqrt{p}^{n-1}$ is an integer. One groups from the q_{n-1} term onward, and the proof is identical.

To show that φ is surjective, take any $a + b\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$. Then, $a + bx$ maps to $a + b\sqrt{p}$.

Lastly, we need that $I = \ker(\varphi) = \langle x^2 - p\rangle$. One sees that $x^2 - p \mapsto \sqrt{p}^2 - p = 0$, so $x^2 - p \in I$. Moreover, since I must be an ideal of $\mathbb{Q}[x]$, $(x^2 - p)q(x) \in I$ for any $q(x) \in \mathbb{Q}[x]$, so $\langle x^2 - p\rangle \subseteq I$.

Since $\mathbb{Q}$ is a field, any ideal of $\mathbb{Q}[x]$ is principal, so $I = \langle f\rangle$ for some unique f. We have now that $x^2 - p \in \langle f\rangle$, so $f | x^2 - p$. Note that $x^2 - p$ is irreducible over $\mathbb{Q}[x]$ (see that the root $\sqrt{p} \notin \mathbb{Q}$), so $f \sim 1$ or $f \sim x^2 - p$. If $f \sim 1$, then $\langle f\rangle = \mathbb{Q}[x]$, which is clearly not the kernel.

$\implies f \sim x^2 - p \implies I = \langle f \rangle = \langle x^2 - p \rangle$. By the first isomorphism theorem, we have that $\mathbb{Q}[\sqrt{p}] \cong \mathbb{Q}[x]/\langle x^2 - p \rangle$

There is a ring isomorphism mapping $\mathbb{Q}[\sqrt{p}] \mapsto \mathbb{Q}[x]/\langle x^2 - p \rangle$ □

QUESTION 3

Part (1): We want a finite field with exactly $27 = 3^3$ elements. This is $\mathbb{F}_3/\langle f \rangle$, where $\deg(f) = 3$ is an irreducible polynomial in $\mathbb{F}_3$. One can take $f(x) = x^3 - x + 1$. We check that this is irreducible by seeing it has no roots in $\mathbb{F}_3$:

$$f(0) = 1 \quad f(1) = 1 \quad f(2) = 7 \equiv_3 1$$

Thus, $\mathbb{F}_3/\langle x^3 - x + 1 \rangle$ is a field with 27 elements.

Part (2): Suppose $t^2 + 1$ were irreducible in the field defined above. Then it would have a root, and so $\overline{t^2 + 1} = \overline{0} \implies \overline{t^2} = \overline{-1} = \overline{2}$. Since all elements of $\mathbb{F}_3/\langle x^3 - x + 1 \rangle$ are defined for a *unique* polynomial of degree less than $\deg(f) = 3$, write $t := ax^2 + bx + c$ and consider:

$$t^2 = (ax^2 + bx + c)^2 : a, b \in \mathbb{F}_3 \implies \overline{a^2x^4 + 2abx^3 + (b^2 + 2ac)x^2 + 2bcx + c^2} = \overline{2}$$

Since $\overline{x^3 - x + 1} = \overline{0}$, we have $\overline{x^3} = \overline{x - 1}$. Furthermore, $\overline{x^4} = \overline{x \cdot x^3} = \overline{x(x-1)} = \overline{x^2 - x}$. We then have

$$\star \quad (a^2 + b^2 + 2ac)x^2 + (2ab + 2bc - a^2)x + (c^2 - 2ab) = 2$$

Our requirements then are that $c^2 = 2ab + 2$ (the constant term), $2ab + 2bc - a^2 = 0$ (the x term), and $a^2 + b^2 + 2ac = 0$ (the x^2 term). In $\mathbb{F}_3$, c could be 0, 1 or 2.

If $c = 1$, then $1 = 2ab + 2 \implies -1 = 2ab \implies 2 = 2ab \implies ab = 1$. This happens only when $a = b = 1$ or $a = b = 2$.

When $a = b = 1$, we plug in to find $1 + 1 + 2 = 4 = 1 \neq 0$ for the x^2 term. When $a = b = 2$, we get $8 + 4 - 4 = 2 \neq 0$ for the x term, so both lead to contradictions, and $c \neq 1$.

Suppose now that $c = 0$. Then $0 = 2ab + 2 \implies -2 = 2ab \implies ab = -1 \implies ab = 2$. This happens only if $a = 1$, $b = 2$, or vise-versa.

When $a = 1, b = 2$, we get $1 + 4 = 2 \neq 0$ for the x^2 term. When $a = 2$, $b = 1$, we get $4 + 1 = 2 \neq 0$ again. Both lead to contradictions, so $c \neq 0$.

Finally, take $c = 2$. Then $c^2 = 4 = 1 = 2ab + 2$. As above, we find that $a = b = 1$ or $a = b = 2$. When $a = b = 1$, we one finds that $2 + 4 - 1 = 5 = 2 \neq 0$ for the x

term. When $a = b = 2$, then $4 + 4 + 8 = 16 = 1 \neq 0$ for the x^2 term. Both lead to contradictions, so $c \neq 2$.

$\implies$ No polynomial t exists s.t. $\overline{t^2 + 1} = \overline{0}$, and we are done.