Homework 5

Thursday, May 3, 2018 6:24 PM

1\. (a) Prove that $\sqrt{-10}$ is irreducible in $\mathbb{Z}[\sqrt{-10}] = \{a+\sqrt{-10}\,b \mid a,b \in \mathbb{Z}\}$.

(Hint. • You do not need to show $\mathbb{Z}[\sqrt{-10}]$ is a ring.

• $\sqrt{-10} = (a+\sqrt{-10}\,b)(c+\sqrt{-10}\,d)$ implies

$10 = (a^2+10b^2)(c^2+10d^2)$. Deduce

$a^2+10b^2 \in \{1,2,5,10\}$. Notice that, if $b \neq 0$, then

$a^2+10b^2 \geq 10$.)

(b) Show that $2 \times 5 \in \langle \sqrt{-10} \rangle$ and $2 \notin \langle \sqrt{-10} \rangle$ and $5 \notin \langle \sqrt{-10} \rangle$.

(c) Prove that $\mathbb{Z}[\sqrt{-10}]$ is not a PID.

(Hint. If it is a PID, then what can you say about $\langle \sqrt{-10} \rangle$?)

2\. We are told that $p(x) = x^4 - 2x^3 + 2x^2 - 2x + 2$ is irreducible in $\mathbb{Q}[x]$ and $\alpha \in \mathbb{C}$ is a zero of $p(x)$. Let

$$\phi_\alpha : \mathbb{Q}[x] \longrightarrow \mathbb{C}, \quad \phi_\alpha(f(x)) := f(\alpha).$$

We know that ϕ_α is a ring homomorphism.

(a) Prove that $\ker \phi_\alpha = \langle p(x) \rangle$.

(b) Prove that $\mathrm{Im}\, \phi_\alpha = \{c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 \mid c_0, c_1, c_2, c_3 \in \mathbb{Q}\}$.

Homework 5

Friday, May 4, 2018 10:56 AM

(c) Prove that $\mathbb{Q}[x]/_{\langle p(x)\rangle} \simeq \{c_0+c_1\alpha+c_2\alpha^2+c_3\alpha^3 \mid c_0, c_1, c_2, c_3 \in \mathbb{Q}\}$

(d) Prove that $\{c_0+c_1\alpha+c_2\alpha^2+c_3\alpha^3 \mid c_0, c_1, c_2, c_3 \in \mathbb{Q}\}$ is a field.

3. We are told that $R=\left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{Z} \right\}$ is a unital commutative ring. Let $\phi: R \to \mathbb{Z}$, $\phi\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right) = a-b$.

(a) Prove that ϕ is a ring homomorphism.

(b) Find $\ker \phi$.

(c) Prove that $R/_{\ker\phi} \simeq \mathbb{Z}$.

(d) Is $\ker \phi$ a prime ideal?

(e) Is $\ker \phi$ a maximal ideal?

4. (a) Show that $x^2-5=0$ has no zero in $\mathbb{Q}[\sqrt{2}]$.

(b) Prove that $\mathbb{Q}[\sqrt{2}] \not\simeq \mathbb{Q}[\sqrt{5}]$.

5. (a) Suppose p is an odd prime, and there is $a \in \mathbb{Z}_p$ such that $a^2=-1$ in $\mathbb{Z}_p$. Prove that the multiplicative order of a is 4.

Homework 5

Thursday, May 3, 2018 6:11 PM

(that means $a^4 = 1$ and $a^m \neq 1$ for $0 < m < 4$.)

(b) Use part (a) and Lagrange's theorem to deduce:

if p is a prime and $p \equiv 3 \pmod 4$, then there is no $a \in \mathbb{Z}_p$ such that $a^2 = -1$.

(c) Suppose p is a prime and $p \equiv 3 \pmod 4$. Prove that p is irreducible in $\mathbb{Z}[i]$.

(<u>Hint</u>. Suppose $p = (a+bi)(c+di)$. Then deduce a^2+b^2 is either 1, p, or p^2. If $a^2+b^2=1$, show $a+ib$ is a unit in $\mathbb{Z}[i]$; if $a^2+b^2=p^2$, show $c+id$ is a unit in $\mathbb{Z}[i]$; and use part (b) to show a^2+b^2 cannot be p.)

(d) Use part (c) to show $\mathbb{Z}[i]/\langle p \rangle$ is a field if p is a prime and $p \equiv 3 \pmod 4$.