Homework 6

Thursday, May 10, 2018 8:53 AM

1. (a) Suppose p is a prime number. Prove that $x^p - x + 1$ has no zero in $\mathbb{Z}_p$.

   (b) Prove that $x^3 - x + 1$ is irreducible in $\mathbb{Z}_3[x]$.

(Remark. Using Galois theory one can show that $x^p - x + 1$ is irreducible in $\mathbb{Z}_p[x]$ for any prime p.)

2. (a) Prove that $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$.

   (b) Let $\phi_{\sqrt[3]{2}} : \mathbb{Q}[x] \longrightarrow \mathbb{R}$, $\phi_{\sqrt[3]{2}}(f(x)) = f(\sqrt[3]{2})$ be the evaluation at $\sqrt[3]{2}$. We know that $\phi_{\sqrt[3]{2}}$ is a ring homomorphism.

   (b-1) Prove that $\ker \phi_{\sqrt[3]{2}} = \langle x^3 - 2 \rangle$.

   (b-2) Prove that $\operatorname{Im} \phi_{\sqrt[3]{2}} = \{a_0 + \sqrt[3]{2}\, a_1 + (\sqrt[3]{2})^2 a_2 \mid a_0, a_1, a_2 \in \mathbb{Q}\}$

   (b-3) Let $\mathbb{Q}[\sqrt[3]{2}] := \{a_0 + \sqrt[3]{2}\, a_1 + (\sqrt[3]{2})^2 a_2 \mid a_0, a_1, a_2 \in \mathbb{Q}\}$.

   Prove that $\mathbb{Q}[x]/\langle x^3 - 2 \rangle \simeq \mathbb{Q}[\sqrt[3]{2}]$.

   (b-4) Prove that $\mathbb{Q}[\sqrt[3]{2}]$ is a field.

3. (a) Prove that $\sqrt{-21}$ is irreducible in $\mathbb{Z}[\sqrt{-21}]$.

   (b) Prove that $\langle \sqrt{-21} \rangle$ is not a prime ideal of $\mathbb{Z}[\sqrt{-21}]$.

   (c) Prove that $\mathbb{Z}[\sqrt{-21}]$ is not a PID.

Homework 6

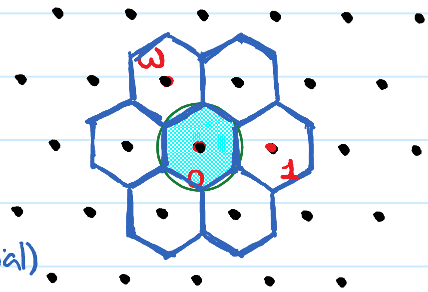
Thursday, May 10, 2018 9:15 AM

4. Let $\omega := \frac{-1+\sqrt{-3}}{2}$. Notice that $\omega^2+\omega+1=0$; and so $\omega+\overline{\omega}=-1$ and $\omega\overline{\omega}=1$ where $\overline{\omega}$ is the complex conjugate of ω. Let $\mathbb{Z}[\omega] := \{a+b\omega \mid a,b\in\mathbb{Z}\}$. We know that $\mathbb{Z}[\omega]$ is a subring of $\mathbb{C}$. Let $\mathbb{Q}[\omega] := \{a+b\omega \mid a,b\in\mathbb{Q}\}$.

(a) Prove that $\mathbb{Q}[x]/\langle x^2+x+1\rangle \simeq \mathbb{Q}[\omega]$ and $\mathbb{Q}[\omega]$ is a field.

(b) Prove that for any $z\in\mathbb{Q}[\omega]$ there is $u\in\mathbb{Z}[\omega]$ such that $|z-u|\le \sqrt{3}/3$.

(Hint. Use the following figure.)
(Only in this part it is OK to be pictorial)



(c) Prove that for any $a\in\mathbb{Z}[\omega]$ and $b\in\mathbb{Z}[\omega]\setminus\{0\}$, there are $q,r\in\mathbb{Z}[\omega]$ such that

$$a=bq+r \quad \text{and} \quad |r|\le \frac{\sqrt{3}}{3}|b|.$$

(Hint. Consider $\frac{a}{b}\in\mathbb{Q}[\omega]$; use part (b) to find $q\in\mathbb{Z}[\omega]$. $\left|\frac{a}{b}-q\right|\le\frac{\sqrt{3}}{3}$. Let $r:=b\left(\frac{a}{b}-q\right)$.)

(d) Prove that $\mathbb{Z}[\omega]$ is a Euclidean domain. (Hint. Let $N(a):=|a|^2$.)

(e) Prove that $\mathbb{Z}[\omega]$ is a PID.

Homework 6

Thursday, May 10, 2018 9:48 AM

5. Suppose $a, b \in \mathbb{Z}$ and $a^2+ab+b^2 = p$ is a prime number > 3.

(a) Prove that $a - b\omega$ is irreducible in $\mathbb{Z}[\omega]$.

(Hint. Consider $|a-b\omega|^2$.)

(b) Prove that $\exists\, \alpha \in \mathbb{Z}_p$ such that

(b-1) $\alpha^2+\alpha+1=0$ in $\mathbb{Z}_p$,

(b-2) $a-b\alpha=0$ in $\mathbb{Z}_p$.

(c) Let $\phi: \mathbb{Z}[\omega] \longrightarrow \mathbb{Z}_p$, $\phi(c+d\omega) := c+d\alpha$

where α is given in part (b). Prove that ϕ is a ring homomorphism.

(d) Prove that $\ker \phi = \langle a-b\omega \rangle$.

(Hint. Use problems 4.e and 5.a.)

(e) Prove that $\mathbb{Z}[\omega]/\langle a-b\omega\rangle \simeq \mathbb{Z}_p$.