Solutions 2010-05-31

1. Let $f(X) \in \mathbb{Z}_1[X]$ and $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ such that $f(X) = \prod_{i=1}^{n} (X - \alpha_i)$. Then

$$\{\alpha_1, \dots, \alpha_n\} \subset \overline{\mathbb{Z}}(\mathbb{C}) = \overline{\mathbb{Z}},$$

because $\overline{\mathbb{Z}} = \overline{\mathbb{Z}}(\mathbb{C})$ is integrally closed in $\mathbb{C}$.

2. $\zeta^s = \zeta^{s-1} \Leftrightarrow s \equiv s-1 \Leftrightarrow 1 \equiv 0 \pmod p$ ↯

$\zeta^s = \zeta^{-s} \Leftrightarrow s \equiv -s \Leftrightarrow 2s \equiv 0 \Leftrightarrow s \equiv 0 \Leftrightarrow s-1 \equiv p-1 \pmod p$

$\Leftrightarrow \zeta^{p-1} = \zeta^{s-1}$ ↯

$\zeta^{s-1} = \zeta^{1-s} \Leftrightarrow s-1 \equiv 1-s \Leftrightarrow 2(1-s) \equiv 0 \Leftrightarrow 1-s \equiv 0 \Leftrightarrow -s \equiv p-1 \pmod p$

$\Leftrightarrow \zeta^{p-1} = \zeta^{-s}$ ↯

$\zeta^{-s} = \zeta^{1-s} \Leftrightarrow -s \equiv 1-s \Leftrightarrow 0 \equiv 1 \pmod p$ ↯

Moreover, $\zeta^s = \zeta^{1-s} \Leftrightarrow \zeta^{s-1} = \zeta^{-s}$.

If $\zeta^s = \zeta^{1-s}$, then $\left|\{\zeta, \zeta^{s-1}, \zeta^{-s}, \zeta^{1-s}\}\right| = \left|\{\zeta, \zeta^{s-1}\}\right| \leq 2$.

If $\zeta^s \neq \zeta^{1-s}$, then $\left|\{\zeta, \zeta^{s-1}, \zeta^{-s}, \zeta^{1-s}\}\right| = 4$, due to the above reasoning.

3. (a) A <u>fractional $\mathbb{Z}[\zeta]$-ideal</u> is a $\mathbb{Z}[\zeta]$-submodule B of $\mathbb{Q}[\zeta]$ of the form

$$B = cA, \text{ where } c \in \mathbb{Q}[\zeta] \setminus \{0\} \text{ and } (0) \neq A < \mathbb{Z}[\zeta].$$

(b) A <u>principal fractional $\mathbb{Z}[\zeta]$-ideal</u> is a $\mathbb{Z}[\zeta]$-submodule B of $\mathbb{Q}[\zeta]$ of the form

$$B = c\,\mathbb{Z}[\zeta] =: (c), \quad \text{where } c \in \mathbb{Q}[\zeta] \setminus \{0\}.$$

(c) The ideal class group of $\mathbb{Z}[\zeta]$ is the quotient group $\mathcal{H} = \mathcal{F}/\mathcal{P}$ of the group $\mathcal{F}$ of all fractional $\mathbb{Z}[\zeta]$-ideals by the normal subgroup $\mathcal{P}$ of all principal fractional $\mathbb{Z}[\zeta]$-ideals. The ideal class number $h = |\mathcal{H}/\mathcal{P}|$ of $\mathbb{Z}[\zeta]$ is finite. A prime number p is called <u>regular</u> if $p \nmid h$.

(d) Let p be regular, and $A \in \mathcal{F}$ such that $A^p \in \mathcal{P}$. Then $\bar{A}^p = \overline{A^p} = \mathcal{P}$ implies $\mathrm{ord}(\bar{A}) \in \{1, p\}$. Since $\mathrm{ord}(\bar{A}) \mid h$ and $p \nmid h$, it follows that $\mathrm{ord}(\bar{A}) = 1$, which means $\bar{A} = \mathcal{P}$, or equivalently $A \in \mathcal{P}$.

4. The identity $p = \varepsilon(1-\zeta)^{p-1}$ holds in $\mathbb{Z}[\zeta]$ for some $\varepsilon \in \mathbb{Z}[\zeta]^\times$. The principal ideal $(1-\zeta) < \mathbb{Z}[\zeta]$ is prime, because $\mathbb{Z}[\zeta]/(1-\zeta) \cong \mathbb{Z}/p\mathbb{Z}$ is a field. Therefor $p\,\mathbb{Z}[\zeta]$ has the unique prime factorization $p\,\mathbb{Z}[\zeta] = (1-\zeta)^{p-1}$.

5. (a) $\mathbb{Z}[\sqrt{-3}]$ is a subring of the field $\mathbb{C}$, hence an id.

(b) $\sqrt{-3}$ is a root of $X^2 + 3 \in \mathbb{Z}_1[X] \Rightarrow \sqrt{-3}$ is integral over $\mathbb{Z}$

$\Rightarrow \mathbb{Z}[\sqrt{-3}]$ is a f.g. $\mathbb{Z}$-module

$\mathbb{Z}$ is a noetherian ring

$\Rightarrow \mathbb{Z}[\sqrt{-3}]$ is a ...

... noetherian $\mathbb{Z}$-module $\Rightarrow \mathbb{Z}[\sqrt{-3}]$ is a noetherian ring

$\overset{(a)}{\Rightarrow} \mathbb{Z}[\sqrt{-3}]$ <u>is a noetherian domain</u>.

(c) $\mathbb{Q}[\sqrt{-3}] \cong \mathbb{Q}[X]/(\operatorname{impol}_{\mathbb{Q}}(\sqrt{-3})) = \mathbb{Q}[X]/(X^2+3)$ is a field, containing $\mathbb{Z}[\sqrt{-3}]$. Hence $\operatorname{frac}(\mathbb{Z}[\sqrt{-3}]) \subset \mathbb{Q}[\sqrt{-3}]$. Conversely, every $\alpha \in \mathbb{Q}[\sqrt{-3}]$ is of the form $\alpha = \frac{\beta}{b}$ for some $\beta \in \mathbb{Z}[\sqrt{-3}]$ and $b \in \mathbb{Z}\setminus\{0\}$. Hence $\mathbb{Q}[\sqrt{-3}] \subset \operatorname{frac}(\mathbb{Z}[\sqrt{-3}])$.

(d) Since $(1, \sqrt{-3})$ is a $\mathbb{Q}$-basis of $\mathbb{Q}[\sqrt{-3}]$ and a $\mathbb{Z}$-basis of $\mathbb{Z}[\sqrt{-3}]$, the element

$\alpha = \frac{1+\sqrt{-3}}{2}$ belongs to $\mathbb{Q}[\sqrt{-3}] \setminus \mathbb{Z}[\sqrt{-3}]$. It satisfies $\alpha^2 - \alpha + 1 = 0$.

Hence $\alpha \in \mathbb{Q}[\sqrt{-3}]$ is integral over $\mathbb{Z}[\sqrt{-3}]$, but $\alpha \notin \mathbb{Z}[\sqrt{-3}]$. Accordingly, the id $\mathbb{Z}[\sqrt{-3}]$ is not integrally closed in its field of fractions $\mathbb{Q}[\sqrt{-3}]$, i.e. $\mathbb{Z}[\sqrt{-3}]$ is not an integrally closed domain.

(e) $\mathbb{Z}[\sqrt{-3}]$ is not a DD, because it is not integrally closed in its field of fractions.

6. Let $(\alpha_1, \dots, \alpha_n)$ be any K-basis of L. Set $O = \bar{R}(L)$. We know that $KO = L$. Hence every α_i can be written $\alpha_i = \frac{\beta_i}{b_i}$ for suitable $\beta_i \in O$ and $b_i \in R\setminus\{0\}$. Now

$\left(\frac{\beta_1}{b_1}, \dots, \frac{\beta_n}{b_n}\right)$ is a K-basis of L

$\Rightarrow$ $(\beta_1, \dots, \beta_n)$ is a K-basis of L, and all β_i are integral over R.

7. Set $O = \bar{\mathbb{Z}}(L)$. We know that O is a f.g. and torsion-free $\mathbb{Z}$-module. Hence O has a finite $\mathbb{Z}$-basis $(\beta_1, \dots, \beta_n)$. Since $\mathbb{Q}O = L$, $(\beta_1, \dots, \beta_n)$ is also a $\mathbb{Q}$-basis of L.

Now let $\alpha \in L \cap \mathbb{Z} = O$. Then $\mu_\alpha(\beta_j) = \alpha\beta_j \in O \Rightarrow \mu_\alpha(\beta_j) = \sum_{i=1}^{n} m_{ij}\beta_i$

where all $m_{ij} \in \mathbb{Z}$. So $M = (m_{ij}) \in \mathbb{Z}^{n\times n}$. Accordingly $N(\alpha) = \det(\mu_\alpha) = \det(M) \in \mathbb{Z}$.

8. Let $(x,y,z) \in \mathbb{Z}^3$ be a mcl, i.e. $x^p + y^p = z^p$, $xyz \neq 0$, $\gcd(x,y,z) = 1$, and $p \nmid xyz$.

De Moivre's identity yields

$$\prod_{i=0}^{p-1} (x + \zeta^i y) = x^p + y^p = z^p .$$

Fermat's Little Theorem implies that

$$x + y \equiv x^p + y^p = z^p \equiv z \not\equiv 0 \pmod{p}$$

Moreover, $\gcd(x,y,z) = 1$ implies $\gcd(x,y) = 1$. Since $p \nmid (x+y)$ and $\gcd(x,y) = 1$, a proposition of Kummer asserts that the $\mathbb{Z}[\zeta]$-ideals $(x+y), \dots, (x+\zeta^i y)$ are pairwise relatively prime. For each $0 \leq i \leq p-1$, let

$$(x + \zeta^i y) = \prod_{j=1}^{\ell_i} P_{ij}^{n_{ij}}$$

be the unique prime factorization of $(x+\zeta^i y)$. Moreover, let

$$(z) = \prod_{k=1}^{\ell} Q_k^{m_k}$$

be the unique prime factorization of (z). Then the $\mathbb{Z}[\zeta]$-ideal

$$\prod_{i=0}^{p-1} (x + \zeta^i y) = (z)^p$$

has prime factorization

$$\prod_{i=0}^{p-1} \prod_{j=1}^{\ell_i} P_{ij}^{n_{ij}} = \prod_{k=1}^{\ell} Q_k^{m_k p} .$$

Uniqueness of prime factorization of non-zero $\mathbb{Z}[\zeta]$-ideals implies that all $n_{ij} = m_{ij} p$, for $m_{ij} \in \mathbb{N}_0$.

Setting $I_i = \prod_{j=1}^{\ell_i} P_{ij}^{m_{ij}} < \mathbb{Z}[\zeta]$, we find that $I_i^p = (x + \zeta^i y)$ holds for all $0 \leq i \leq p-1$.