HW 10 Solutions

23rd April 2019 at 1:02pm

Problem 1.

Prove that $\mathbb{Z}[\sqrt{-2}]$ is a PID.

Solution.

It suffices to show that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain with the size function

$$\sigma : \mathbb{Z}[\sqrt{-2}] \to \mathbb{Z}[\sqrt{-2}] : a + b\sqrt{-2} \mapsto a^2 + 2b^2.$$

Let $x, y \in \mathbb{Z}[\sqrt{-2}]$ with y nonzero. Then

$$x/y = a + b\sqrt{-2} \in \mathbb{Q}[\sqrt{-2}]$$

for some $a, b \in \mathbb{Q}$. Choose $c, d \in \mathbb{Z}$ such that $|a - c| \leq 1/2, |b - d| \leq 1/2$. Then

$$\sigma\left(\frac{x}{y} - (c + d\sqrt{-2})\right) = \sigma\left((a - c) + (b - d)\sqrt{-2}\right) \leq (1/2)^2 + 2\,(1/2)^2 = 3/4.$$

Since σ is multiplicative,

$$\sigma(x - (c + d\sqrt{-2})y) \leq (3/4) \cdot \sigma(y) < \sigma(y).$$

Therefore $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain with the size function σ.

▨

Problem 2.

Decide whether or not $x^4 + 6x^3 + 9x + 3$ is irreducible in $\mathbb{Q}[x]$.

Solution.

It is irreducible over $\mathbb{Q}$ by applying Eisenstein's criterion at the prime $p = 3$.

▨

Problem 3.

Factor the integral polynomial $x^5 + 2x^4 + 3x^3 + 3x + 5$ in $\mathbb{F}_2[x], \mathbb{F}_3[x], \mathbb{Q}[x]$.

Solution.

Over $\mathbb{F}_2$, the polynomial $x^5 + 2x^4 + 3x^3 + 3x + 5$ factors as $(x + 1)(x^4 + x^3 + 1)$. The quartic has no roots and no quadratic factors over $\mathbb{F}_2$ and so is irreducible.

Over $\mathbb{F}_2$, the polynomial $x^5 + 2x^4 + 3x^3 + 3x + 5$ factors as $(x+1)^2(x^3 + 2x + 2)$. The cubic has no roots and so is irreducible.

Over $\mathbb{Q}$, the polynomial $x^5 + 2x^4 + 3x^3 + 3x + 5$ factors as $(x+1)(x^4 + x^3 + 2x^2 - 2x + 5)$. The quartic is irreducible over $\mathbb{Q}$ for the following reason: From our work above, we know this quartic remains irreducible over $\mathbb{F}_2$, so it must be irreducible over $\mathbb{Z}$ to begin with. Therefore it is also irreducible over $\mathbb{Q}$.

Note.

Recall that Gauss's lemma states that a primitive polynomial $f \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Z}$ iff it is irreducible over $\mathbb{Q}$. The hard part of this lemma is the converse. Since we only use the forward direction, we don't need to cite the lemma.

Problem 4.

Prove that a prime number p can be written as $p = m^2 + 2n^2$ with $m, n \in \mathbb{Z}$ if and only if $x^2 + 2$ has a root in $\mathbb{F}_p$.

Solution.

If $p = m^2 + 2n^2$, then taking mod p, we have $m^2 + 2n^2 \equiv 0 \pmod{p}$. If $n \not\equiv 0 \pmod{p}$, then $(m/n)^2 + 2 \equiv 0 \pmod{p}$. Otherwise $n \equiv 0 \pmod{p}$ and so $m^2 \equiv 0 \pmod{p}$ and so $m \equiv 0 \pmod{p}$. Therefore, m, n are multiples of p, so $m^2 + 2n^2$ has a factor of p^2 and is equal to p, a contradiction.

Conversely, suppose that $x^2 + 2 \equiv 0 \pmod{p}$ has solutions. Then $\mathbb{F}_p[x]/(x^2+2)$ is not an integral domain. Since

$$\frac{\mathbb{F}_p[x]}{(x^2+2)} \cong \frac{\mathbb{Z}[x]}{(p, x^2+2)} \cong \frac{\mathbb{Z}[\sqrt{-2}]}{(p)},$$

p is not a prime in $\mathbb{Z}[-\sqrt{-2}]$. Therefore,

$$p = (a + b\sqrt{-2})(m + n\sqrt{-2})$$

for some nonunits $a + b\sqrt{-2}, m + n\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$.

There are now two ways to argue.

Argument 1. Since $p \in \mathbb{Z}$, these two factors must be conjugate, so we conclude that

$$p = (a + b\sqrt{-2})(a - b\sqrt{-2}) = a^2 + 2b^2.$$

Argument 2. Taking the norm of both sides, we get

$$p^2 = (a^2 + 2b^2)(m^2 + 2n^2).$$

Since $a+b\sqrt{-2}, m+n\sqrt{-2}$ are nonunits in $\mathbb{Z}[\sqrt{-2}]$, their norms are not equal to 1. Therefore,

$$a^2+2b^2=m^2+2n^2=p.$$

▧

add comment