

5.1.4 Show that, under congruence modulo $x^3 + 2x + 1$ in $\mathbb{Z}_3[x]$, there are exactly 27 distinct congruence classes.

By Corollary 5.5 every congruence class is of the form $[a_2x^2 + a_1x + a_0]$ with $a_0, a_1, a_2 \in \mathbb{Z}_3$ and all such classes are distinct. Since there are three possibilities for each of a_0, a_1 and a_2 , there are in all $3^3 = 27$ congruence classes. \blacklozenge

5.1.8 Prove or disprove: If $p(x)$ is relatively prime to $k(x)$ and $f(x)k(x) \equiv g(x)k(x) \pmod{p(x)}$, then $f(x) \equiv g(x) \pmod{p(x)}$.

We will prove the assertion is true (assuming that we are speaking about polynomials over a field). Let $p(x), k(x), f(x), g(x) \in F[x]$ (for some field F) with $p(x) \neq 0$. Suppose that $p(x)$ is relatively prime to $k(x)$ and $f(x)k(x) \equiv g(x)k(x) \pmod{p(x)}$. Then by definition of congruence $f(x)k(x) - g(x)k(x)$ is divisible by $p(x)$. That is, we have $p(x) \mid (f(x) - g(x))k(x)$. Since $p(x)$ and $k(x)$ are relatively prime, Theorem 4.7 (p. 93) applies and we have $p(x) \mid f(x) - g(x)$. Hence, $f(x) \equiv g(x) \pmod{p(x)}$ as required. \blacklozenge

5.2.6 Each element of the given congruence-class ring can be written in the form $[ax + b]$ (Why?). Determine the rules for addition and multiplication of congruence classes. (In other words, if the product $[ax + b][cx + d]$ is the class $[rx + s]$, describe how to find r and s from a, b, c, d , and similarly for addition.): $\mathbb{Q}[x]/(x^2 - 2)$.

Since we are dealing with congruence classes modulo a polynomial of degree two $x^2 - 2$, all nonzero remainders will be of degree one or less. So each congruence class is of the form $[ax + b]$ for some $a, b \in \mathbb{Q}$. Let $a, b, c, d \in \mathbb{Q}$ be given. Then

$$[ax + b] + [cx + d] = [(a + c)x + (b + d)].$$

Note that $x^2 = 2 + (x^2 - 2)$, hence, $[x^2] = [2]$ and thus

$$[ax + b][cx + d] = [acx^2 + (ad + bc)x + bd] = [(ad + bc)x + (2ac + bd)].$$

So $[ax + b][cx + d] = [rx + s]$ with $r = ad + bc$ and $s = 2ac + bd$. \blacklozenge

5.2.14b Explain why $[f(x)]$ is a unit in $F[x]/(p(x))$ and find its inverse: $[f(x)] = [x^2 + x + 1] \in \mathbb{Z}_3[x]/(x^2 + 1)$.

Let $f(x) = x^2 + x + 1 \in \mathbb{Z}_3[x]$. We first check that $p(x) = x^2 + 1$ is irreducible in $\mathbb{Z}_3[x]$ by showing that it has no roots in \mathbb{Z}_3 . We have $p(0) = 1 \neq 0$ and $p(1) = p(2) = 2 \neq 0$. So $p(x)$ has no roots and is therefore irreducible. Since $p(x)$ is irreducible and $f(x)$ is not divisible by $p(x)$, then $p(x)$ and $f(x)$ are relatively prime. It follows by Theorem 5.9 that $[f(x)]$ is a unit in $\mathbb{Z}_3[x]/(p(x))$. We apply the Euclidean algorithm to obtain:

$$2x(x^2 + x + 1) + (x + 1)(x^2 + 1) = 1.$$

Hence, $[2x][x^2 + x + 1] = [1]$ and so the inverse of $[f(x)] = [x^2 + x + 1]$ in $\mathbb{Z}_3[x]/(x^2 + 1)$ is $[2x]$. \blacklozenge

5.3.1a Determine whether the given congruence-class ring is a field: $\mathbb{Z}_3[x]/(x^3 + 2x^2 + x + 1)$.

The given congruence-class ring is a field. To show this it suffices to establish that $p(x) = x^3 + 2x^2 + x + 1$ is irreducible in $\mathbb{Z}_3[x]$ by Theorem 5.10. Since $\deg p(x) = 3$, $p(x)$ is irreducible if it has no roots in \mathbb{Z}_3 (see Corollary 4.18). We tabulate the values of the associated polynomial function on \mathbb{Z}_3 as follows:

a	0	1	2
$p(a)$	1	2	1

Hence, $p(x)$ has no roots and is thus irreducible. Therefore, $\mathbb{Z}_3[x]/(x^3 + 2x^2 + x + 1)$ is a field. \blacklozenge

5.3.2b Show that $\mathbb{Q}(\sqrt{2})$ is isomorphic to $\mathbb{Q}[x]/(x^2 - 2)$. [*Hint:* Exercise 6 in Section 5.2 may be helpful.]

Recall that $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a subring of \mathbb{R} with addition and multiplication given by

$$\begin{aligned} (a + b\sqrt{2}) + (c + d\sqrt{2}) &= (a + c) + (b + d)\sqrt{2} \\ (a + b\sqrt{2})(c + d\sqrt{2}) &= (ac + 2bd) + (ad + bc)\sqrt{2} \end{aligned}$$

for $a, b, c, d \in \mathbb{Q}$. We refer to Exercise 5.2.6 for addition and multiplication in $\mathbb{Q}[x]/(x^2 - 2)$. We define a map $\varphi : \mathbb{Q}[x]/(x^2 - 2) \rightarrow \mathbb{Q}(\sqrt{2})$ by $\varphi([ax + b]) = b + a\sqrt{2}$. We will show that φ is an isomorphism. First observe that it is a bijection. We must now show that φ is a homomorphism, that is, that it preserves addition and multiplication. Let $[ax + b], [cx + d] \in \mathbb{Q}[x]/(x^2 - 2)$ be given. Then

$$\begin{aligned} \varphi([ax + b] + [cx + d]) &= \varphi([(a + c)x + (b + d)]) = (b + d) + (a + c)\sqrt{2} = (b + a\sqrt{2}) + (d + c\sqrt{2}) \\ &= \varphi([ax + b]) + \varphi([cx + d]) \quad \text{and} \\ \varphi([ax + b][cx + d]) &= \varphi([(ad + bc)x + (2ac + bd)]) = (2ac + bd) + (ad + bc)\sqrt{2} = (b + a\sqrt{2})(d + c\sqrt{2}) \\ &= \varphi([ax + b])\varphi([cx + d]). \end{aligned}$$

Hence, φ is an isomorphism and, therefore, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}[x]/(x^2 - 2)$ are isomorphic. \blacklozenge