Supplemental Problem Solutions for 3.2

Jim Brown

1. Consider the ring $R = \mathbb{Q}[x]/(x^3 - x + 1)$.

(a) Find a polynomial $h(x)$ of degree less then 3 so that $g(x) = x^5 + 4x^2 + 10$ is congruent to $h(x)$.

The important thing to observe is that in R one has $\overline{x}^3 = \overline{x} - 1$. Therefore, we have that

$$\begin{aligned} g(x) &\equiv x^2(x^3) + 4x^2 + 10(\text{mod}(x^3 - x + 1)) \\ &\equiv x^2(x-1) + 4x^2 + 10(\text{mod}(x^3 - x + 1)) \\ &\equiv x^3 + 3x^2 + 10(\text{mod}(x^3 - x + 1)) \\ &= 3x^2 + x + 9(\text{mod}(x^3 - x + 1)). \end{aligned}$$

So the polynomial we seek is $3x^2 + x + 9$.

(b) Finish the following statement: "$\overline{x^7} =$ ___ in R".

This proceeds just as above, observing that

$$\begin{aligned} \overline{x}^7 &= (\overline{x}^3)^2\overline{x} \\ &= (\overline{x} - 1)^2\overline{x} \\ &= (\overline{x}^2 - 2\overline{x} + 1)\overline{x} \\ &= \overline{x}^3 - 2\overline{x}^2 + \overline{x} \\ &= -2\overline{x}^2 + 2\overline{x} - 1. \end{aligned}$$

(c) Is this ring a field? Justify your answer.

This ring is a field as the polynomial $x^3 - x + 1$ is irreducible. One checks this by showing it has no rational roots. One can use the rational root theorem or apply the solution to the cubic equation we studied in Chapter 2.

2. Recall that the n^{th} roots of unity are the roots of the polynomial $\phi_n(x) = x^n - 1$. Note that $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$.

(a) Show that if we set $\omega = e^{\frac{2\pi i}{n}}$, then the roots of $x^{n-1} + x^{n-2} + \cdots + x + 1$ are given by $\omega, \omega^2, \cdots, \omega^{n-1}$.

Proof: We know that $1, \omega, \omega^2, \cdots, \omega^{n-1}$ are roots of the polynomial $x^n - 1$. Using the factorization above, we see that for $1 \leq j \leq n-1$, we have

$$\begin{aligned} 0 &= (\omega^j)^n - 1 \\ &= (\omega^j - 1)((\omega^j)^{n-1} + \cdots + \omega^j + 1). \end{aligned}$$

Since $\omega^j - 1 \neq 0$ as ω is a primitive n^{th} root of unity, we have that $((\omega^j)^{n-1} + \cdots + \omega^j + 1) = 0$ using that $\mathbb{Q}[x]$ is an integral domain. ■

(b) Let p be a prime. Is the ring $\mathbb{Q}[x]/(x^p - 1)$ a field? Is the ring $\mathbb{Q}[x]/(x^{p-1} + x^{p-2} + \cdots + x + 1)$ a field? Justify your answers!

The ring $\mathbb{Q}[x]/(x^p - 1)$ is not a field as we know that

$$\overline{(x-1)} \cdot \overline{(x^{p-1} + x^{p-2} + \cdots + x + 1)} = \overline{0}$$

in this ring. In other words, there are zero divisors. This shows that the ring cannot be an integral domain. Since all fields are integral domains, it therefore cannot be a field.

The ring $\mathbb{Q}[x]/(x^{p-1} + x^{p-2} + \cdots + x + 1)$ is a field. You were told that $x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible, which gives you that the ring is a field.

(c) Consider the ring $\mathbb{Q}[x]/(x^{p-1} + x^{p-2} + \cdots + x + 1)$. Show that there is an element (not equal to 1) so that when you raise it to the p^{th} power you get 1.

Proof: Note that in this ring one has that the element $\overline{x} \neq 1$ and $(\overline{x})^p + \cdots + \overline{x} + 1 = 0$. Multiply both sides of this equation by $\overline{x} - 1$ to obtain $(\overline{x})^p - 1 = 0$, i.e., $\overline{x}$ is the element we seek. ■

3. Denote the field obtained by adjoining the third root of unity $\omega = e^{\frac{2\pi i}{3}}$ to $\mathbb{Q}$ by $\mathbb{Q}[\omega]$. This field is given by

$$\mathbb{Q}[\omega] = \left\{ a + b\omega + c\omega^2 | a, b, c \in \mathbb{Q} \right\}.$$

(a) Let $a + b\omega + c\omega$ and $d + e\omega + f\omega^2$ be elements in $\mathbb{Q}[\omega]$. Compute their sum and product and write it in a form so that it is clear that it is in $\mathbb{Q}[\omega]$.

The sum is completely straightforward:

$$(a + b\omega + c\omega^2) + (d + e\omega + f\omega^2) = (a + d) + (b + e)\omega + (c + f)\omega^2.$$

To compute the product, one must use that $\omega^3 = 1$.

$$\begin{aligned}(a + b\omega + c\omega^2) \cdot (d + e\omega + f\omega^2) &= ad + (ae + bd)\omega + (af + be + cd)\omega^2 + (bf + ce)\omega^3 + cf\omega^4 \\ &= (ad + bf + ce) + (ae + bd + cf)\omega + (af + be + cd)\omega^2.\end{aligned}$$

(b) Determine a polynomial $f(x)$ so that $\mathbb{Q}[\omega]$ is isomorphic to $\mathbb{Q}[x]/(f(x))$ (remember your $f(x)$ must be such that $\mathbb{Q}[x]/(f(x))$ is actually a field!)

We need a polynomial that has ω as a root and is irreducible. Using the previous problem we see such a polynomial is given by $f(x) = x^2 + x + 1$.

(c) Show that $\mathbb{Q}[\omega] = \mathbb{Q}[\sqrt{3}i]$ by showing containment in each direction.

Proof: Recall that $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. To show that $\mathbb{Q}[\omega] = \mathbb{Q}[\sqrt{3}i]$ we need to show $\omega \in \mathbb{Q}[\sqrt{3}i]$ and $\sqrt{3}i \in \mathbb{Q}[\omega]$. We use repeatedly that since these are fields they are closed under addition, subtraction, multiplication, and division. First, observe that $\sqrt{3}i \in \mathbb{Q}[\omega]$ since $\sqrt{3}i = 2\omega + 1 \in \mathbb{Q}[\omega]$. Similarly, we have that $\omega \in \mathbb{Q}[\sqrt{3}i]$ since $\omega = -\frac{1}{2} + \frac{\sqrt{3}i}{2} \in \mathbb{Q}[\sqrt{3}i]$. ■

4. Consider the ring $(\mathbb{Z}/5\mathbb{Z})[x]/(x^2 - 2)$.

(a) Show this is a field.

Proof: We need only show that $x^2 - 2$ is an irreducible polynomial in $(\mathbb{Z}/5\mathbb{Z})[x]$. To see this, we just check it has no roots. Namely, plug in $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}$ in for x and see that one never gets $\overline{0}$, so there are no roots. ■

(b) List all the elements of this field.

There are 25 elements in this field, they are of the form $ax + b$ with $a, b \in \mathbb{Z}/5\mathbb{Z}$. You should make sure you can list them all out.

(c) Compute $\overline{2x+3} + \overline{4x+1}$ and $\overline{2x+3} \cdot \overline{4x+1}$.

$$\begin{aligned}\overline{2x+3} + \overline{4x+1} &= \overline{6x+4} \\ &= \overline{x+4}\end{aligned}$$

$$\begin{aligned}\overline{2x+3}\cdot\overline{4x+1} &= \overline{8x^2+14x+3}\\ &= \overline{3x^2+4x+3}\\ &= \overline{3\cdot 2+4x+3}\\ &= \overline{4x+4}\end{aligned}$$

(d) Find a polynomial $r(x)$ of degree smaller then 2 so that $\overline{f(x)} = \overline{r(x)}$ where $f(x) = x^7 + 3x^2 + 8$.

As in part (c), we use that $x^2 = 2$ in this ring. So we have

$$\begin{aligned}x^7+3x^2+8 &\equiv x^7+3x^2+3 (\mathrm{mod}\, x^2-2)\\ &\equiv (x^2)^3x+3(2)+3(\mathrm{mod}\, x^2-2)\\ &\equiv 8x+9(\mathrm{mod}\, x^2-2)\\ &\equiv 3x+4(\mathrm{mod}\, x^2-2).\end{aligned}$$

5. Let p be a prime and let $f(x)$ be an irreducible polynomial of degree n. How many elements are there in the field $(\mathbb{Z}/p\mathbb{Z})[x]/(f(x))$?

This ring will have all polynomials of degree less then or equal to $n-1$ with coefficients in $\mathbb{Z}/p\mathbb{Z}$. Let $f(x) = a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be such a polynomial. There are n coefficients and each one can be any of the p elements in $\mathbb{Z}/p\mathbb{Z}$, so there are p^n such polynomials.