

## Solutions to Homework 7

**§3.1 #1** Apply the division algorithm...

$$\begin{aligned} \text{d. } f &= x^6 + \bar{3}x^5 + \bar{4}x^2 - \bar{3}x + \bar{2} \in \mathbb{Z}_7[x] \\ g &= \bar{3}x^2 + \bar{2}x - \bar{3} \\ q &= \bar{5}x^4 + \bar{5}x^2 + \bar{6}x \\ r &= x + \bar{2} \end{aligned}$$

$$\begin{aligned} \text{e. } f &= x^7 + x^6 + x^4 + x + \bar{1} \in \mathbb{Z}_2[x] \\ g &= x^3 + x + \bar{1} \\ q &= x^4 + x^3 + x^2 + x \\ r &= \bar{1} \end{aligned}$$

**§3.1 #8** Let  $F$  be a field. Prove that if  $f \in F[x]$  is a polynomial of degree 2 or 3, then  $f$  is irreducible in  $F[x]$  if and only if it has no root in  $F$ .

I will prove that  $f$  is reducible if and only if it has a root in  $F$ , which is equivalent.

If  $f$  has a root  $c \in F$ , then by the root-factor theorem (Corollary 1.5) we can write  $f = (x - c) \cdot g$ , where  $\deg g = \deg f - 1$ . Thus if  $\deg f \geq 2$  then  $\deg g \geq 1$ , so  $f$  is reducible.

For the converse, suppose that  $\deg f = 2$  or  $3$  and  $f$  is reducible, say  $f = gh$  with  $\deg g \geq 1$  and  $\deg h \geq 1$ . We must have either  $\deg g = 1$  or  $\deg h = 1$ ; otherwise we would have  $\deg f = \deg g + \deg h \geq 4$ . If  $\deg g = 1$ , write  $g = ax + b$  with  $a \neq 0$ . Because  $F$  is a field,  $a$  is invertible, so  $b \cdot a^{-1}$  is a root of  $g$  and hence of  $f$ . If  $\deg h = 1$  then the argument is similar.

**§3.1 #9** As I said by email, Shifrin doesn't define what it means for a polynomial in  $R[x]$  to be irreducible when  $R$  is not a field, so our answers to (a) and (b) must necessarily be a little vague.

- a. *Show that unique factorization fails horribly in  $R[x]$  when  $R$  is not an integral domain. . .*

Following his hint, let us consider the product

$$(\bar{2}x + \bar{3})(\bar{3}x + \bar{2}) = x$$

in  $\mathbb{Z}_6[x]$ . If the conclusion of Theorem 1.8 held in this ring, then we would have the same number of factors on each side of the equation, and we could pair them off such that they differed by a constant multiple. But here we see that the left-hand side has two linear factors while the right-hand side has only one, and neither  $\bar{2}x + \bar{3}$  nor  $\bar{3}x + \bar{2}$  is a constant multiple of  $x$ .

The other product that he asks us to consider is

$$(\bar{2}x + \bar{4})(\bar{3}x^2 + \bar{3}) = \bar{0},$$

which is even worse.

- b. *Show that Proposition 1.7 also fails when  $R$  is not an integral domain.*

Proposition 1.7 states that if  $f$  is irreducible and  $f \mid gh$ , then  $f \mid g$  or  $f \mid h$ . In  $\mathbb{Z}_6[x]$  we have  $x \mid (\bar{2}x + \bar{3})(\bar{3}x + \bar{2})$ , but neither  $x \mid \bar{2}x + \bar{3}$  nor  $x \mid \bar{3}x + \bar{2}$ , because any multiple of  $x$  has constant term  $\bar{0}$ . Now maybe we don't want to say that  $x$  is irreducible in  $\mathbb{Z}_6[x]$ , but again Shifrin hasn't defined "irreducible" when the coefficient ring is not a field.

- c. *How many roots does  $f = \bar{2}x - \bar{4} \in \mathbb{Z}_6[x]$  have?*

It has two roots, namely  $\bar{2}$  and  $\bar{5}$ :

$$\begin{array}{lll} f(\bar{0}) = \bar{2} & f(\bar{1}) = \bar{4} & f(\bar{2}) = \bar{0} \\ f(\bar{3}) = \bar{2} & f(\bar{4}) = \bar{4} & f(\bar{5}) = \bar{0}. \end{array}$$

This contrasts with what happens in a polynomial ring over a field, where a polynomial of degree  $d$  can have at most  $d$  roots.

**§3.1 #10** *Decide whether each of the following polynomials is irreducible.*

Notice that every polynomial but the last one has degree 2 or 3, so we can apply problem 8 and just check if they have any roots.

a.  $f = x^2 + \bar{1} \in \mathbb{Z}_5[x]$ .

It is reducible:  $f = (x + \bar{2})(x + \bar{3})$ .

b.  $f = x^2 + \bar{1} \in \mathbb{Z}_7[x]$ .

It is irreducible, because it has degree 2 and no roots:

$x$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$f(x)$	$\bar{1}$	$\bar{2}$	$\bar{5}$	$\bar{5}$	$\bar{2}$

c.  $f = x^2 + \bar{1} \in \mathbb{Z}_{19}[x]$ .

It is irreducible, because it has degree 2 and no roots:

$x$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\bar{10}$	$\bar{11}$	$\bar{12}$	$\bar{13}$	$\bar{14}$	$\bar{15}$	$\bar{16}$	$\bar{17}$	$\bar{18}$
$f(x)$	$\bar{1}$	$\bar{2}$	$\bar{5}$	$\bar{10}$	$\bar{17}$	$\bar{7}$	$\bar{18}$	$\bar{12}$	$\bar{8}$	$\bar{6}$	$\bar{6}$	$\bar{8}$	$\bar{12}$	$\bar{18}$	$\bar{7}$	$\bar{17}$	$\bar{10}$	$\bar{5}$	$\bar{2}$

Notice that this polynomial satisfies  $f(-x) = f(x)$ , so we didn't really need to check  $\bar{10} = -\bar{9}$  and  $\bar{11} = -\bar{8}$  and so on.

d.  $f = x^3 - \bar{9} \in \mathbb{Z}_{11}[x]$ .

It is reducible:  $f = (x + \bar{7})(x^2 + \bar{4}x + \bar{5})$ .

e.  $f = x^3 + x + \bar{1} \in \mathbb{Z}_2[x]$ .

It is irreducible, because it has degree 3 and no roots: we see that  $f(\bar{0}) = \bar{1}$  and  $f(\bar{1}) = \bar{1}$ .

f.  $f = x^4 + x^2 + \bar{1} \in \mathbb{Z}_2[x]$ .

It has no roots, but it is still reducible:  $f = (x^2 + x + 1)^2$ .