

## Math 113 HW #9 Solutions

Fraleigh 22.22. In  $\mathbb{Z}_4[x]$ , we have  $(1+2x)(1-2x) = 1$ , so  $1+2x$  is a unit.

Fraleigh 22.23. (a) True by definition.

(b) True: if  $R$  is commutative and  $f = \sum_i a_i x^i$  and  $g = \sum_j b_j x^j$  are elements of  $R[x]$  then we have

$$fg = \sum_{i,j} a_i b_j x^{i+j} = \sum_{i,j} b_j a_i x^{j+i} = gf.$$

(c) True; we proved this in class.

(d) True. Any divisor of zero in  $R$  can be regarded as a constant polynomial in  $R[x]$ , which is then a divisor of zero in  $R[x]$ .

(e) False. If  $f$  and  $g$  are nonzero elements of  $R[x]$ , then the highest exponent in the sum defining  $fg$  is the sum of the degrees of  $f$  and  $g$ . When  $R$  is not an integral domain, it is possible that  $\deg(fg) < \deg(f) + \deg(g)$ , see (f). But we always have  $\deg(fg) \leq \deg(f) + \deg(g)$ ; and equality must hold when  $R$  is an integral domain.

(f) False. For example let  $R = \mathbb{Z}_6$  and  $f = 1 + 2x^3$ ,  $g = 1 + 3x^4$ . Then since  $2 \cdot 3 = 0$  we have  $fg = 1 + 2x^3 + 3x^4$  which has degree only 4.

(g) True since  $h(\alpha) = f(\alpha)g(\alpha) = 0 \cdot g(\alpha) = 0$ .

(h) True. A unit must have degree zero since degree of polynomials is additive under multiplication, and any unit of  $F$ , regarded as a constant polynomial, is also a unit in  $F[x]$ , with the same multiplicative inverse.

(i) True. Multiplying a polynomial by  $x$  simply increases each exponent by one, so if  $f$  is nonzero, i.e.  $f$  has some nonzero coefficient, then  $xf$  also has a nonzero coefficient so  $xf \neq 0$ .

(j) False. For example in  $\mathbb{Z}_6[x]$  we have  $(2x)(3x) = 0$  so  $2x$  is a zero divisor in  $\mathbb{Z}_6[x]$  which is not a zero divisor in  $\mathbb{Z}_6$ .

Fraleigh 22.26. Let  $f = \sum_i a_i x^i$ ,  $g = \sum_j b_j x^j$ , and  $h = \sum_k c_k x^k$ . We then

manipulate sums as follows:

$$\begin{aligned}
 f(g+h) &= \sum_i a_i x^i \left( \sum_j b_j x^j + \sum_k c_k x^k \right) \\
 &= \sum_i a_i x^i \sum_j (b_j + c_j) x^j \\
 &= \sum_{i,j} a_i (b_j + c_j) x^{i+j} \\
 &= \sum_{i,j} (a_i b_j + a_i c_j) x^{i+j} \\
 &= \sum_{i,j} a_i b_j x^{i+j} + \sum_{i,j} a_i c_j x^{i+j} \\
 &= fg + fh.
 \end{aligned}$$

Here we have used the distributive law in  $R$  to get from the third line to the fourth, while to get between the other lines we use the definitions of addition and multiplication in  $R[x]$ .

Frleigh 22.27. (a) If  $f = \sum_i a_i x^i$  and  $g = \sum_j b_j x^j$  then

$$\begin{aligned}
 D(f+g) &= D \sum_i (a_i + b_i) x^i = \sum_i i(a_i + b_i) x^{i-1} \\
 &= \sum_i i a_i x^{i-1} + \sum_i i b_i x^{i-1} = Df + Dg
 \end{aligned}$$

so  $D$  is a homomorphism of additive groups. However  $D$  is *not* a ring homomorphism. We have  $D(fg) = (Df)g + f(Dg)$ , which is usually not the same thing as  $(Df)(Dg)$ . For example take  $f = g = x^2$ ; then  $D(fg) = 4x^3$  while  $(Df)(Dg) = 4x^2$ .

(b) The kernel of  $D$  consists of the constant polynomials.

(c) The map  $D : F[x] \rightarrow F[x]$  is surjective. We can define a formal integral  $I : F[x] \rightarrow F[x]$  by

$$I \left( \sum_i a_i x^i \right) = \sum_i \frac{a_i}{i+1} x^{i+1}.$$

Here we use the fact that  $F$  has characteristic zero so that  $1/(i+1) \in F$ . Then  $I$  is a right inverse of  $D$ , that is  $D \circ I = \text{id} : F[x] \rightarrow F[x]$ , which implies that  $D$  is surjective.

Fraleigh 23.8. We first try to find a single generator. We have  $2^{11} = 1$ , so 2 is not a generator. The same problem occurs with 3 and 4. Let's try  $-2 = 21$  instead. The successive powers of  $-2$  are  $-2, 4, -8, 16, -9, 18, -13, 3, -6, 12, -1, 2, -4, 8, -16, 9, -18, 13, -3, 6, -12, 1$ . So  $-2$  has order 22 and is a generator. By Corollary 6.16, the set of all generators consists of the elements  $(-2)^n$  where  $n$  is relatively prime to 22, i.e.  $n = 1, 3, 5, 7, 9, 13, 15, 17, 19, 21$ . Reading these off from the above list, the generators are  $-2, -8, -9, -13, -6, -4, -16, -18, -3, -12$ . Adding 23 to these to make them positive and sorting, we get 5, 7, 10, 11, 14, 15, 17, 19, 20, 21.

Fraleigh 23.10. To do this we look for a root  $\alpha$  in  $\mathbb{Z}_7$  by trying all 7 possibilities, then divide by  $x - \alpha$ , then repeat this process with the quotient. 0 and 1 are not roots, but 2 is, so we divide to get  $x^3 + 2x^2 + 2x + 1 = (x - 2)(x^2 + 4x + 3)$ . Now we see that the quotient  $x^2 + 4x + 3$  factors over  $\mathbb{Z}$ , and hence over  $\mathbb{Z}_7$ , as  $(x + 1)(x + 3)$ . Thus the final answer is  $(x - 2)(x + 1)(x + 3)$ .

Fraleigh 23.18. Yes, use  $p = 3$ .

Fraleigh 23.19. Yes, use  $p = 3$  again.

Fraleigh 23.25. (a) True because it has degree 1 and we are over a field.

(b) True as in (a).

(c) True by Eisenstein with  $p = 3$ .

(d) False, because 5 is a root, so in  $\mathbb{Z}_7[x]$  we have  $x^2 + 3 = (x + 2)(x - 2)$ .

(e) True by a previous problem since the units in a field are the nonzero elements, by the definition of a field.

(f) True; this seems to be exactly the same as (e). (?!?)

(g) True; this follows from the factor theorem as we showed in class.

(h) True. This follows from (g) since a polynomial in  $F[x]$  can be regarded as a polynomial in  $E[x]$  also.

(i) True. A polynomial of degree 1 in  $F[x]$  has the form  $ax + b$  with  $a \neq 0$ , and then  $-b/a$  is a zero.

(j) True; this follows from (g).

Fraleigh 23.26.  $x + 2$  is a factor of  $f(x) = x^4 + x^3 + x^2 - x + 1$  in  $\mathbb{Z}_p[x]$  if and only if  $f(-2) = 0$  in  $\mathbb{Z}_p$ , if and only if  $p$  divides  $f(-2)$  in  $\mathbb{Z}$ . In  $\mathbb{Z}$  we compute  $f(-2) = 15 = 3 \cdot 5$ , so the possibilities are  $p = 3$  and  $p = 5$ .

Fraleigh 23.37. (a) Since  $\sigma_m$  is a homomorphism, it follows that  $\overline{\sigma_m}$  is a homomorphism. More generally, as remarked in class, a ring homomorphism  $\phi : R \rightarrow S$  induces a homomorphism  $\overline{\phi} : R[x] \rightarrow S[x]$  defined by  $\overline{\phi}(\sum_i a_i x^i) =$

$\sum_i \phi(a_i)x^i$ . If  $f = \sum_i a_i x^i$  and  $g = \sum_j b_j x^j$  then

$$\overline{\phi}(f + g) = \sum_i \phi(a_i + b_i)x^i = \sum_i (\phi(a_i) + \phi(b_i))x^i = \overline{\phi}(f) + \overline{\phi}(g),$$

and similarly  $\overline{\phi}(fg) = \overline{\phi}(f)\overline{\phi}(g)$ . Since  $\sigma_m$  is surjective, it follows that  $\overline{\sigma}_m$  is surjective; given any polynomial in  $\mathbb{Z}_m[x]$ , you can find inverse images of its coefficients in  $\mathbb{Z}$ , to obtain an inverse image of the polynomial in  $\mathbb{Z}[x]$ .

(b) If  $f$  is reducible in  $\mathbb{Q}[x]$ , then by a theorem we proved,  $f$  is reducible in  $\mathbb{Z}[x]$ , so we can write  $f = gh$  with  $g, h \in \mathbb{Z}[x]$  and  $\deg(g), \deg(h) < n$ , so then  $\sigma_m(f) = \sigma_m(g)\sigma_m(h)$ , and  $\deg(\sigma_m(g)) \leq \deg(g) < n$ , likewise  $\deg(\sigma_m(h)) < n$ .

(c) Let's look for a prime  $p$  such that  $x^3 + 17x + 36$  is irreducible in  $\mathbb{Z}_p$ . It is tempting to try  $p = 17$ , but that doesn't work because in  $\mathbb{Z}_{17}$  the polynomial has 9 as a root. So let's try small primes.  $p = 2$  or  $p = 3$  won't work because the polynomial mod 2 or 3 will be divisible by  $x$ . Let's try  $p = 5$ . We want to show that  $x^3 + 2x + 1$  is irreducible in  $\mathbb{Z}_5$ . Since  $\mathbb{Z}_5$  is a field and the polynomial has degree 3, this is equivalent to showing that there is no root. Trying all 5 possibilities, we see that none of them is a root.