Mathematics 351 – Abstract Algebra 1
Solutions for Problem Set 3
September 22, 2007

Section 4.3

5. $\Rightarrow$: If f and g are associates, then $f = ug$, where u is a unit in $F[x]$. By Corollary 4.9, this says $f = ug$ where $u \neq 0$ is a constant polynomial. The equation $f = ug$ shows $g|f$ by definition. Since u^{-1} exists in F, we also have $u^{-1}f = g$, which shows $f|g$.

$\Leftarrow$: Assume $f|g$ and $g|f$. Then we have equations $g = fk$ and $f = g\ell$ for some $k, \ell \in F[x]$. Substituting from the second equation into the first and using the associative law for multiplication in $F[x]$, we have $g = (k\ell)g$. By considering degrees, we see that $\deg(k\ell) = 0$, so both k and ℓ must be nonzero constants. Hence f, g are associates in $F[x]$.

6. If $x^2 + 1 = (ax + b)(cx + d)$ for $a, b, c, d \in \mathbb{Q}$, then by equating coefficients on both sides, $ac = 1$, $bd = 1$ and $ad + bc = 0$. This Shows $d = \frac{1}{b}$ and $c = \frac{1}{a}$, so $\frac{a}{b} + \frac{b}{a} = 0$. Multiplying both sides of the last equation by ab, $a^2 + b^2 = 0$, which is only possible if $a = b = 0$, which is absurd since $ac = bd = 1$. This contradiction shows $x^2 + 1$ must be irreducible in $\mathbb{Q}[x]$.

14. The two ways are $x^2+x = x(x+1)$ and $x^2+x = (x+3)(x+4)$ (note $x^2+7x+12 \equiv x^2+x \bmod 6$). *Comment:* This problem shows that unique factorization for polynomials (as in Theorem 4.12) can fail in $R[x]$ when R is not a field!

16. $\Rightarrow$: Assume that p is irreducible in $F[x]$ and p does not divide g. We must show that $(p, g) = 1$. Suppose not. Then There is some polynomial d of positive degree with $d|p$ and $d|g$. Since p is irreducible, the first divisibility statement can only be true if d is an associate of p. But then $p|g$ as well since p and d differ only by a nonzero constant multiple. This is a contradiction to the assumption that d does not divide g. Hence $(p, g) = 1$.

$\Leftarrow$: Assume that p is a polynomial such that for *every* $g \in F[x]$, either $p|g$ or $(p, g) = 1$. We want to show that p must be irreducible. Suppose not. Then $p = hk$ for two polynomials h, k of positive degrees. Apply the hypothesis with $g = h$. we get that either $p|h$ or $(p, h) = 1$. But both of these lead to contradictions. First, p cannot divide h, since $p = hk$ and $\deg(k) \geq 1$. Second, $(p, h) = 1$ is also impossible since h is a common divisor of h and p of positive degree. Therefore, p satisfying the given condition must be irreducible.

20. The hypothesis is that p, q are both irreducible, but $p \neq cq$ for any nonzero constant $c \in F$. By Exercise 16 above, since p is irreducible, either $p|q$ or $(p, q) = 1$. However, $p|q$ is not possible since q irreducible says that the only factors of q are units and associates of q. But we are given that p and q are not associates. Hence p and q are relatively prime.

21. (a) The reducible monic polynomials of degree 2 in $\mathbb{Z}_p[x]$ come in two "flavors:" $(x + a)(x + b)$ with $a, b \in F$ distinct, and $(x + a)^2$ for $a \in F$. There are p of the second type because a can be any

one of the p elements of $\mathbb{Z}_p$. There are $\frac{p(p-1)}{2}$ of the second type because:

- a can be any one of the p elements $\mathbb{Z}_p$,
- b can be any one of the $p-1$ elements of $\mathbb{Z}_p$ different from a, but
- every such polynomial is obtained in exactly two different ways by this construction.

The total number is $p + \frac{p(p-1)}{2} = \frac{p(p+1)}{2}$.

(b) Every monic polynomial of degree 2 is either reducible or irreducible (these are mutually exclusive properties). There are p^2 total monic polynomials $f = x^2 + \alpha x + \beta$ of degree 2 in $\mathbb{Z}_p[x]$, since α can be any one of the p elements of $\mathbb{Z}_p$ and for each α, β can be any one of the p elements of $\mathbb{Z}_p$. Hence the number of monic irreducibles of degree 2 is

$$p^2 - \frac{p(p+1)}{2} = \frac{p(p-1)}{2}.$$

22. (a) The quick way to see this is to note that for all $a \in \mathbb{Z}_3$, since $\mathbb{Z}_3[x]$ is a commutative ring:

$$(x+a)^3 = x^3 + 3ax^2 + 3a^2x + a^3 \equiv x^3 + a \bmod 3.$$

This shows $x^3 + a$ is reducible.

(b) Similar to (a):

$$(x+a)^5 = x^5 + 5ax^4 + 10a^2x^3 + 10a^3x^2 + 5a^4x + a^5 \equiv x^5 + a \bmod 5.$$

(where we used the fact $a^5 \equiv a \bmod 5$ for all a, easy to check, and mentioned in class).

23. (a) Since $x^2 + 2$ is quadratic, using some results (Corollary 4.18 in particular) from the next section, it suffices to show that it has no roots in $\mathbb{Z}_5$. This is clear since $0^2 + 2 \equiv 2$, $1^2 + 2 \equiv 3$, $2^2 + 2 \equiv 1$, $3^2 + 2 \equiv 1$, $4^2 + 1 \equiv 3$.

(b) $x^4 - 4 = (x^2 + 2)(x^2 - 2)$. Both factors can be seen to be irreducible. The first one is by part (a), the other one is by a similar argument.

Section 4.4

4. (a) $x - 2$ is a factor of the polynomial if and only if 2 is a root, or $16 - 40 + 20 + 6 + k = 0$, which says $k = -2$.

(b) $x + 1$ is a factor if and only if $-1 \equiv 4$ is a root in $\mathbb{Z}_5$. This says $1 - 2 - 3 + k + 1 = 0$, or $k = -3 \equiv 2 \bmod 5$.

5. By Theorem 4.15, $x - 1_F$ divides $f(x) = a_n x^n + \cdots a_1 x + a_0$ if and only if 1_F is a root of f. This is equivalent to

$$0_F = f(1_F) = a_n + a_{n-1} + \cdots + a_1 + a_0,$$

which is what we wanted to show.

8. (e) Since this is a cubic polynomial, we can test for irreducibility by seeing if there are roots in $\mathbb{Z}_{11}$. With $x = 4$, we have $4^3 - 9 = 64 - 9 = 55 \equiv 0 \bmod 11$. Hence $x - 4$ is a factor of $x^3 - 9$ in $\mathbb{Z}_{11}$, and this polynomial is reducible. (f) If we substitute $x = 1$ we get $1^4 + 1^2 + 1 \equiv 0 \bmod 3$, so 1 is a root and this polynomial is reducible too.

9. (See Exercise 21 from Section 4.3 above!) There are precisely $\frac{3(3-1)}{2} = 3$ monic irreducibles of degree 2 in $\mathbb{Z}_3[x]$:

$$x^2 + 1, x^2 + x + 2, x^2 + 2x + 2.$$

The systematic ways to find them are either

- to list all monic polys of degree 2, then cross off the ones that have roots in $\mathbb{Z}_3$, or
- to make all of the reducible monic polys of degree 2 in $\mathbb{Z}_5$ as in Exercise 21 from Section 4.3, multiply them out, and take all the polynomials not obtained that way.

Similarly, in $\mathbb{Z}_5[x]$, we get $\frac{5(5-1)}{2} = 10$ such polynomials:

$$x^2 + 2, x^2 + 3, x^2 + 2x + 4, x^2 + x + 1, x^2 + 3x + 3,$$
$$x^2 + 3x + 4, x^2 + 4x + 1, x^2 + 4x + 2, x^2 + x + 2, x^2 + 2x + 3.$$

12. If $c_n a^n + \cdots + c_1 a + c_0 = 0_F$, then multiply both sides by $(a^{-1})^n$ to obtain $c_n + c_{n-1} a + \cdots + c_1 a^{n-1} + c_0 a^n$. This shows a^{-1} is a root of the "reversed" polynomial $c_n + c_{n-1} x + \cdots + c_0 x^n$.

13. (a) If f, g are associates in $F[x]$, then $g = uf$ for some $u \neq 0 \in F$. Then for all $a \in F$, $g(a) = uf(a)$. If a is a root of f, then $f(a) = 0_F$, so $g(a) = u \cdot 0_F = 0_F$ as well. Conversely, if a is a root of g, then $g(a) = 0_F$. Hence $0_F = uf(a)$, so $f(a) = u^{-1} 0_F = 0_F$, and a is a root of f.

(b) The answer is no, since for instance g could equal f times a polynomial in $F[x]$ that has no roots in F. An explicit counterexample is $f(x) = x - 1$ and $g(x) = (x - 1)(x^2 + 1)$ in $\mathbb{Q}[x]$. These have the same roots in F (namely $x = 1$), but f, g are not associates.

16. Consider the polynomial $h = f - g$. By the given information $\deg(h) = \deg(f - g) \leq n$. But $h(c_i) = f(c_i) - g(c_i) = 0$ for $i = 0, \ldots, n$, so h has $n + 1$ roots in F. Therefore, by Corollary 4.16, $h = 0$ (the zero polynomial), and $f = g$.

18. Let $f = c_n x^n + \cdots + c_1 x c_0 \in \mathbb{Q}[x]$. Apply φ to both sides of the equation $0 = f(r)$:

$$\begin{aligned} 0 = \varphi(f(r)) &= \varphi(c_n r^n + \cdots + c_1 r + c_0) \\ &= \varphi(c_n r^n) + \cdots + \varphi(c_1 r) + \varphi(c_0) \text{ (sum property of homomorphisms)} \\ &= \varphi(c_n)\varphi(r)^n + \cdots + \varphi(c_1)\varphi(r) + \varphi(c_0) \text{ (mult. property of homomorphisms)} \\ &= c_n \varphi(r)^n + \cdots + c_1 \varphi(r) + c_0 \text{ (since } c_i \in \mathbb{Q}) \end{aligned}$$

This shows that $\varphi(r)$ is also a root of f.

19. (a) $\Leftarrow$: If a is a multiple root of f, then $f(x) = (x-a)^k q(x)$ for some $k \geq 2$, and some $q \in \mathbb{R}[x]$. Hence by the product rule for derivatives

$$f'(x) = k(x-a)^{k-1}q(x) + (x-a)^k q'(x).$$

Since $k \geq 2$, $k-1 \geq 1$, so $f'(a) = 0$ and a is also a root of f'.

$\Rightarrow$: Conversely, assuming a is a root of f and f', write $f(x) = (x-a)^k q(x)$ where $q(a) \neq 0$ (i.e. k is as large as possible). Then by the equation above,

$$0 = f'(a) = k(a-a)^{k-1}q(a) + (a-a)^k q'(a) = k(a-a)^{k-1}q(a).$$

Since $q(a) \neq 0$, $k-1 \geq 1$, and hence $k \geq 2$. This shows a is a multiple root of f.

(b) We show the contrapositive: If f has a multiple root, then $(f, f') \neq 1$. But this is clear from the above, since if $k \geq 2$, then $(x-a)|f$ and $(x-a)|f'$.

24. Consider the mapping

$$\begin{aligned} \varphi_a : F[x] &\to F \\ f &\mapsto f(a). \end{aligned}$$

Then φ_a is a homomorphism of rings since for all $f, g \in F[x]$,

$$\begin{aligned} \varphi_a(f+g) &= (f+g)(a) = f(a) + g(a) = \varphi_a(f) + \varphi_a(g) \\ \varphi_a(f \cdot g) &= (f \cdot g)(a) = f(a) \cdot g(a) = \varphi_a(f) \cdot \varphi_a(g). \end{aligned}$$

It is surjective (onto), since for all $b \in F$ there are $f \in F[x]$ such that $\varphi_a(f) = f(a) = b$. For a very simple example, take the constant polynomial $f = b$ (!)