Solutions to Homework #20

1. Saracino, Section 19, Problem 19.2(a,b,c):
For each of the following polynomials, determine whether or not they are irreducible in $\mathbb{Q}[X]$. If they are reducible, factor them into a product of irreducibles.

(a) $X^3 - X^2 + 36$ (b) $2X^3 - 8X^2 - 6X + 20$ (c) $2X^4 + 3X^3 + 15X + 6$

Solutions. (a): Since $f = X^3 - X^2 + 36 \in \mathbb{Z}[X]$, we may apply Exercise 19.1, to see that the only possible roots in $\mathbb{Q}$ are $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 9, \pm 12, \pm 18, \pm 36$. However, $f(a) > 36 > 0$ for any $a > 0$, so we can discard all the positive numbers in that list. Similarly, for $a \leq -4$, we have $f(a) \leq (-4)^3 - (-4)^2 + 36 < 0$. So we only need to check $-1, -2, -3$, and we see that $f(-3) = -27 - 9 + 36 = 0$.
Doing long division of $X + 3$ into $X^3 - X^2 + 36$ [not shown here; see me if you are not sure how to do this computation], we get $f(X) = (X + 3)(X^2 - 4X + 12)$.
Write $q(X) = X^2 - 4X + 12$. We have already seen that the only possible roots of f in $\mathbb{Q}$ are $-1, -2, -3$, so these are also the only possible roots of q in $\mathbb{Q}$.
But $q(-3) = 9 + 12 + 12 \neq 0$, and $q(-2) = 4 + 8 + 12 \neq 0$, and $q(-1) = 1 + 4 + 12 \neq 0$. So q has no roots in $\mathbb{Q}$. Thus, by Theorem 19.8, q is irreducible over $\mathbb{Q}$.
Thus, $\boxed{f \text{ is reducible and factors as } f(X) = (X + 3)(X^2 - 4X + 12)}$

[Here are three other possible ways to show q is irreducible. First, complete the square to write $q(X) = (X - 2)^2 + 8$, which has no roots in $\mathbb{R} \supseteq \mathbb{Q}$ since for any $a \in \mathbb{R}$, we have $q(a) \geq 8 > 0$. Second, its discriminant is $(-4)^2 - 4(8) = -16 < 0$, so by the quadratic formula q has no roots in $\mathbb{R} \supseteq \mathbb{Q}$. Third, apply Exercise 19.1 directly to q, to see that the only possible roots in $\mathbb{Q}$ are $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$, and then deduce that none of them are roots.]

(b): Note that $g = 2X^3 - 8X^2 - 6X + 20$ can be written as $g = 2h$, for $h = X^3 - 4X^2 - 3X + 10$. Since $h \in \mathbb{Z}[X]$, we may again apply Exercise 19.1, showing that the only possible rational roots of h are ± 1, ± 2, ± 5, ± 10.
We check $h(1) = 4 \neq 0$, $h(-1) = 8 \neq 0$, $h(2) = -4 \neq 0$, $h(-2) = -8 \neq 0$, $h(5) = 20 \neq 0$, $h(-5) < -125 < 0$, $h(10) > 600 > 0$, and $h(-10) < -1000 < 0$. Thus, h has no roots in $\mathbb{Q}$; g also has no roots in $\mathbb{Q}$, since $h = (1/2)g$.
Thus, by Theorem 19.8, $\boxed{g \text{ is irreducible in } \mathbb{Q}[X]}$

[Alternately: reducing mod 3, we have $\bar{g} = 2X^3 + X^2 + 2 \in \mathbb{F}_3[X]$, and a quick check shows $\bar{g}(a) \neq 0$ (in $\mathbb{F}_3$) for $a = 0, 1, 2 \in \mathbb{F}_3$. So $\bar{g}$ is irreducible in $\mathbb{F}_3[X]$ by Theorem 19.8. So g is irreducible in $\mathbb{Q}[X]$, by Theorem 19.12.]

(c) Apply Eisenstein's Criterion with $p = 3$. The lead coefficient is not divisible by p, whereas all the other coefficients are; and the constant coefficient 6 is not divisible by $p^2 = 9$.
So Eisenstein says $\boxed{\text{the polynomial is irreducible in } \mathbb{Q}[X]}$

---

2. Saracino, Section 19, Problem 19.3, variant
For each of the following polynomials, determine whether or not they are irreducible in $\mathbb{F}_3[X]$. If they are reducible, factor them into a product of irreducibles. [As always, justify your answers.]

(a) $X^4 + X^3 + 2X^2 + X + 2$ (b) $X^4 + 2X^2 + X + 2$

Solutions.
(a): Call this polynomial $f(X)$. Checking shows $f(2) = 1 - 1 - 1 + 2 + 2 = 0$ in $\mathbb{F}_3$, so $X = 2 = -1$ is a root, and hence $X + 1$ is a factor. Doing long division of polynomials [computation skipped here] shows $f(X) = (X + 1)g(X)$, where $g(X) = X^3 + 2X + 2$. We check $g(0) = 2 \neq 0$, $g(1) = 2 \neq 0$, and

$g(2) = 2 \neq 0$, so g has no roots in $\mathbb{F}_3$. Thus, by Theorem 19.8, since g is cubic, g is irreducible in $\mathbb{F}_3[X]$. So the desired product of irreducibles is $\boxed{(X+1)(X^3+2X+2)}$

(b): Call this polynomial $h(X)$. Checking shows $h(1) = 1+2+1+2 = 0$ in $\mathbb{F}_3$, so $X = 1$ is a root, and hence $X - 1 = X + 2$ is a factor. Doing long division of polynomials [computation skipped here] shows $h(X) = (X+2)k(X)$, where $k(X) = X^3 + X^2 + 1$.
Further checking shows $k(1) = 1+1+1 = 0$ in $\mathbb{F}_3$, so again $X+2$ is a factor, and a second long division [computation skipped here] shows $k(X) = (X+2)q(X)$, where $q(X) = X^2 + 2X + 2$.
We check $q(0) = 2 \neq 0$, $q(1) = 2 \neq 0$, and $q(2) = 1 \neq 0$, so q has no roots in $\mathbb{F}_3$. Thus, by Theorem 19.8, since q is quadratic, q is irreducible in $\mathbb{F}_3[X]$. So the desired product of irreducibles is $\boxed{(X+2)^2(X^2+2X+2)}$

---

3. Saracino, Section 19, Problem 19.12:
Let R be a commutative ring, and let $r \in R$. Define $\varphi_r : R[X] \to R$ by $\varphi_r(f) = f(r)$.
Prove that φ_r is a ring homomorphism.

Proof. Given $f, g \in R[X]$, write $f = \sum a_i X^i$ and $g = \sum b_i X^i$ with both sums for $i \geq 0$, with $a_i, b_i \in R$, and with only finitely many coefficients nonzero. Then

$$(f+g)(r) = \sum_{i\geq 0}(a_i + b_i)r^i = \sum_{i\geq 0}(a_i r^i + b_i r^i) = \sum_{i\geq 0}(a_i r^i) + \sum_{i\geq 0}(b_i r^i) = f(r) + g(r),$$

where the second equality is by the distributive law in R, and the third is by the commutativity of $+$.
Multiplication is a bit more complicated:

$$\begin{aligned}(fg)(r) &= \sum_{k\geq 0}\Big(\sum_{i=0}^{k} a_i b_{k-i}\Big)r^k = \sum_{i\geq 0}\sum_{k\geq i} a_i b_{k-i} r^k = \sum_{i\geq 0}\sum_{j\geq 0} a_i b_j r^{i+j} = \sum_{i\geq 0}\sum_{j\geq 0}(a_i r^i)(b_j r^j) \\ &= \sum_{i\geq 0}(a_i r^i)\sum_{j\geq 0}(b_j r^j) = f(r)g(r),\end{aligned}$$

where we switched the order of summation of $0 \leq i \leq k$ in the second inequality, re-indexed via $j = k - i$ in the third, used commutativity of multiplication in R in the fourth, and used distributivity in R in the fifth. QED

Proof Without Sigmas. If you found the Sigma notation confusing, here is the same proof with "dot-dot-dot" notation instead.
Given $f, g \in R[X]$, write $f = a_0 + a_1 r + a_2 r^2 + \cdots$ and $g = b_0 + b_1 r + b_2 r^2 + \cdots$, with $a_i, b_i \in R$, and with only finitely many coefficients nonzero. Then

$$\begin{aligned}(f+g)(r) &= (a_0 + b_0) + (a_1 + b_1)r + (a_2 + b_2)r^2 + \cdots \\ &= (a_0 + b_0) + (a_1 r + b_1 r) + (a_2 r^2 + b_2 r^2) + \cdots \\ &= (a_0 + a_1 r + a_2 r^2 + \cdots) + (b_0 + b_1 r + b_2 r^2 + \cdots) = f(r) + g(r),\end{aligned}$$

where the second equality is by the distributive law in R, and the third is by the associativity and commutativity of $+$.
Multiplication is a bit more complicated:

$$\begin{aligned}(fg)(r) &= a_0 b_0 + (a_0 b_1 + a_1 b_0)r + (a_0 b_2 + a_1 b_1 + a_2 b_0)r^2 + \cdots \\ &= a_0 b_0 + (a_0 b_1 r + a_1 b_0 r) + (a_0 b_2 r^2 + a_1 b_1 r^2 + a_2 b_0 r^2) + \cdots \\ &= (a_0 b_0 + a_0 b_1 r + a_0 b_2 r^2 + \cdots) + (a_1 b_0 r + a_1 b_1 r^2 + a_1 b_2 r^3 + \cdots) \\ &\qquad + (a_2 b_0 r^2 + a_2 b_1 r^3 + a_2 b_2 r^4 + \cdots) + \cdots \\ &= a_0(b_0 + b_1 r + b_2 r^2 + \cdots) + a_1 r(b_0 + b_1 r + b_2 r^2 + \cdots) + a_2 r^2(b_0 + b_1 r + b_2 r^2 + \cdots) + \cdots \\ &= (a_0 + a_1 r + a_2 r^2 + \cdots)\cdot(b_0 + b_1 r + b_2 r^2 + \cdots) = f(r)g(r),\end{aligned}$$

where we used the distributive law in the second equality, regrouped using associativity and commutativity of $+$ in the third, used the commutativity of $\cdot$ and the distributive law again in the fourth, and used the distributive law yet again in the fifth. QED

---

4. [Not from Saracino, but may be useful on the next problem.]
Let R be a ring, let $k \geq 0$ be an integer, and let $a_0, \ldots, a_{k+1} \in R$ and $b_0, \ldots, b_{k+1} \in R$. Prove that

$$\sum_{i=0}^{k}(i+1)a_{i+1}b_{k-i} + \sum_{i=0}^{k}(k+1-i)a_i b_{k+1-i} = (k+1)\sum_{i=0}^{k+1} a_i b_{k+1-i}$$

Proof. Re-index the first sum as $\displaystyle\sum_{i=1}^{k+1} i a_i b_{k+1-i}$, by replacing all appearances of i by $i-1$, and hence letting the new i run from 1 to $k+1$. That gives us:

$$\sum_{i=0}^{k}(i+1)a_{i+1}b_{k-i} + \sum_{i=0}^{k}(k+1-i)a_i b_{k+1-i} = \sum_{i=1}^{k+1} i a_i b_{k+1-i} + \sum_{i=0}^{k}(k+1-i)a_i b_{k+1-i}$$
$$= \sum_{i=0}^{k+1} i a_i b_{k+1-i} + \sum_{i=0}^{k+1}(k+1-i)a_i b_{k+1-i} = \sum_{i=0}^{k+1}\big(i+(k+1-i)\big)a_i b_{k+1-i}$$
$$= \sum_{i=0}^{k+1}(k+1)a_i b_{k+1-i} = (k+1)\sum_{i=0}^{k+1} a_i b_{k+1-i}$$

where in the second equality, we have added an $i=0$ term to the first sum (which is OK since $0a_0b_{k+1} = 0_R$) and an $i = k+1$ term to the second sum (which is OK since $0a_{k+1}b_0 = 0_R$). QED

Proof Without Sigmas. If you found the Sigma notation confusing, here is the same proof with "dot-dot-dot" notation instead.

$$\sum_{i=0}^{k}(i+1)a_{i+1}b_{k-i} + \sum_{i=0}^{k}(k+1-i)a_i b_{k+1-i}$$
$$= \big(1a_1b_k + 2a_2b_{k-1} + \cdots + (k+1)a_{k+1}b_0\big) + \big((k+1)a_0b_{k+1} + ka_1b_k + \cdots + 1a_kb_1\big)$$
$$= \big(0a_0b_{k+1} + 1a_1b_k + 2a_2b_{k-1} + \cdots + (k+1)a_{k+1}b_0\big) + \big((k+1)a_0b_{k+1} + ka_1b_k + \cdots + 1a_kb_1 + 0a_{k+1}b_0\big)$$
$$= \big(0+(k+1)\big)a_0b_{k+1} + \big(1+(k)\big)a_1b_{k1} + \big(2+(k-1)\big)a_2b_{k-1} + \cdots + \big((k+1)+0\big)a_{k+1}b_0$$
$$= (k+1)a_0b_{k+1} + (k+1)a_1b_k + \cdots + (k+1)a_{k+1}b_0$$
$$= (k+1)\big(a_0b_{k+1} + a_1b_k + \cdots + a_{k+1}b_0\big) = (k+1)\sum_{i=0}^{k+1} a_i b_{k+1-i}$$ QED

---

5. Saracino, Section 19, Problem 19.17, variant:
Let R be a ring. For $f(X) = a_0 + a_1X + \cdots + a_nX^n \in R[X]$, define the *formal derivative* $f'(X)$ by

$$f'(X) = a_1 + 2a_2X + 3a_3X^2 + \cdots + na_nX^{n-1} = \sum_{i\geq 0}(i+1)a_iX^i.$$

or in Sigma notation,

$$f'(X) = \sum_{i\geq 0}(i+1)a_{i+1}X^i.$$

(a) For $f, g \in R[X]$, define $h = f+g$. Prove that $h'(X) = f'(X) + g'(X)$.

(b) For $f, g \in R[X]$, define $k = fg$. Prove that $k'(X) = f(X)g'(X) + f'(X)g(X)$.

(c) Assume that R is commutative. Let $n \geq 1$ be a positive integer.
Prove that the formal derivative of $[f(X)]^n$ is $n[f(X)]^{n-1} \cdot f'(X)$.

Proof. Given $f, g \in F[X]$, write $f = \sum a_iX^i$ and $g = \sum b_iX^i$. We'll denote the formal derivative of an expression with $\frac{d}{dx}$.

(a): $\displaystyle(f+g)' = \frac{d}{dx}\left[\sum_{i\geq 0}(a_i+b_i)X^i\right] = \sum_{i\geq 0}(i+1)(a_{i+1}+b_{i+1})X^i = \sum_{i\geq 0}\big((i+1)a_{i+1} + (i+1)b_{i+1}\big)X^i$

$$= \sum_{i\geq 0}(i+1)a_{i+1}X^i + \sum_{i\geq 0}(i+1)b_{i+1}X^i = f' + g'. \qquad \text{QED (a)}$$

(b): $(fg)' = \dfrac{d}{dx}\left[\sum_{k\geq 0}\left(\sum_{i=0}^{k} a_i b_{k-i}\right)X^k\right] = \sum_{k\geq 0}\left((k+1)\sum_{i=0}^{k+1} a_i b_{k+1-i}\right)X^k$

$$= \sum_{k\geq 0}\left(\sum_{i=0}^{k}(i+1)a_{i+1}b_{k-i} + \sum_{i=0}^{k}(k+1-i)a_i b_{k+1-i}\right)X^k$$

$$= \sum_{k\geq 0}\Big(\sum_{i=0}^{k}(i+1)a_{i+1}b_{k-i}\Big)X^k + \sum_{k\geq 0}\Big(\sum_{i=0}^{k}(k-i+1)a_i b_{k-i+1}\Big)X^k = f'g + g'f,$$

where in the third equality, we used Problem 4. QED (b)

(c): We proceed by induction on $n \geq 1$. For $n = 1$, we have $(f^1)' = f' = 1f^0 f'$, as desired. Assuming the statement is true for a particular $n \geq 1$, we have

$$(f^{n+1})' = (f^n f)' = (f^n)'f + f^n f' = (nf^{n-1}f')f + f^n f' = nf^n f' + f^n f' = (n+1)f^n f',$$

where the second equality is by part (b), the third is by the inductive hypothesis, and the fourth is because R is commutative. This proves the statement for $n+1$ and completes the induction. QED

Proof Without Sigmas. If you found the Sigma notation confusing in (a) and (b), here are the same proofs with "dot-dot-dot" notation instead.

(a): Pick $n \geq \deg f, \deg g$, and define $a_i = 0$ for any $i \geq \deg f$, and $b_i = 0$ for any $i \geq \deg g$. Then

$$(f+g)' = \frac{d}{dx}\Big[(a_0+b_0) + (a_1+b_1)X + (a_2+b_2)X^2 + \cdots + (a_n+b_n)X^n\Big]$$

$$= (a_1+b_1) + 2(a_2+b_2)X + \cdots + n(a_n+b_n)X^{n-1} = (a_1+b_1) + (2a_2+2b_2)X + \cdots + (na_n+nb_n)X^{n-1}$$

$$= \big(a_1 + 2a_2X + \cdots + na_nX^{n-1}\big) + \big(b_1 + 2b_2X + \cdots + nb_nX^{n-1}\big) = f' + g'. \qquad \text{QED (a)}$$

(b): $(fg)' = \dfrac{d}{dx}\Big[a_0b_0 + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2 + (a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)X^3 + \cdots\Big]$

$$= 1(a_0b_1 + a_1b_0) + 2(a_0b_2 + a_1b_1 + a_2b_0)X + 3(a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)X^2 + \cdots$$

$$= (1a_1b_0 + 1a_0b_1) + \big((1a_1b_1 + 2a_2b_0) + (2a_0b_2 + 1a_1b_1)\big)X$$
$$+\big((1a_1b_2 + 2a_2b_1 + 3a_3b_0) + (3a_0b_3 + 2a_1b_2 + 1a_2b_1)\big)X^2 + \cdots$$

$$= \big[1a_1b_0 + (1a_1b_1 + 2a_2b_0)X + (1a_1b_2 + 2a_2b_1 + 3a_3b_0)X^2 + \cdots\big]$$
$$+\big[1a_0b_1 + (2a_0b_2 + 1a_1b_1)X + (3a_0b_3 + 2a_1b_2 + 1a_2b_1)X^2 + \cdots\big]$$

$$= \Big[\big(1a_1 + 2a_2X + 3a_3X^2 + \cdots\big)\cdot\big(b_0 + b_1X + b_2X^2 + \cdots\big)\Big]$$
$$+\Big[\big(a_0 + a_1X + a_2X^2 + \cdots\big)\cdot\big(1b_1 + 2b_2X + 3b_3X^2 + \cdots\big)\Big] = f'g + g'f,$$

where in the third equality, we used Problem 4. QED (b)