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 $\mathbb{Q}[X]$.

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

Solutions. (a) Since $f = X^3 + X + 36 \in \mathbb{Z}[X]$, we may apply Exercise 19.1, to see that the only possible roots in $\mathbb{Q}$ are $\pm1, \pm2, \pm3, \pm4, \pm6, \pm9, \pm12, \pm18, \pm36$. However, $f(a) > 36 > 0$ for any $a > 0$, so we can discard all the positive numbers in that list. In addition, for $a \leq -4$, we have $f(a) \leq (-4)^3 - 4 + 36 = -32 < 0$, so $f(a) \neq 0$. The only remaining numbers to test are $-1, -2, -3$. We check $f(-1) = 34 \neq 0$, $f(-2) = 26 \neq 0$, and $f(-3) = 6 \neq 0$, so f has no roots in $\mathbb{Q}$. Since $\deg f = 3$, it follows by Theorem 19.8 that f is irreducible in $\mathbb{Q}[X]$.

———— ———— ———— ———— ———— ———— ————

(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, g 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 is not divisible by p^2. So Eisenstein says the polynomial is irreducible in $\mathbb{Q}[X]$.

---

2. Saracino, Section 19, Problem 19.3(a,d):
Write each of the following polynomials as a product of irreducible polynomials over the given field.

(a) $2X^3 + X^2 + 2$ over $\mathbb{F}_3$ (d) $X^4 + X^3 + 2X^2 + X + 2$ over $\mathbb{F}_3$

Solutions. (a) Plugging in $X = 0, 1, 2$ gives the values $2, 2, 1 \in \mathbb{F}_3$, respectively. Thus, the cubic polynomial has no roots in $\mathbb{F}_3$ and hence is itself irreducible. So it is already written as a product of a (single) irreducible polynomial.

———— ———— ———— ———— ———— ———— ————

(b) Call this polynmial $f(X)$. 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 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, since g is cubic, g is irreducible in $\mathbb{F}_3[X]$. So the desired product of irreducibles is $(X + 1)g(X)$.

---

3. Saracino, Section 19, Problem 19.12:
Let R be a commutative ring, let $r \in R$, and let $f, g \in R[X]$. Define $h = f + g$ and $k = fg$. Prove that

$$h(r) = f(r) + g(r) \quad \text{and} \quad k(r) = f(r)g(r).$$

Proof. Given f, g, r as above, 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

---

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

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

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

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

(c) 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): $(f+g)' = \dfrac{d}{dx}\Big[\sum_{i\geq 0}(a_i + b_i)X^i\Big] = \sum_{i\geq 0}(i+1)(a_{i+1} + b_{i+1})X^i$

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

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

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

$= \sum_{k\geq 0}\Big(\sum_{i=0}^{k}(i+1)a_{i+1}b_{k-i}\Big)X^k + \sum_{k\geq 0}\Big(\sum_{i=0}^{k}(k-i+1)a_i b_{k-i+1}\Big)X^k = f'g + g'f$, where in the last equality, we re-indexed the first sum.

(c): We proceed by induction on $n \geq 1$. For $n = 1$, we have $(f^1)' = f' = 1f^0f'$, as desired.
Assuming the statement is true for a particular $n \geq 1$, we have
$(f^{n+1})' = (f^nf)' = (f^n)'f + f^nf' = (nf^{n-1}f')f + f^nf' = nf^nf' + f^nf' = (n+1)f^nf'$,
where the second equality is by part (b). This proves the statement for $n+1$ and completes the induction.
QED