

ABSTRACT ALGEBRA A
HOMEWORK 6 SOLUTIONS

CHAPTER 6

- 6-16.** If $f(x) = x^5 - x^4 - 2x^3 + 2x^2 - 15x + 15$, then clearly $f(1) = 0$; so $x - 1$ is a factor of $f(x)$. Dividing it out, we get

$$f(x) = (x - 1)(x^4 - 2x^2 - 15).$$

It's easy to see that if $x = \pm\sqrt{5}$, then $x^2 = 5$, and so $f(x) = 5^2 - 2 \cdot 5 - 15 = 0$. This means that both of $x \pm \sqrt{5}$ are factors of $f(x)$. It's also easy to see that if $x = \pm\sqrt{3}$, then $x^2 = 3$, and so $f(x) = 3^2 - 2 \cdot 3 - 15 \neq 0$, so that neither of $x \pm \sqrt{3}$ is a factor of $f(x)$. Of course, we're close. What we have done so far is probably enough for us to see that

$$f(x) = (x - 1)(x + \sqrt{5})(x - \sqrt{5})(x + i\sqrt{3})(x - i\sqrt{3}).$$

- 6-22.** I'm trying to do this one using tools that would have been available to a student in 1971—no *Maple* or graphing calculators or whatever. First of all, easy algebra gives us

$$\begin{aligned} f(x) &= x^5 - 4x^4 + 2x + 2 \\ f'(x) &= 5x^4 - 16x^3 + 2 \\ f''(x) &= 20x^3 - 48x^2 = (20x - 48)x^2. \end{aligned}$$

The lead term of x^5 in $f(x)$ means that if f is going to have exactly 3 roots, then from left to right, the graph has to start out negative, become positive, drop back negative again, and then head on up to $+\infty$. With this in mind, we can start looking for values of f . Rather minimal experimentation shows that

$$\begin{aligned} f(-1) &= -5 \\ f(0) &= 2 \\ f(1) &= 1 \\ f(2) &= -26 \\ f(3) &= -73 \\ f(4) &= 10. \end{aligned}$$

The Intermediate Value Theorem therefore guarantees at least 3 real roots, one between -1 and 0 , one between 1 and 2 , and one between 3 and 4 .

Could there be more than these 3 real roots? Well, Rolle's Theorem guarantees that between any two roots of f , there must be a root of f' ; so it makes sense to see what we can learn about the roots of f' . It's easy to see that $f''(x) < 0$, and therefore that $f'(x)$ is decreasing, on both the intervals $(-\infty, 0)$ and $(0, 2.4)$. (Could you use the Mean Value Theorem to prove this?) There can therefore be at most one root for f' on $(-\infty, 2.4)$. Similarly, $f''(x) > 0$ and therefore $f'(x)$ is increasing on $(2.4, +\infty)$; so f' has at most one root on $(2.4, +\infty)$. Since it's easy to

check that $f'(2.4) \neq 0$, this means that f' has at most 2 roots, and therefore that f has at most 3 roots.

6-23. Multiplying the first factor by $\frac{3}{5}$ and multiplying the second by $\frac{5}{3}$ gives

$$\begin{aligned} 15x^5 - 9x^4 - 4x^3 + 21x^2 - 13x + 6 &= (5x^3 - \frac{10}{3}x + \frac{15}{3})(3x^2 - \frac{9}{5}x + \frac{6}{5}) \\ &= (3x^3 - 2x + 3)(5x^2 - 3x + 2). \end{aligned}$$

This is probably all the problem wanted you to do, but if you wanted to push a little farther, you could ask whether the factors produced here are in fact irreducible over $\mathbb{Q}[x]$ (and therefore over $\mathbb{Z}[x]$). The quadratic factor is easy to dispose of: the quadratic formula shows that it has no real roots, and therefore no rational roots. The cubic factor is a bit more of a bother, but not much. The Rational Roots Theorem says that its only possible rational roots are ± 3 , ± 1 , and $\pm \frac{1}{3}$. It's easy to check that none of these numbers is in fact a root, which means that $3x^3 - 2x + 3$ has no linear factors. If it factors at all, though, it has to factor into a linear and a quadratic factor; so it is also irreducible. See how much information you can get if you just put a little effort in?

6-24. In $\mathbb{Z}_2[x]$, $x^2 + 1 = (x + 1)^2$. In $\mathbb{Z}_3[x]$, $x^2 + x + 1 = (x - 1)(x - 2) = (x + 2)(x + 1)$. Finally, in $\mathbb{Z}_p[x]$, $x^{p-1} + x^{p-2} + \cdots + x + 1$ obviously has the root 1; doing the long division shows that it factors as

$$(x - 1)(x^{p-2} + 2x^{p-3} + 3x^{p-4} + \cdots + (p - 2)x + (p - 1)).$$

It might be interesting to see if this factors further (it does), and to explore what you can learn about its factorization in general.

6-25. Apply Eisenstein with $p = 13$.

6-26. I assume we're supposed to regard c as an integer, though the problem doesn't say so.

If c has no square divisors (such c are said to be *square-free*, though some people also use the German term *quadratifrei*), then $c = p_1 p_2 \cdots p_k$ is a product of distinct primes. Eisenstein can be used with p equal to any of the p_i to show that $x^2 - c$ is irreducible.

If c is not a perfect square, then c has a unique representation in the form

$$c = q^2 r,$$

where q and r are integers and $r \neq 1$ is quadratifrei.

(For instance, $c = 2 \cdot 3^2 \cdot 5^3 \cdot 7^4 \cdot 11^5$ factors as $c = (3 \cdot 5 \cdot 7^2 \cdot 11^2)^2 (2 \cdot 5 \cdot 11)$.)

Suppose $x^2 - c$ factors as $x^2 - c = (x - a)(x - b)$. If we define y to satisfy $qy = x$, then

$$x^2 - c = q^2 y^2 - q^2 r = (qy - a)(qy - b),$$

so that

$$y^2 - r = \left(y - \frac{a}{q}\right) \left(y - \frac{b}{q}\right)$$

factors over $\mathbb{Q}[x]$. By the first part of the problem, though, this cannot be; so $x^2 - c$ is irreducible over $\mathbb{Q}[x]$.

Notice that what this problem has done is to prove in a very succinct way that Unique Factorization implies that \sqrt{c} is irrational for every integer c which

isn't a perfect square. This close connection between Unique Factorization and irrationality is worth meditating upon.

6-27. Well, there's a ton of the puppies. How about $x^5 - 3$ (use $p = 3$) and $81x^5 - 32x^4 + 64x^3 + 128x^2 + 256x - 102$ (use $p = 2$).

6-28. Use Eisenstein with $p = 2$.

6-29. The way we did this back in Discrete Math was first to use Euclid's Algorithm to compute the gcd:

$$104 = 65 \cdot 1 + 39$$

$$65 = 39 \cdot 1 + 26$$

$$39 = 26 \cdot 1 + 13$$

$$26 = 13 \cdot 2.$$

Thus, $\gcd(104, 65) = 13$, a fact that probably comes as no shock.

We then rewrote the equations above as equations for the remainders:

$$(1) \quad 39 = 104 - 65 \cdot 1$$

$$(2) \quad 26 = 65 - 39 \cdot 1$$

$$(3) \quad 13 = 39 - 26 \cdot 1.$$

We want to write 13 as an integer linear combination of 104 and 65. Equation (3) writes 13 as a linear combination of 39 and 26; then (2) lets us get rid of the 26 and write 13 as a linear combination of 65 and 39; then (1) lets us get rid of the 39 and write 13 as a linear combination of 65 and 104. Here's the algebra:

$$\begin{aligned} 13 &= 39 - 26 \cdot 1 \\ &= 39 - [65 - 39 \cdot 1] \cdot 1 \\ &= 39 \cdot 2 - 65 \cdot 1 \\ &= [104 - 65 \cdot 1] \cdot 2 - 65 \cdot 1 \\ &= 104 \cdot 2 - 65 \cdot 3 \end{aligned}$$

6-30. If P and Q have no common factors of positive degree, then their gcd must be a constant c . By Theorem 6-8, there exist polynomials \bar{S} and \bar{T} such that

$$P\bar{S} + Q\bar{T} = \gcd(P, Q) = c.$$

Letting $S = \bar{S}/c$ and $T = \bar{T}/c$ then gives $PS + QT = 1$, as desired.

Even this argument makes the problem look harder than it is, since gcds are only defined up to multiplication by units (that is, by ring elements having multiplicative inverses). Since the coefficients lie in a field, every non-zero element c is a unit. We might therefore just as well have set $c = 1$ to begin with.