March 27, 2021

18.702 Comments on Problem Set 5

due Friday, March 26

1. Chapter 12, Exc. 2.4. (*infinitely many primes in* $F[x]$)

2. In the ring of integers $\mathbb{Z}$, the greatest common divisor d of two positive integers a, b is the positive integer that generates the ideal $a\mathbb{Z} + b\mathbb{Z}$. So $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. The intersection $z\mathbb{Z} \cap b\mathbb{Z}$ is also an ideal. It is a principal ideal $m\mathbb{Z}$ for some positive integer m. The integer m is called the *least common multiple* of a and b.
(i) Prove that a and b divide m, and that if an integer n is divisible by a and b, then it is divisible by m.
(ii) Prove that $ab = md$.

First, $(ab)/d = (a/d)b = a(b/d)$ is an integer and it is divisible by a and by b. Therefore m divides $(ab)/d$ and md divides ab. Next, we write $d = ra + sb$. Then $md = ram + sbm$. Since both a and b divide m, ab divides md.

3. Chapter 12, Exercise 4.5. (*irreducibility of some polynomials*)

They are all irreducible. The Eisenstein Criterion applies to **(a)** and **(d)**, the only possible integer roots of **(c)** are ± 1. For **(b)**, a linear factor must be $x \pm 1$, $2x \pm 1$, $4x \pm 1$ or $8x \pm 1$. If the coefficient of x is $2, 4$ or 8, the term $8x^3$ is too big to cancel out, and $pm1$ aren't roots.

4. Chapter 12, Exc. 4.6. (*factoring* $x^5 + 5x + 5$)

For $\mathbb{Q}[x]$, Eisenstein applies. Modulo 2, we get $x^5 + x + 1$. It is divisible by the only irreducible polynomial of degree 2, which is x^2+x+1: $x^5+x+1 = (x^2+x+1)(x^3+x^2+1)$.

5. Chapter 12, Exc. 4.8. (*factoring certain quartics*)

One case in which $f = +bx^2 + c$ factors is that the quadratic polynomial $y^2 + by + c$ has a root in the field F. If $y^2 + by + c = (y - u)(y - v)$, then, setting $y = x^2$, one sees that $f = (x^2 - u)(x^2 - v)$.

I assigned this problem because there is another way that f might factor. It can be found by solving the equation $x^4 + bx^2 + c = (x^2 + px + q)(x^2 + p'x + q')$ with indeterminate coefficients:

$$(x^2 + px + q)(x^2 + p'x + q') = x^4 + (p + p')x^3 + (q + q' + pp')x^2 + (pq' + p'q)x + qq'$$

Equating coefficients, $p' = -p$, $q' = q$, $q^2 = c$, and $2q - p^2 = b$. If these equations can be solved in F, then $f = (x^2 + px + q)(x^2 - px + q)$.