Sample homework solutions for 3.1

Jim Brown

5. Suppose $\deg(f(x)) = n$, $\deg(g(x)) = m$, and $m \geq n$. Prove or give a counterexample:

(a) $\deg(f(x) + g(x)) = m$.

This statement is false. Consider the polynomial ring $(\mathbb{Z}/2\mathbb{Z})[x]$ and polynomials $f(x) = x+1$ and $g(x) = x$. Then $f(x)+g(x) = 1$, which has degree 0.

(b) $\deg(f(x) \cdot g(x)) = m + n$.

This statement is false as well. Consider the polynomial ring $(\mathbb{Z}/4\mathbb{Z})[x]$ and polynomials $f(x) = 2x+1$ and $g(x) = 2x$. Then $f(x) \cdot g(x) = 2x$, which has degree 1.

6. Prove that if F is a field, $f(x) \in F[x]$, and $\deg(f(x)) = n$, then $f(x)$ has at most n roots in F.

Proof: We proceed by induction on the degree of $f(x)$. Suppose $f(x)$ is a polynomial of degree 1, i.e., $f(x) = ax + b$ for some $a, b \in F$. Then $-\frac{b}{a} \in F$ is a root of this polynomial and the only root, so the base case of $n = 1$ is true. Now suppose that for some positive integer k we know that any polynomial of degree k has at most k roots in F. Let $f(x)$ be a polynomial of degree $k+1$. If $f(x)$ has no roots in F we are done. Therefore assume $f(x)$ has at least one roots, call it c. Corollary 1.5 goves that $(x-c)$ divides $f(x)$. So there exists a polynomial $g(x) \in F[x]$ with $\deg(g(x)) = k$ and $f(x) = (x-c)g(x)$. By our induction hypothesis we know that $g(x)$ has at most k roots in F, thus we see that $f(x)$ can have at most $k+1$ roots in F. Therefore by induction we have that a polynomial of degree n can have at most n roots in F. ■

11. Find all odd prime numbers p so that $x + \overline{2}$ is a factor of $f(x) = x^4 + x^3 + x^2 - x + \overline{1} \in (\mathbb{Z}/p\mathbb{Z})[x]$.

Recall that Corollary 1.5 gives that $x+\overline{2}$ is a factor of $f(x)$ if and only if $-\overline{2}$ is a root of $f(x)$. This says that we need $(-2)^4+(-2)^3+(-2)^2-(-2)+1 \equiv 0 (\mathrm{mod}\, p)$, i.e., we must have $15 \equiv 0 (\mathrm{mod}\, p)$. Since the only primes that

satisfy this condition are 3 and 5, we see that p must be 3 or 5.

14. For each of the following numbers c, find an irreducible polynomial in $\mathbb{Q}[x]$ that has the number $c \in \mathbb{C}$ as a root:

(d) $\sqrt{1+\sqrt{3}}$

The first step is to find a polynomial that $\sqrt{1+\sqrt{3}}$ is a root of, and then either show it is irreducible or find its irreducible factor that $\sqrt{1+\sqrt{3}}$ is a root of. We begin by squaring $\sqrt{1+\sqrt{3}}$ to obtain

$$(\sqrt{1+\sqrt{3}})^2 = 1+\sqrt{3}.$$

Since we have a $\sqrt{3}$ left over, we square again to obtain

$$(\sqrt{1+\sqrt{3}})^4 = 4+2\sqrt{3}.$$

Now we can combine these two and obtain that $\sqrt{1+\sqrt{3}}$ is a root of the polynomial $f(x) = x^4 - 2x^2 - 2$. Now to show this is irreducible one must show that there are no polynomials of lower degree that multiply to give this polynomial. Checking there is no degree 1 factor is not difficult. Make the substitution $y = x^2$ and then solve the resulting quadratic equation to see that there are no roots in $\mathbb{Q}$. Then one must check that there are not 2 degree 2 polynomials that multiply to give $f(x)$. Assume there are $g(x) = ax^2 + bx + c$ and $h(x) = \alpha x^2 + \beta x + \gamma$ so that $f(x) = g(x)h(x)$. If one works out the equations resulting from the coefficients one will reach a contradiction. The easiest way to see this polynomial is irreducible however is to use Eisenstein's criterion, a theorem that we will get to in Section 3.3.