LECTURE 13: POLYNOMIALS AND FACTORING...

(I took this from Nichol's Abstract Algebra text, 3rd Ed, p.201)

Th$^{\text{m}}$ (DIVISION ALGORITHM)

Let R be any ring and let $f(x)$, $g(x)$ be polynomials in $R[x]$. Assume $f(x) \neq 0$ and that the leading coefficient of $f(x)$ is a <u>unit</u> in R. Then uniquely determined polynomials $q(x)$ and $r(x)$ exist s.t.

$$(1.) \quad g(x) = q(x)f(x) + r(x)$$

$$(2.) \quad \text{Either } r(x) = 0 \text{ or } \deg r(x) < \deg(f(x))$$

<u>Proof</u>: write f for $f(x)$ and g for $g(x)$ for brevity. If $g = 0$ or $\deg(g) < \deg(f)$ then $g = 0 \cdot f + g$ establishes (1.) and (2.) hold with $r(x) = g(x)$. Otherwise, suppoce $m = \deg(g)$ and $n = \deg(f)$ where $m \geq n$. We prove the Th$^{\text{m}}$ by <u>induction</u> on m. Let

$$f = ux^n + ax^{n-1} + \cdots$$
$$g = bx^m + cx^{m-1} + \cdots$$

where $u \in R^\times$ by assumption. Consider then

$$\begin{aligned} g_1 &= g - bu^{-1}x^{m-n}f \\ &= (bx^m + cx^{m-1} + \cdots) - bu^{-1}x^{m-n}(ux^n + ax^{n-1} + \cdots) \\ &= 0 \cdot x^m + (c - bu^{-1}a)x^{m-1} + \cdots \end{aligned}$$

Hence either $g_1 = 0$ or $\deg(g_1) < m$ thus by induction hypothesis, polynomials q_1 and r exist s.t. $g_1 = q_1 f + r_1$ where either $r = 0$ or $\deg(r) < \deg(f)$. But then,

$$g = g_1 + bu^{-1}x^{m-n}f = [q_1 + bu^{-1}x^{m-n}]f + r$$

which completes the induction and proves (1.) and (2.). ↲

Proof: uniqueness remains. Suppose we have

$$g(x) = q(x) f(x) + r(x)$$

and

$$g(x) = q_1(x) f(x) + r_1(x)$$

Then

$$r - r_1 = (q_1 - q) f$$

If $q_1 - q \neq 0$ then since leading coeff of f is a unit, $(q_1 - q) f \neq 0$ and thus

$$\deg(r - r_1) = \deg[(q_1 - q) f]$$
$$= \deg(q_1 - q) + \deg(f)$$

$$\Rightarrow \deg(r - r_1) \geq \deg(f)$$

$\Rightarrow$ contradiction with $\deg(r), \deg(r_1) < \deg(f)$

$$\therefore q_1 - q = 0 \Rightarrow \underline{q = q_1}$$

$$\Rightarrow r - r_1 = 0 \quad \therefore \underline{r = r_1}$$

Then $\underline{g = qf + r}$, uniquely so. //

4.6 Lecture 26: factorization of polynomials

What are the rules for factoring? How do we factor? We begin to answer these questions in certain special cases. We discover some suprising results about the interplay between $\mathbb{Z}$, $\mathbb{Z}_n$ and $\mathbb{Q}$.

Definition 4.6.1. *Let D be an integral domain. We say $f(x) \in D[x]$ which is neither zero nor a unit in $D[x]$ is* **irreducible over** *D if whenever $f(x) = g(x)h(x)$ with $g(x), h(x) \in D[x]$ then $g(x)$ or $h(x)$ is a unit in $D[x]$. A nonzero, nonunit, element of $D[x]$ that is not irreducible over D is known as a* **reducible polynomial over** *D.*

In other words, if a polynomials is not not reducible then it's reducible.

Example 4.6.2. *Consider $f(x) = x^2 + 1$. Note $f(x)$ is irreducible over $\mathbb{R}$ or $\mathbb{Q}$. However, $f(x)$ is reducible over $\mathbb{C}$ as $f(x) = (x + i)(x - i)$.*

Example 4.6.3. *If $f(x) = 2x + 4$ then $f(x) = 2(x + 2)$ thus $f(x)$ is reducible over $\mathbb{Z}$ as 2 is not a unit in $\mathbb{Z}$. On the other hand, $f(x)$ is irreducible over $\mathbb{Q}$ or $\mathbb{R}$ as $2x + 4 = g(x)h(x)$ implies one of these is a nonzero constant. In $\mathbb{Q}$ or $\mathbb{R}$ every nonzero element is a unit.*

Our main point in these examples is that context matters. Irreducibility depends both on the polynomial in question and the ring from which coefficients are taken.

Example 4.6.4. *Let $f(x) = x^2 - 7$ then $f(x) = (x - \sqrt{7})(x + \sqrt{7})$ hence $f(x)$ is reducible over $\mathbb{R}$ (it is obvious that the factors are not units in $\mathbb{R}[x]$, the units in $\mathbb{R}[x]$ are all in $\mathbb{R}^{\times}$). In contrast, $f(x)$ is irreducible over $\mathbb{Q}$ or $\mathbb{Z}$.*

Example 4.6.5. *Consider $f(x) = x^2 + 1$. We use Corollary 4.5.12 in what follows. Considering $f(x) \in \mathbb{Z}_3$ we calculate:*

$$f(0) = 1, \quad f(1) = 1 + 1 = 2, \quad f(2) = 4 + 1 = 5 = 2$$

thus $f(x)$ has no factor of the form $x - a$ in $\mathbb{Z}_3[x]$. That is, $x^2 + 1$ is irreducible in $\mathbb{Z}_3[x]$. In contrast, for $f(x) \in \mathbb{Z}_5[x]$ we have $f(2) = 4 + 1 = 5 = 0$ hence $(x - 2) \mid f(x)$. We seek a for which:

$$x^2 + 1 = (x - 2)(x + a) = x^2 + (a - 2)x - 2a$$

apparently, $a - 2 = 0$ whereas $-2a = 1$ which are simultaneously solved by $a = 2$ as $-4 = 1$ modulo 5. Indeed, this squares well with the following calculation: in $\mathbb{Z}_5[x]$ we find:

$$x^2 + 1 = x^2 - 4 = (x - 2)(x + 2)$$

As you can see, $f(x)$ is reducible over $\mathbb{Z}_5$.

The following theorem is very useful.

Theorem 4.6.6. *Suppose F is a field and $f(x) \in F[x]$ has degree 2 or 3 then $f(x)$ is reducible over F if and only if $f(x)$ has a zero in F.*

Proof: let F be a field and $f(x) \in F[x]$ with degree 2 or 3. If $f(x)$ is reducible then $f(x)$ has a factorization including a linear factor hence $f(x)$ has a zero[6] by Corollary 4.5.12. Conversely, if $f(x)$ has a zero c then $f(x) = (x - c)g(x)$ where either $g(x)$ is degree 1 or degree 2. Thus, $g(x)$ is not a unit and find $f(x)$ is reducible. □

I use the observation that units of $F[x]$ are simply the nonzero constant polynomials in $F[x]$ which we naturally identify with $F^{\times}$.

[6] hmmm, it seems half of the solution to Problem 104 is contained in the proof of Theorem 17.1