Lecture 11

The Rest on Polynomials

This week we finish our study on polynomial rings. If you have not already done so, be sure to download my article on factoring over the rationals, reals, and complexes. It can be downloaded from the assignment page in the reading section for this course or from my home page. I'm not going to say any more about it as I wrote it to be self-contained for undergraduates. Instead I will look more at sections 9.3-9.5.

9.3 An important corollary to Gauss' Lemma is that, if $p \in \mathbb{Q}[x]$ is reducible, then it is reducible in $\mathbb{Z}[x]$. In particular, by contrapositive, if $p \in \mathbb{Z}[x]$ is irreducible, it is irreducible over the rational numbers. Notice that $2x$ is reducible over $\mathbb{Z}$ because 2 is not a unit, but is irreducible over $\mathbb{Q}$ because 2 is a unit in $\mathbb{Q}$. So the converse if false unless the gcd of the coefficients is 1 (see Corollary 6). If is sufficient, but not necessary, that a polynomial is monic for the gcd of the coefficients to be 1.

The main corollary of Gauss' Lemma is that R is a UFD if and only if $R[x]$ is a UFD.

9.3.1: Let R be an integral domain with quotient field F. Let $p(x)$ be a monic polynomial in $R[x]$. Suppose that $p(x) = a(x)b(x)$ where $a(x), b(x)$ are monic polynomials in $F[x]$ of smaller degree than p. Suppose that $a(x) \notin R[x]$. By Gauss' Lemma, if R is a UFD, then p is reducible in $R[x]$, whence $p(x) = f(x)g(x) = a(x)b(x)$ where $ra(x) = f(x)$ for some $r \in R$. By the proof of Gauss' Lemma, each prime that divides the least common denominator of the coefficients of $a(x)$ and $b(x)$ must divide either $a(x)$ or $b(x)$. But $a(x)$ is monic, so divisible only by units in R, whence $r = 1$ and $a(x) = f(x) \in R[x]$. Contradiction. Therefore, R is not a UFD.

9.3.4: Let $R = \mathbb{Z} + x\mathbb{Q}[x] \subset \mathbb{Q}[x]$.

9.3.4a: Since R is a subring of an integral domain, R is an integral domain. Any unit in R is a unit in $\mathbb{Q}[x]$, so is a constant. The only units in $\mathbb{Z}$ are ± 1. Thus the only units in R are ± 1.

9.3.4b: By definition, $\pm p$, p a prime integer, are irreducible in R. If $f = c+xg(x) \in R$, then $f = c(1+c^{-1}xg(x)$ is reducible unless $c = \pm 1$. Therefore all irreducibles are $\pm p, \pm 1 + xg(x)$.

Suppose $p|(c + xg(x))(d + xh(x)) = cd + xf(x)$. Then $p|cd$, so $p|c$ or $p|d$. Since p is a unit is $\mathbb{Q}$, $p|xg(x)$ and $p|xh(x)$. Therefore p divides one of the factors and is prime. If $1 + xf(x)|(c + xg(x))(d + xh(x)) = cd + xq(x)$, then the factorization holds in $\mathbb{Q}$, whence $1 + xf(x)$ divides one of the factors and is prime.

9.3.4c: Suppose $x = (c + xg(x))(d + xh(x)) = cd + (ch_0 + dg_0)x + \cdots$. Since the degree of $x = 1$, the degrees of $g(x), h(x)$ are $0, 1$ in some order. We may assume$g(x) = c, h(x) = d + ex$. Then $x = c(d + ex) = cd + ex$. Thus either $c = 0$ or $d = 0$. But $c \neq 0$, so $d = 0$, whence $cx = 1$ and $c = 1$. But we already showed that x is not one of the irreducibles. Therefore, R is not a UFD.

9.3.4d: Note that $x = 2(x/2)$. Since the degree of 2 is 0, and the degree of x is one, x does not divide 2. If $x/2 \in (x)$, then $x/2 = ax$. Since R is an integral domain, we conclude that $a = 1/2 \in R$, a contradiction. Therefore, x is not prime. This means that $R/(x)$ is not an integral domain, so certainly not equal to $\mathbb{Z}$ which would be our first guess. I claim that $R/(x) = \{a+bx+(x)|a \in \mathbb{Z}, b \in \mathbb{Q}, 0 \leq b < 1\}$. We know that every element of $R/(x)$ is $a + xp(x) + (x)$. Since $qx^i \in (x)$ for all $q \in \mathbb{Q}, i \geq 2$, we may assume that an element of $R/(x)$ is $a + bx + (x)$ with $a \in \mathbb{Z}$. Since $nx \in (x)$ for $n \in \mathbb{Z}$, $0 \leq b < 1$ as claimed.

9.4 All of the theorems in this section are also in my handout, so I'll simply go on to some problems.

9.4.1a: Let $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$. Since $f(0) = 1 = f(1)$, $f(x)$ is irreducible as it has no linear factors and is of degree 2.

9.4.1b: Let $f(x) = x^3+x+1 \in \mathbb{F}_3$. Again, we need only look for linear factors. $f(0) = 1$, but $f(1) = 0$ so f is reducible; in fact $f(x) = (x + 2)(x^2 + x + 2)$.

9.4.1c: Let $f(x) = x^4 + 1 \in \mathbb{F}_5[x]$. Since $f(0) = 1, f(1) = 2 = f(4), f(2) = 2 = f(3)$, there are no linear terms. Now we check for two quadratics and may assume they are monic. $x^4 + 1 = (x^2 + ax + b)(x^2 + cx + d) = (x^4 + (a + c)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd$. Therefore, $c = -a, bd = 1, a(d - b) =$

$0, -a^2 + b + d = 0$. Since we are over a field, $a = 0$ or $b = d$. If $a = 0 = c$, then $b = -d, bd = 1$. So $b = 2, d = 3$ and $x^4 + 1 = (x^2 + 2)(x^2 + 3)$, so is reducible.

9.4.1d: Let $f(x) = x^4 + 10x^2 + 1 \in \mathbb{Z}[x]$. Since ± 1 are the only possible rational roots, $f(x)$ has no linear term. Let $y = x^2$. Then $f(y) = y^2+10y+1$. From what we found in part c, $a+c = 0, ac+b+d = 10, ad+bc = 0, bd = 1$. Thus, $c = -a, b = d = \pm 1, -a^2 \pm 2 = 10$. But $a^2 = 8, 12$ have no rational solutions. Therefore, f is irreducible.

9.4.3: Let $f(x) = (x-1)(x-1)\cdots(x-n)-1$. Suppose $f(x) = a(x)b(x) \in \mathbb{Z}[x]$. Then $a(i)b(i) = -1$ for $i = 1, 2, ..., n$, whence $a(i) = -b(i) \in \{-1, 1\}$. Let $A = \{i|a(i) = -1\}$ and $B = 1, 2, \cdots, n - A$, so $b(i) = -1$ for $i \in B$. Then $a(x) = \Pi_{i\in A}(x - i) - 1$ and similarly for b. Thus $f(x) = (\Pi_{i\in A}(x - i) - 1)(\Pi_{i\in B}(x - i) - 1) = \Pi_{i=1}^{n}(x - i) - \Pi_{i\in A}(x - i) - \Pi_{i\in B}(x - i) + 1 = f(x) - (\Pi_{i\in A}(x-i)+\Pi_{i\in B}(x-i))+2$. Thus $\Pi_{i\in A}(x-i)+\Pi_{i\in B}(x-i) = 2$, a contradiction because the left-hand side has positive degree. Therefore, $f(x)$ is irreducible.

9.5 This section is a culmination of all we've been doing in group and ring theory and introduces no new techniques. It simply pulls together theorems from various sections and reaches powerful conclusions.

9.5.1: Let F be a field, and let $f(x) \in F[x]$ have degree at least 1. We defined the nilradical in the lecture on 7.3 as the set of nilpotent elements, i.e., the set of $r \in R$ such that $r^n = 0$ for some positive integer n. In our current case, let $f = p_1^{n_1} \cdots p_s^{n_s}$ be a factoring of f into non-associate irreducibles p_i. If $q(\overline{x})^t = 0 \in F[x]/(f(x))$, then $q(x)^t \in (f(x))$. Thus $p_i|q$ for all i. Therefore, the nilradical of $F[x]/(f(x))$ is the set of polynomial $rp_1^{m_1} \cdots p_s^{m_s}$ where r is not divisible by p_i for any i. In practice we may assume that some $m_i < n_i$ otherwise the polynomial is zero in $F[x]/(f(x))$ anyway. This gives us a finite number of generators for the nilradical.