6.885 Algebra and Computation	September 14, 2005
Lecture 3	
Lecturer: Madhu Sudan	*Scribe: Victor Chen*

1 Introduction

Today we will cover polynomial rings and look at the Division Algorithm and Gauss's Lemma. Then we will introduce finite fields.

2 Polynomial Rings

We first note the division algorithm for polynomials.

Fact 1 *Given $a(x), b(x) \in F[x]$ for some field F, there exists polynomials $q(x), r(x) \in F[x]$ with degree of r less than the degree of b, such that $a(x) = q(x)b(x) + r(x)$.*

This motivates the concept of evaluation of polynomials. Formally, let R be a ring. Then define Eval : $R[x] \times R \longmapsto R$, where $(p(x), \alpha) \longmapsto p(\alpha) = \sum c_i \alpha^i$, where $p(x) = \sum c_i x^i$. From this, we can record the following useful corollary.

Corollary 2 1. *If $b(x) = x - \alpha$, then the polynomial $r(x)$ is simply $a(\alpha)$.*
2. *$a(\alpha) = 0$ iff $(x - \alpha)|a(x)$.*

Proof 1. Note that $r(x)$ has degree less than 1 and so is constant. Evaluate $a(x)$ at α.
2. Write $a(x) = q(x)(x - \alpha) + a(\alpha)$. ■

Last time we mentioned Gauss's Lemma, which asserts that $R[x]$ is a UFD iff R is a UFD. We first show this when R is a field.

Lemma 3 *If F is a field, then $F[x]$ is a UFD.*

Sketch of Proof Let $p(x) \in F[x]$. Then it factors into finitely many irreducibles. Suppose $p(x) = p_1(x) \ldots p_l(x) = q_1(x) \ldots q_k(x)$, with each p_i, q_j being irreducible. We want to show that $k = l$, and that for each i, there exists some j such that $p_i(x) = q_j(x)$. To prove this, we need to show that $p_i|q_j$ and $q_j|p_i$. To do this, we need the notion of GCD. The idea is that since p_1 divides $q_1(x) \ldots q_k(x)$, p_1 divides either q_1 or $q_2(x) \ldots q_k(x)$. (Else, $\gcd(p_1, q_1) = \gcd(p_1, q_2 \ldots q_k) = 1$ would imply $\gcd(p_1, q_1(x) \ldots q_k(x) = 1$.) Repeating this will show that p_1 divides q_j for some j. ■

Lemma 4 *Let F be a field. Then $F[x, y]$ is a UFD.*

Proof Note that $F[x, y] = (F[x])[y]$. The field of fraction of $F[x]$ is

$$F(x) = \widetilde{F[x]} = \{a(x)/b(x) | a(x), b(x) \in F[x]\}.$$

Claim: If a polynomial $p(y) \in R[y]$ factors in $\widetilde{R}[y]$, then it also factors over $R[y]$.

Proof of Claim: Write $p(y) = a_0 + \dots a_j y^j$. Suppose $p(y) = p_1(y)p_2(y)$ over $\widetilde{R}[y]$. Let the coefficients of $p_1(y)$ be $b_0, \dots, b_l \in \widetilde{R}$, and let the coefficients of $p_2(y)$ be $c_0, \dots, c_l \in \widetilde{R}$. Note that we can write $b_i = e_i/f_i$, where $e_i, f_i \in R$. Let $F = \mathrm{lcm}(f_0, \dots, f_l)$. Thus we can write $p_1(y) = \frac{1}{F}p'_1(y)$, where $p_i \in R[y]$. Similarly, we can write $p_2(y) = \frac{1}{G}p'_2(y)$ for some $G \in R$. So $p(y) = \frac{1}{FG}p'_1(y)p'_2(y)$. If FG is a unit, then we are done. Else, with a little more work, we can conclude that F divides every coefficient of p'_2, and G divides every coefficient of p'_1.

From the previous lemma, $F[x]$ is a UFD. Let $R = F[x]$. Then the claim implies that $F[x, y]$ is a UFD. ■

More generally, we have Gauss's Lemma:

Lemma 5 *Let R be a UFD. Then $R[x]$ is a UFD.*

Sketch of Proof Again we work over the field of fraction $\widetilde{R}[x]$. Start with $p(x) \in R[x]$. Suppose $p(x) = p_1 \dots p_l = q_1 \dots q_l$.

Claim: If p_i is irreducible in $R[x]$, then it is also irreducible in $\widetilde{R}[x]$.
Note that this Claim is the same one in the previous lemma. Hence, $p_1 \dots p_l = q_1 \dots q_l$ are still irreducible over $\widetilde{R}[x]$. Since $\widetilde{R}[x]$ is a UFD, the two factorizations are unique up to permutations and units. ■

This motivates the following algorithmic question. If we can factor over R, can we factor over $R[x]$? Suppose we work over a field F. There is the issue of finite precision when dealing with reals, so we will work with finite fields and rationals. In later lectures, we will investigate how to factor over polynomials over finite fields and rationals. For now, we will give a quick introduction to finite field in the next section.

3 Finite Fields

Lemma 6 *Let F be a finite field. Then $|F| = p^t$ for some prime p and integer t. Furthermore, for every prime p, integer $t \geq 0$, there exists a finite field F_{p^t} of size p^t.*

Before proving this, we make some observations. First consider $t = 1$. Observe that Z_p is a field. To see this, note that this is an integral domain (Suppose $ab = 0$. Then $p|ab$, implying $p|a$ or $p|b$, implying $a = 0$ or $b = 0$.) Since Z_p is a finite integral domain, it is a field. Note that inverses can be found efficiently in Z_p by using the Extended Euclidean Algorithm.

Suppose $h(x) \in F[x]$ is irreducible. Then $K = F[x]/h(x)$ is a field. To see this, let $a(x), b(x)$ be polynomials in K with degree less than h such that $a(x)b(x) = 0$. Then $a(x)b(x) = h(x)p(x)$ in $F[x]$ for some polynomial $p(x)$. Then we have $h|a$ or $h|b$ (irreducibles are primes in UFD), implying $a = 0$ or $b = 0$. Hence F is a finite domain and thus a field. To find the inverse of $a(x) \in K$, one can again run the Extended Euclidean Algorithm on $a(x)$ and $h(x)$.

Definition 7 *Suppose $h(x) \in F[x]$ is irreducible. Then $K = F[x]/h(x)$ is called an algebraic extension of F. If F has no algebraic extension, then it is called algebraically closed.*

Definition 8 *The splitting field of $h(x) \in F[x]$ is the field K such that h decomposes into linear factors over K.*

Fact 9 *Every polynomial $h(x) \in F[x]$ has a splitting field.*

Sketch of Proof Suppose h is irreducible. Then consider $K = F[z]/h(z)$. Note $h(x) \in K[x]$. $h(z) = 0 \in K$ implies that $(x - z)|h(x)$. Factoring out $x - z$, we can repeat this process until h factors completely in a much larger field. If h is not irreducible, then it factors into finitely many. Repeat this for each irreducible factors. ■

Proof (of Lemma) Let K be the splitting field of $X^{p^t} - X$ over Z_p. Consider $S = \{\alpha \in K : \alpha^{p^t} - \alpha = 0\}$, the roots of the polynomial. Since K is the splitting field of $X^{p^t} - X$, K contains all the roots of $X^{p^t} - X$. Furthermore, it can be shown that all the roots are distinct. (To show that all roots of a polynomial are distinct over the reals, it suffices to compute the GCD of the polynomial and its derivative and check if it is 1. Over a finite field, one can define derivative formally, and the same technique will work.) This implies that $|S| = p^t$. To show that S is a field, it suffices to show that it is closed under addition and multiplication, and inverses for both operations exist. To check that the sum of two elements remain in S, one would apply the Binomial Theorem; the other properties are also easy to verify.

Alternatively, one can use a counting argument to show that for every prime p and integer t, there exists a monic irreducible polynomial h of degree t over $Z_p[x]$. Then by our previous discussion, $Z_p[x]/h(x)$ is a field of size p^t. ■

4 Group representation

Given a group G and an object x, how can one determine is x in G? To do this, we must how are G and x specified? Here is one approach using the free group relation. Let $\Sigma = \{x_1, \ldots, x_k, x_1^{-1}, \ldots, x_k^{-k}\}$ be the alphabet. The elements of G are specified by sequences of letters from the alphabet, modulo some set of relations, e.g., $x_1x_2x_3x_4^{-1} = 1$, where 1 is the empty string. However, it is undecidable to determine if a group is finite using this setting (related to the Post Correspondence Problem). Even though every finite group can be represented in this way, we do not consider such representation useful.

Here is another approach. Recall from group theory that every finite group of order n is isomorphic to a subgroup (permutation group) of the symmetric group S_n, which consists of all permutations on $[n]$. So given a finite group G generated by $\{\pi_1, \ldots, \pi_k\}$, and $x \in S_n$, we can ask if $x \in G$.

We will later see that every finite group has a nice representation that allows us to solve this question in polynomial time. The question also has an interesting interpretation. Consider a Rubik's cube. Then x represents the finished configuration of the cube. The question then becomes how to go from an initial configuration, through a series of operations on the cube, that would lead to the final configuration.