LECTURE 16.

ALIREZA SALEHI GOLSEFIDY

1. Recall.

In the previous lecture, we said what an irreducible polynomial is: a non-zero, non-unit polynomial \( f(x) \) such that, if \( f(x) = p(x)q(x) \), then either \( p(x) \) or \( q(x) \) is unit.

**Remark 1.** Let \( F \) be a field. Then a non-constant polynomial \( p(x) \in F[x] \) is irreducible if and only if it cannot be written a product of two smaller degree polynomials.

We also proved

**Proposition 2.** Let \( F \) be a field. A non-constant polynomial \( p(x) \in F[x] \) is irreducible if and only if \( \langle p(x) \rangle \) is a maximal ideal if and only if \( F[x]/\langle p(x) \rangle \) is a field.

2. Reducibility test for degrees 2 and 3.

In general, it is not easy to prove if a given polynomial is irreducible or not. But if the polynomial is of degree 2 or 3, it is relatively easy.

**Theorem 3.** Let \( F \) be a field and \( p(x) \in F[x] \). Assume \( \deg(p) = 2 \) or 3. Then it is reducible over \( F \) if and only if it has a solution in \( F \).

**Proof.** In both of these cases, it is easy to see, that if \( p \) is reducible then, one of the factors is of degree 1, which implies that \( p \) has a solution over \( F \). The other direction is a corollary of the Factor Theorem. \( \Box \)

3. Gauss’s Lemma and reducibility over \( \mathbb{Z} \).

Now we would like to explore the relation between reducibility over \( \mathbb{Q} \) and \( \mathbb{Z} \).

**Example 4.** \( f(x) = 2x \) is reducible over \( \mathbb{Z} \) but irreducible over \( \mathbb{Q} \).

How about the other direction? What is the real obstruction? In Example 4, the scalar term was the problem. That is the motivation to define the *content* of a non-zero integer polynomial.

**Definition 5.** Let \( 0 \neq p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x] \). The content of \( p \) is defined to be \( c(p) := \gcd(a_0, \ldots, a_n) \).

\( p \) is called *primitive* if \( c(p) = 1 \).

**Example 6.**

1. \( c(2x + 1) = 1 \).
2. \( c(4x^3 + 2) = 2 \).
3. \( c(ap(x)) = ac(p) \) for any \( a \in \mathbb{N} \) and \( 0 \neq p(x) \in \mathbb{Z}[x] \).

**Theorem 7.** Let \( f(x) \in \mathbb{Z}[x] \) be a primitive polynomial. Then \( f(x) \) is irreducible over \( \mathbb{Q} \) if and only if it is irreducible over \( \mathbb{Z} \).

---

*Date: 2/17/2012.*
(2) Let \( p(x) \in \mathbb{Z}[x] \). If \( p(x) \) is reducible over \( \mathbb{Q} \), then it is reducible over \( \mathbb{Z} \).

In order to prove Theorem 7, first we need to prove the following lemma.

Lemma 8 (Gauss’s Lemma).

1. Product of two primitive polynomials is also primitive.
   2. For any \( f(x), g(x) \in \mathbb{Z}[x] \), we have that \( c(fg) = c(f)c(g) \).

Proof. 1. If not, then there is a prime \( p \) which divides all the coefficients of \( f(x)g(x) \), i.e. \( f(x)g(x) = 0 \), where \( f(x), g(x) \in \mathbb{Z}/p\mathbb{Z}[x] \) are obtained by reducing the coefficients modulo \( p \). Since \( \mathbb{Z}/p\mathbb{Z}[x] \) is an integral domain, either \( f \) or \( g \) = 0. This implies that \( p \) divides all the coefficients of either \( f \) or \( g \), which contradicts the fact that \( f \) and \( g \) are primitive.

2. By the definition, \( f = c(f)f_1 \) and \( g = c(g)g_1 \), where \( f_1 \) and \( g_1 \) are primitive. So \( fg = c(f)c(g)f_1g_1 \). By the first part, we know that \( f_1g_1 \) is primitive. Therefore \( c(fg) = c(f)c(g) \). \( \square \)

Proof of Theorem 7. 1. If \( f(x) \) is reducible over \( \mathbb{Z} \), then \( f(x) = p(x)q(x) \). Since \( f \) is primitive, \( \deg(p), \deg(q) > 1 \). Thus \( f \) is also reducible over \( \mathbb{Q} \). The other direction is a corollary of the second part.

2. If \( f(x) \) is reducible over \( \mathbb{Q} \), then \( f(x) = p(x)q(x) \) for some \( p(x), q(x) \in \mathbb{Q}[x] \) of smaller degree. Without loss of generality we can and will assume that \( f \) is primitive. Let \( a, b \in \mathbb{N} \) such that \( p_1(x) = ap(x) \in \mathbb{Z}[x] \) and \( q_1(x) = bq(x) \in \mathbb{Z}[x] \). So
   \[
   abf(x) = p_1(x)q_1(x).
   \]
   By Gauss’s Lemma, we have \( ab = ab \cdot c(f) = c(abf(x)) = c(p_1q_1) = c(p_1)c(q_1) \). Hence \( f = p_1/c(p_1) \cdot q_1/c(q_1) \), which shows that \( f \) is reducible over \( \mathbb{Z} \). \( \square \)

4. Irreducibility Test.

Modulo \( p \) might be easier to see if a polynomial is irreducible or not.

Theorem 9. Let \( f(x) \in \mathbb{Z}[x] \) and \( p \) be prime. Let \( \bar{f}(x) \in \mathbb{Z}/p\mathbb{Z}[x] \) be the the polynomial obtained by the reducing modulo \( p \). If \( \deg(f) = \deg(\bar{f}) \) and \( \bar{f} \) is irreducible, then \( f \) is irreducible over \( \mathbb{Q} \).

Example 10. (1) \( f(x) = (15/7)x^3 - (4/9)x^2 + x + (17/19) \).

(2) \( f(x) = x^4 + 1 \) is reducible over \( \mathbb{Z}/p\mathbb{Z} \) for any \( p \) but it is irreducible over \( \mathbb{Z} \).

Mathematics Dept, University of California, San Diego, CA 92093-0112

E-mail address: golsefidy@ucsd.edu