LECTURE 17.

ALIREZA SALEHI GOLSEFIDY

1. Recall

Last time we talked about reducibility of degree 2 and 3 polynomials over a field and then started to investigate polynomials over $\mathbb{Z}$. We finished the first part of Gauss's lemma.

2. Gauss's lemma and reducibility over $\mathbb{Z}$

Let us recall Gauss's Lemma.

Lemma 1. (1) *If $f, g \in \mathbb{Z}[x]$ are primitive, then fg is also primitive.*
(2) *For any $f.g \in \mathbb{Z}[x]$, $c(fg) = c(f)c(g)$.*

Proof. We saw the proof of the first part in the previous lecture. Here is the proof of the second part:

Let $f = c(f)f_1$ and $g = c(g)g_1$. By the definition, it is clear that f_1 and g_1 are primitive polynomials. Hence by Gauss's Lemma f_1g_1 is also primitive. Thus $c(fg) = c(c(f)c(g)f_1g_1) = c(f)c(g)c(f_1g_1) = c(f)c(g)$, and we are done. □

Theorem 2. (1) *If $f(x)$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.*
(2) *Let $f(x)$ be a primitive polynomial. $f(x)$ is irreducible over bbz if and only if it is irreducible over $\mathbb{Q}$.*

Proof. 1. Let $f = c(f)f_1$. If f is reducible over $\mathbb{Q}$, then f_1 is also reducible over $\mathbb{Q}$. Let $f_1 = g \cdot h$, where $g, h \in \mathbb{Q}[x]$ and $\deg(g)$ and $\deg(h)$ are smaller than $\deg(f_1)$. There are integers n and m such that $ng, mh \in \mathbb{Z}[x]$. Hence $(mn)f_1 = (ng)(mh)$. So

$$mn = mnc(f_1) = c((mn)f_1) = c(ng)c(mh).$$

On the other hand, $ng = c(ng)g_1$ and $mh = c(mh)h_1$ where $g_1, h_1 \in \mathbb{Z}[x]$. Therefore $f_1 = g_1h_1$ and $f = c(f)g_1h_1$ and we are done.

2. By the first part, we know that if $f(x)$ is irreducible over $\mathbb{Z}$, then it is irreducible over $\mathbb{Q}$. Now if $f(x)$ is reducible over $\mathbb{Z}$, then there are $g, h \in \mathbb{Z}[x]$ such that $g \neq \pm 1$, $h \neq \pm 1$ and $f(x) = g(x)h(x)$. If g (resp. h) is a constant, then g (resp. h) divides $c(f)$, which is a contradiction. Thus $1 \leq \deg(g), \deg(h) < \deg(f)$, which implies f is reducible over $\mathbb{Q}$. □

3. Irreducibility test

In a finite world, in principle, one can check all the possible cases to see if a given polynomial is irreducible or not.

Example 3. *Is $x^5 - 2x^2 - x + 1$ irreducible over $\mathbb{F}_3$ (when we would like to look at $\mathbb{Z}/p\mathbb{Z}$ as a field, we sometimes use $\mathbb{F}_p$ notation instead!)?*

Date: 2/22/2012.

Let's check case-by-case. Does it have a degree 1 factor? After we plug in we see that it has no zero in $\mathbb{F}_3$, so it does not have a degree one factor.

Does it have a degree 2 factor? Without loss of generality we can just check monic degree 2 polynomials: there are 9 of them. We can then use the division algorithm to check if each one of these polynomials is a factor or not.

It is faster if we just check the degree 2 monic irreducible polynomials. How can we identify them?

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

E-mail address: golsefidy@ucsd.edu