

Algebra - II
Professor Amritanshu Prasad
Mathematics
The Institute of Mathematical Science
Gauss Lemma

(Refer Slide Time: 0:15)

Gauss's Lemma


Thm (Gauss's Lemma): If $f(t) \in \mathbb{Z}[t]$, suppose $c(f)=1$ and
 $f(t) = u(t)v(t)$ in $\mathbb{Q}[t]$

Then $\exists a, b \in \mathbb{Q}$ such that $f(t) = au(t)bv(t)$, where $au(t), bv(t) \in \mathbb{Z}[t]$

Lemma: For $u(t), v(t) \in \mathbb{Z}[t]$, $c(u)c(v) = c(uv)$.

Pf: Assume that $c(u) = c(v) = 1$.
 Need to show that $c(uv) = 1$.

If $f(t) = a_0 + a_1t + \dots + a_nt^n$
 Content of f , denoted $c(f)$ is
 $c(f) := \gcd(a_0, a_1, \dots, a_n)$



As we have seen in order to construct field extensions. We need irreducible polynomials. In this lecture I am going to explain to you Gauss's Lemma which helps us to understand when some polynomials are irreducible. The statement is the following. So this theorem is called Gauss's theorem. It says that if $f(t)$ is a polynomial with coefficients in the integers.

So this $\mathbb{Z}[t]$ means we are looking at polynomials in the variable t whose coefficients are all integers and suppose the content of f is 1. So I need to explain to you what the content of f means. So if you have a polynomial $f(t) = a_0 + a_1t + \dots + a_nt^n$. Then the content of f denoted $c(f)$ is defined by, $c(f)$ is just the gcd of the numbers a_0, a_1, \dots, a_n .

So if the content of a polynomial is 1, it means that the gcd of its coefficients is 1. So if you have a polynomial with content 1 and we write $f(t)$ as a factorization $u(t)v(t)$ in $\mathbb{Q}[t]$. So I am not claiming that $u(t)$ and $v(t)$ have integer coefficients, I am just saying that $u(t)$ and $v(t)$ are polynomials with rational coefficient.

Then there exist rational numbers a and b such that $f(t)$ is equal to $au(t)bv(t)$ where these scalings of the polynomials have integer coefficients $au(t), bv(t) \in \mathbb{Z}[t]$. So

basically what it is saying is that if you have factorization in $\mathbb{Q}[t]$, then you also have a factorization in $\mathbb{Z}[t]$. And this proof of this lemma this theorem rather, Gauss's Lemma is another lemma, which is also due to Gauss, which says the content is multiplicative.

So the proof uses the following lemma. This is also due to Gauss. For u, v in $\mathbb{Z}[t]$ the content of u times the content of v is equal to the content of uv . So the content of the product of 2 polynomials is the product of their contents. \square

Now to prove this lemma here we can assume that the content of u and v is 1 because if the content of u is not 1 or the content of v is not 1, then we can divide u by its content and get a polynomial with content 1. Similarly we can divide v by its content and get a polynomial with content 1. So we can assume without loss of generality and then we need to show that the content of uv is equal to 1.

For this we will use a technique that is very useful for analyzing polynomials which is the reduction of coefficients modulo a prime. Now we need to show that the content of uv is 1. For which it is enough to show that no prime divides all the coefficients of uv . So we will just use reduction modulo p . So let me just explain that.

(Refer Slide Time: 5:07)


Idea: reduction modulo p :

$$f(t) = a_0 + a_1 t + \dots + a_n t^n \in \mathbb{Z}[t]$$

Define $\bar{f}(t) = \bar{a}_0 + \bar{a}_1 t + \dots + \bar{a}_n t^n$ where \bar{a}_i is the image of a_i in $\mathbb{Z}/p\mathbb{Z}[t]$

$$\bar{f}g = \overline{fg}$$

Observation: $f(t) \in \mathbb{Z}[t]$ is primitive (i.e., $c(f)=1$) iff its reduction modulo p is non-zero for every prime p .



So the idea is reduction modulo p . So if you have a polynomial $f(t)$ equals a_0 plus $a_1 t$ plus $a_n t$ to the n with integer coefficients. Then you can take each of these coefficients and reduce it modulo p . So define $\bar{f}(t)$ to be \bar{a}_0 plus $\bar{a}_1 t$ plus $\bar{a}_n t$ to the n .

bar t to the n where a_i bar is the image of a_i in $\mathbb{Z} \bmod p$. So this is a polynomial in $\mathbb{Z} \bmod p$.

Now this reduction map is a very nice property that if I take fg bar t , then this is f bar g part t , so this reduction map is a ring homo-morphism now to say that a polynomial is primitive it is enough to show that for every prime p its reduction modulo p is non-zero because that would mean that the prime p does not divide all of its coefficients. So the observation is f bar t belongs to $\mathbb{Z} \bmod p$ is primitive. It has content 1, if and only if its reduction mod p is non-zero for every prime p .

(Refer Slide Time: 7:30)

Gauss's Lemma

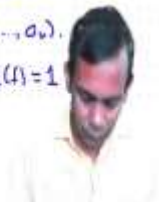
Thm (Gauss's Lemma): If $f(t) \in \mathbb{Z}[t]$, suppose $c(f)=1$ and $f(t) = u(t)v(t)$ in $\mathbb{Q}[t]$

Then $\exists a, b \in \mathbb{Q}$ such that $f(t) = au(t)bv(t)$, where $au(t), bv(t) \in \mathbb{Z}[t]$

Lemma: For $u(t), v(t) \in \mathbb{Z}[t]$, $c(u)c(v) = c(uv)$.

Pf: Assume that $c(u) = c(v) = 1$.
Need to show that $c(uv) = 1$.

If $f(t) = a_0 + a_1t + \dots + a_nt^n$
Content of f , denoted $c(f)$ is
 $c(f) := \gcd(a_0, a_1, \dots, a_n)$.
 f is primitive if $c(f) = 1$



So now coming back to this, we want to show that if, so let us just put this definition down f is primitive if $c(f)$ is 1. That is just the definition of primitivity and so what we want to show is that the product of 2 primitive polynomials is primitive. And so we take the product and we want to show that its reduction modulo any prime is non-zero. So suppose that there was a prime p with respect to which its reduction was 0.

(Refer Slide Time: 8:11)

Suppose p is a prime such that the reduction of uv mod p is 0.

$$\overline{uv} = \overline{u}\overline{v} \Rightarrow \overline{u} = 0 \text{ or } \overline{v} = 0 \text{ b/c } \mathbb{Z}/p\mathbb{Z} \text{ is an int-domain.}$$


a contradiction.

Proof of Gauss's lemma: $f(t) \in \mathbb{Z}[t]$

$$f(t) = u(t)v(t), \quad u(t), v(t) \in \mathbb{Q}[t].$$

$\exists a, b \in \mathbb{Q}$ such that $au(t) \in \mathbb{Z}[t], c(au(t))=1$
 $bv(t) \in \mathbb{Z}[t], c(bv(t))=1.$

also $f(t) = au(t)bv(t) \Rightarrow ab=1.$
 So $f(t) = au(t)bv(t)$ as needed.



Gauss's Lemma

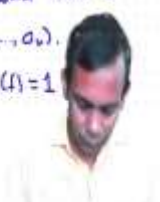
Thm (Gauss's Lemma): If $f(t) \in \mathbb{Z}[t]$, suppose $c(f)=1$ and $f(t) = u(t)v(t)$ in $\mathbb{Q}[t]$

Then $\exists a, b \in \mathbb{Q}$ such that $f(t) = au(t)bv(t)$, where $au(t), bv(t) \in \mathbb{Z}[t]$

Lemma: For $u(t), v(t) \in \mathbb{Z}[t], c(u)c(v) = c(uv).$

Pf: Assume that $c(u) = c(v) = 1.$
 Need to show that $c(uv) = 1.$

If $f(t) = a_0 + a_1t + \dots + a_nt^n$
 Content of f , denoted $c(f)$ is
 $c(f) := \gcd(a_0, a_1, \dots, a_n).$
 f is primitive if $c(f) = 1$



So suppose p is a prime such that the reduction of uv mod p is 0. But then note the uv bar, the reduction of uv mod p is $\overline{u}\overline{v}$ which implies that \overline{u} is 0 or \overline{v} is 0 just because the ring $\mathbb{Z}/p\mathbb{Z}$ is an integral domain. But this cannot happen because we know that u and v are also primitive.

So this concludes the proof of this lemma here that the product of 2 primitive polynomials is again primitive. Now we are ready to prove Gauss's Lemma, the main theorem of this lecture. So suppose we have fx equals, ft equals ut vt where ft is in as per hypothesis is has integer coefficients has ut, vt have rational coefficients.

Now if you have a polynomial with rational coefficients you can clear out the denominators of all its coefficients and get a polynomial with integer coefficients. Say you multiply all the coefficients by some integer n and you get all integer coefficients. You can choose this carefully enough so that the resulting polynomial is primitive.

So just take for example the LCM of all the denominators and that should do the trick. So there exist rational numbers a and b in \mathbb{Q} such that aut equals, aut belongs to $\mathbb{Z}t$ and content of aut is 1. That is it is primitive. bvt belongs to $\mathbb{Z}t$ and content of bvt is equal to 1 and we have ft equals aut . So here we would have a b times ft is aut by t .

But recall that in Gauss's Lemma we assume that f itself is primitive. That c of f is 1. And so c of f is 1 then c of a b times f is going to be ab but here on the right hand side we have a product of 2 primitive polynomials. So ab times f should also be a primitive polynomial which implies that ab is equal to 1 and so we have that ft is equal to aut by t as needed. This concludes the proof of Gauss's Lemma.

When we talk about field extensions we are often dealing with monic polynomials. For example, when you construct the irreducible polynomial of an algebraic element you can scale it so that it becomes monic. And so if we just talk about monic polynomials the Gauss's Lemma takes a nice monic polynomials with integer coefficients are obviously primitive because the leading coefficient is 1.


(Refer Slide Time: 12:30)

Corollary: If $f(t) \in \mathbb{Z}[t]$ is monic and $f(t) = u(t)v(t)$, where $u(t), v(t) \in \mathbb{Q}[t]$ are monic, then $u(t), v(t) \in \mathbb{Z}[t]$.

Pf: $f(t) = au(t)bu(t)$
 $au(t), bu(t) \in \mathbb{Z}[t]$
 $\Rightarrow a, b \in \mathbb{Z} \Rightarrow a=b=1.$

Example: $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$.
 ζ_n is a root of $t^n - 1$.
 $\Phi_n(t) \in \mathbb{Z}[t]$.

$\varphi_n: \mathbb{Q}[t] \rightarrow \mathbb{C}$
 $t \mapsto \zeta_n$
 $\ker \varphi_n = \Phi_n(t)$. monic.
 n th cyclotomic polynomial.



So here is the corollary of Gauss's Lemma. If f_t belongs to $\mathbb{Z}[t]$ is monic and we write f_t equals u_t times v_t where u_t and v_t belong to $\mathbb{Q}[t]$ are also monic. The u_t and v_t are in $\mathbb{Z}[t]$. But the proof is very simple. Just apply Gauss's Lemma. So what we have is, f_t is $a u_t$ times $b v_t$. Then a and b are rational numbers, u_t , v_t are primitive.

But $a u_t$ $b v_t$ belongs to $\mathbb{Z}[t]$ and if the product is monic then their leading terms must be equal to 1. The leading term of u_t and v_t must be equal to 1. So this implies that a and b are integers. So what we have is that this implies that a times b equals 1, well we know that a times b is 1. So this implies that a equals b equals 1.


So let us look at an example. A very interesting example of an algebraic integer is the n th root of unity define ζ_n to be $e^{2\pi i/n}$ this is a complex number and then ζ_n satisfies the polynomial. It is an n th root of unity. So it is a root of $t^n - 1$. So ζ_n is an algebraic polynomial.

We can construct the evaluation map, substitution map ϕ to \mathbb{C} obtained by taking t to ζ_n and the kernel of ϕ is $\mathbb{Z}[\zeta_n]$, let us say that is let us call that $\mathbb{Z}[\zeta_n]$ of capital \mathbb{Z} . It is actually denoted as $\mathbb{Z}[\zeta_n]$ of \mathbb{Z} . We can assume that this is monic by scaling it. So let us say monic and it will be reducible. This is called the n th cyclotomic polynomial.

So now $\mathbb{Z}[\zeta_n]$ is a factor of $t^n - 1$. $t^n - 1$ is a primitive monic polynomial. And so what we have is $\mathbb{Z}[\zeta_n]$ and t is a polynomial with integer coefficients. We can compute some examples of $\mathbb{Z}[\zeta_n]$ and t for small cases by hand.

(Refer Slide Time: 16:21)

n	$\Phi_n(t)$
2	$t+1$
3	t^2+t+1
4	t^2+1
5	$t^4+t^3+t^2+t+1$
6	t^2-t+1



So for example, let us write down n and v and t for some small example. So if n is equal to 2, then we are looking at zeta 2 which is a square root of 1, which is minus 1. So we just get t plus 1. Minus 1 satisfies the reducible polynomial is the root of the irreducible polynomial t plus 1. If n equals 3 then we are looking at cube roots of unity.

We are looking at e to the $2\pi i$ by 3. Are these satisfy the equation t squared plus t plus 1 which turns out to be irreducible over q . It is a quadratic polynomial. So its reducibility just means that there are no roots and if we take n equals 4, then a little bit of thinking, you may come up with t squared plus 1. So n equals 4 means we are looking at fourth roots of unity which are $1i$ minus 1 and minus i .

Zeta 4 is just i e to the $2\pi i$ by 4 and that is just i . And zeta 5 it turns out that its irreducible polynomial is t to the power 4 plus t cubed plus t squared plus t plus 1 and plus 6 it turns out that the polynomial is a bit smaller than the earlier cases. It turns out that it is t squared minus t plus 1.

So that is a few examples of cycloatomic polynomials and in the next lecture we will try to compute some infinite families of cycloatomic polynomials.