Modern Algebra Lecture Notes: Rings and fields set 4 (Revision 2)

Kevin Broughan

University of Waikato, Hamilton, New Zealand

May 13, 2010

Definition of factor

If $f(x) = g(x).h(x)$ in $R[x]$ we say $g(x)$ is a factor of $f(x)$ in $R[x]$.

Examples

(1) The polynomial $x + 2$ is a factor of $x^2 + 5x + 6$ in $\mathbb{Z}[x]$.

(2) The polynomial $x^2 + 1 = (x + i)(x - i)$ in $\mathbb{Z}[i]$, but has no factors in $\mathbb{Z}[x]$.

(3) Polys like $f(x) = x^8 + 3x^6 - 6x^5 + 3x^4 - 12x^3 + 10x^2 - 6x + 9$ are difficult to factor in any ring.

In $\mathbb{Z}[x]$ we have $f(x) = \left(x^2 + 1\right)\left(x^3 + x - 3\right)^2$. How is this done ?

Theorem 15

Let F be a field, $a \in F$ an element and $f(x) \in F[x]$ a polynomial. Then $f(x) = (x - a)q(x) + f(a)$, i.e. $f(a)$ is the remainder when we divide $f(x)$ by $x - a$. If $f(a) = 0$ then $(x - a)$ is a factor of $f(x)$.

Proof of Theorem 15

By the division identity in $F[x]$ there exist polynomials $q(x),\ r(x)$ such that $f(x) = (x-a)q(x) + r(x)$ with $r(x) = 0$ or $\deg r(x) < \deg x - a = 1$.

Therefore $r(x) = constant = r(a)$.

But $f(a) = (a-a)q(a) + r(a) = r(a)$ so $f(a) = r(a)$ and we can write $f(x) = (x-a)q(x) + f(a)$.

If $f(a) = 0$ we have $f(x) = (x-a)q(x) + 0 = (x-a)q(x)$ so $x-a$ is a factor of $f(x)$.$\square$

Theorem 16: A poly over a field of degree n has at most n zeros in the field

Proof

The polynomial must be non-zero. If n is zero the polynomial has no zeros.

Assume every polynomial of degree up to and including n has at most n zeros and let $f(x)$ be a polynomial of degree $n+1$.

If $f(x)$ has no zeros we are done. If a is a zero of $f(x)$, by Theorem 15 we can write $f(x) = (x-a)^k g(x)$, by Theorem 15, where $k \geq 1$ and $g(a) \neq 0$, $\deg f(x) = k + \deg g(x)$, so the degree of $g(x)$ is $\leq n$.

By the inductive hypothesis it has at most n zeros, $a_1, \ldots, a_m$ say with $m \leq n$.

Every zero of $g(x)$ is a zero of $f(x)$. If b is a zero of $f(x)$ other than a then $0 = f(b) = (b-a)^k g(b)$ so b is a zero of $g(x)$.

Hence the zeros of $f(x)$ are $\{b, a_1, \ldots a_m\}$ so are in number less than or equal to $n+1$, completing the proof by induction.$\square$

This is not true in general for polynomials over a ring: $x^2 + x$ has 4 zeros in $\mathbb{Z}/6Z$.

If $F \subset K$ and K is also a field, a so-called extension field, then we have actually shown $f(x)$ has at most $\deg f(x)$ zeros in K.

Examples

(1) $x^2 + 1$ has no zeros in $\mathbb{Q}$ but a full set in $\mathbb{Q}(i)$ and in $\mathbb{C}$.

(2) $x^2 - 2$ has no zeros in $\mathbb{Q}$ but a full set in $\mathbb{Q}(\sqrt{2})$.

Definition of a principal ideal domain

A principal ideal domain or PID, is an integral domain R where every ideal has the form $\langle a \rangle$ for some $a \in R$.

Examples:

(1) $\mathbb{Z}$: If $A \subset \mathbb{Z}$ is an ideal let $a > 0$ be the smallest positive element of A. Then $A = \langle a \rangle$.

(2) If F is a field then $F[x]$ **is** a principal ideal domain. This is Theorem 17 proved below.

(3) The ring $\mathbb{Z}[\sqrt{5}]$ **is** a principal ideal domain, but $\mathbb{Z}[\sqrt{-5}]$ is **not**. So being a PID is a big issue and quite subtle.

Proof of Theorem 17

Let $A \subset F[x]$ be an ideal. If $A = \{0\}$ we have $A = \langle 0 \rangle$.

If $A \neq \{0\}$ let $g(x)$ be a polynomial in A of minimum degree. We can assume $g(x)$ is monic. Then we claim $A = \langle g(x) \rangle$.

To see this let $f(x) \in A$. Then, by the division identity there are polynomials $q(x),\ r(x)$ such that $f(x) = q(x).g(x) + r(x)$ where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

If $r(x) = 0$ then $f(x) = q(x).g(x) \in \langle g(x) \rangle$.

Otherwise $r(x) = f(x) - q(x).g(x) \in A$. But $\deg r(x) < \deg g(x)$ so this case is impossible. Therefore $A = \langle g(x) \rangle$.$\square$

Definitions

If F is a field we say a polynomial $f(x) \in F[x]$ is irreducible over F if it cannot be expressed as the product of two polynomials over F with strictly lower degrees than that of $f(x)$.

If R is an integral domain we say a polynomial $f(x) \in R[x]$ is irreducible over R if whenever we write $f(x) = g(x).h(x)$ we must have either $g(x)$ or $h(x)$ a unit in $R[x]$.

Examples

(1) $x + 1$ is irreducible over $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$.

(2) A unit in $R[x]$ is a constant polynomial $f(x) = u$ where u is a unit in R.

(3) $3x + 6$ is irreducible over $\mathbb{Q}[x]$ but factors non-trivially as $3.(x + 2)$ in $\mathbb{Z}[x]$.

(4) $x^2 + 1$ is irreducible in $\mathbb{R}[x]$ but factors as $(x + i)(x - i)$ in $\mathbb{C}[x]$.

(5) $x^2 + x + 1$ is irreducible in $\mathbb{Q}[x]$ but factors as $(x + 2)(x + 2)$ in $(\mathbb{Z}/3\mathbb{Z})[x]$.

The quadratic and cubic formulas

Quadratic

If $f(x) = ax^2 + bx + c$, $a, b, c \in \mathbb{C}$ and $a \neq 0$ then in $\mathbb{C}[x]$

$$f(x) = a(x - \alpha)(x - \beta)$$

where $\alpha, \beta = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

Cubic

If $f(x) = x^3 + ax + b$ then $f(x) = (x - \alpha)(x - \beta)(x - \gamma)$ where

$$\alpha = \frac{\sqrt[3]{\sqrt{3}\sqrt{4a^3 + 27b^2} - 9b}}{\sqrt[3]{2}3^{2/3}} - \frac{\sqrt[3]{\frac{2}{3}}a}{\sqrt[3]{\sqrt{3}\sqrt{4a^3 + 27b^2} - 9b}}$$

$$\beta = \frac{\left(1 - i\sqrt{3}\right)a}{2^{2/3}\sqrt[3]{3}\sqrt[3]{\sqrt{3}\sqrt{4a^3 + 27b^2} - 9b}} - \frac{\left(1 + i\sqrt{3}\right)\sqrt[3]{\sqrt{3}\sqrt{4a^3 + 27b^2} - 9b}}{2\sqrt[3]{2}3^{2/3}}$$

$$\gamma = \frac{\left(1 + i\sqrt{3}\right)a}{2^{2/3}\sqrt[3]{3}\sqrt[3]{\sqrt{3}\sqrt{4a^3 + 27b^2} - 9b}} - \frac{\left(1 - i\sqrt{3}\right)\sqrt[3]{\sqrt{3}\sqrt{4a^3 + 27b^2} - 9b}}{2\sqrt[3]{2}3^{2/3}}$$

Factors for low degree polynomials

Degree 1

If a non-zero polynomial over a field has degree 0 it is irreducible. For degree 1, $f(x) = ax + b$, then $f(-b/a) = 0$ and $f(x)$ is irreducible.

Degree 2 or 3

If $f(x) \in F[x]$ has a zero or root, $f(a) = 0$ then $f(x)$ is reducible since $f(x) = (x - a)g(x)$. If $f(x)$ has degree 2 or 3 then it is reducible if and only if it has a factor of degree 1 if and only if it has a zero/root.

Degree 4 or more

Over $\mathbb{Q}[x]$ $(x^2 + 1)(x^2 + 2) = x^4 + 3x^2 + 2$ so the right hand side is reducible but has no root in $\mathbb{Q}$.

Polynomials over finite fields

Finding roots is easy, just test each element of the field and see if the polynomial vanishes, e.g. $f(x) = x^4 + 3x + 1$ over $\mathbb{Z}/5Z$ has $f(1) = 0$ so $x - 1 = x + 4$ divides exactly with quotient $4 + x + x^2 + x^3$. This does not vanish at $x = 0, 1, 2, 3, 4$ modulo 5, therefore it is irreducible (over $\mathbb{Z}/5Z$).

Gauss' Lemma

Definition

Let $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$. The content of $f(x)$, denoted $c(f(x))$, is the gcd of the coefficients, i.e. $\gcd(a_0, \ldots, a_n)$. If $c(f(x)) = 1$ we say $f(x)$ is primitive.

Example

(1) $f(x) = 2x^2 - 4x + 12 \implies c(f(x)) = 2$

$f(x) = 2x^3 - 3x + 6 \implies c(f(x)) = 1.$

Statement of the Lemma

Let $f(x),\ g(x) \in \mathbb{Z}[x]$ be primitive. Then $f(x).g(x)$ is also primitive, i.e. the product of two primitive polynomials is primitive.

Reduction Modulo p

A useful operation on polynomials with integer coefficients is reduction modulo p where p is a fixed prime. This is a homomorphism of polynomial rings:

$$f(x) \in \mathbb{Z}[x] \to \theta(f(x)) \in \mathbb{Z}_p[x] : \quad a_n x^n + \cdots a_0 \to [a_n]x^n + \cdots + [a_0].$$

Proof of Gauss' Lemma

Let $f(x)$, $g(x)$ be primitive and suppose $f(x).g(x)$ is not primitive. Let the prime p divide the content, i.e. p divides every coefficient of $f(x).g(x)$.

Then in $\mathbb{Z}_p[x]$, $\theta(f(x).g(x)) = 0$. But this is an integral domain (because $\mathbb{Z}_p$ is an integral domain) and, because θ is a homomorphism, $0 = \theta(f(x)).\theta(g(x))$.

Therefore $\theta(f(x)) = 0$ or $\theta(g(x)) = 0$. Suppose the former is true. But this means p divides each of the coefficients of $f(x)$.

But this is impossible, since $f(x)$ is primitive.$\square$

Factoring over $\mathbb{Q}$ equals factoring over $\mathbb{Z}$

Example

$6x^4 + 8x^3 + 3x^2 + 7x + 4 = (2x + \frac{8}{3})(3x^3 + \frac{3}{2}x + \frac{3}{2}) = (3x + 4)(2x^3 + x + 1)$

Content fact

If $f(x) \in \mathbb{Z}[x]$ then we can write $f(x) = c(f(x)).f_1(x)$ where $c(f_1(x)) = 1$.

Example

$f(x) = 12x^4 - 6x^3 + 3x + 18 = 3(4x^4 - 2x^3 + x + 6) = c(f(x)).f_1(x)$ where $f_1(x)$ has content 1, i.e. is primitive.

Theorem 18

Statement

If $f(x) \in \mathbb{Z}[x]$ and $f(x) = g(x).h(x)$ factors in $\mathbb{Q}(x)$ then $f(x) = g_1(x).h_1(x)$ in $\mathbb{Z}[x]$ and the degrees of $\deg g_1(x) = \deg g(x),\ \deg h_1(x) = \deg h(x)$.

Proof

Make $f(x)$ primitive by dividing both $f(x)$ and $g(x)$ by $c(f(x))$.

Let a be the least common multiple of the denominators of the coefficients of $g(x)$ and b the LCM of the denominators of $h(x)$ so $ag(x) \in \mathbb{Z}[x]$ and $bh(x) \in \mathbb{Z}[x]$.

Let $ag(x) = c(ag(x)).g_1(x)$ and $bh(x) = c(bh(x)).h_1(x)$, so $g_1(x),\ h_1(x)$ are primitive and in $\mathbb{Z}[x]$.

Then, since $f(x)$ is primitive, $c(abf(x) = ab$. But $abf(x) = ag(x)bh(x) = c(ag(x).g_1(x)c(bh(x)).h_1(x) = c(ag(x))c(bh(x)g_1(x).h_1(x)$.

Since, by Gauss, $g_1(x).h_1(x)$ is primitive the content of the RHS is $c(ag(x)).c(bh(x))$ which must be the content of the LHS, so they cancel leading to $f(x) = g_1(x).h_1(x)$ the factorization over $\mathbb{Z}[x]$. $\square$