Modern Algebra Lecture Notes: Rings and fields set 6, revision 2

Kevin Broughan

University of Waikato, Hamilton, New Zealand

May 20, 2010

Solving quadratic equations: traditional

The procedure

Work in $\mathbb{Q}[x]$: Let $ax^2 + bx + c = 0,\ a \neq 0$ so we can write $x^2 + (b/a)x + (c/a) = x^2 + Bx + C = 0$.

Complete the square: $(x + \frac{B}{2})^2 + C - \frac{B^2}{4} = 0$.

Take square roots (now we are outside $\mathbb{Q}$ sometimes): $x + \frac{B}{2} = \pm\sqrt{\frac{B^2}{4} - C}$.

Solve for x: $x = -\frac{B}{2} \pm \sqrt{\frac{B^2}{4} - C} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.

When are the solutions integers ?

If $a, b, c \in \mathbb{Z}[x]$ we need $b^2 - 4ac = \square$, i.e. a perfect positive square.

Solving cubic equations: traditional

Vieta's method

The equation is $x^3 + \alpha x^2 + \beta x + \gamma = 0$ in $\mathbb{C}[x]$.

Complete the cube: $(x + \frac{\alpha}{3})^3 + \beta' x + \gamma' = 0$. So replace $x + \frac{\alpha}{3}$ by y.

The equation becomes $y^3 + py + q = 0$ in $\mathbb{C}[y]$.

Let a, b satisfy $y = a - b,\ p = 3ab$ and transform to $\mathbb{C}[a, b]$.

$$\begin{aligned} 0 &= a^3 - 3a^2 b + 3ab^2 - b^3 + pa - pb + q, \\ &= a^3 - b^3 + (a - b)(-3ab + p) + q, \\ &= a^3 - b^3 + q. \end{aligned}$$

A solution (a, b) to the system $a^3 - b^3 + q = 0,\ 3ab = p$ implies $y = a - b$, which solves $y^3 + py + q = 0$.

Vieta's method completed

Multiply by 3^3a^3 to get

$$3^3a^6 - 3^3a^3b^3 + 3^3a^3q = 0.$$

Therefore

$$27a^6 + 27a^3q - p^3 = 0,$$

a quadratic equation in a^3, so solve it using the quadratic formula. Let a be a cube root of the solution and then set $b = p/(3a)$ to give $y = a - b$ and hence $x = y - (a/3)$ to solve the original equation.

Example

Expand $(x+1)(x+2)(x+3) = 0$ and then find the roots using Vieta's method. Then try $(x+i)(x+2i)(x+3i) = 0$ in $\mathbb{C}[x]$.

Historical note

A method similar to that for quadratics and cubics also, with difficulty, was achieved for quartic equations. There is no such general method available for polynomials of the 5th degree and higher.

Looking ahead

We will return to polynomial rings, especially the fields $F[x]/\langle f(x)\rangle$ later. But now we must look at unique factorization of rings more general than $\mathbb{Z}$.

Definitions

(1) An integral domain R is a commutative ring with a unity 1.
(2) Elements $a,\ b \in R$ are called associates if there is a unit $u \in R$ such that $a = ub$.
(3) An element $a \neq 0 \in R$ is called irreducible in R if whenever $a = bc$ in R, b or c is a unit.
(4) An element $a \neq 0 \in R$ is called a prime of R if whenever $a \mid bc$ in R, $a \mid b$ or $a \mid c$.
(5) If $m \in \mathbb{Z} \setminus \{0, 1\}$ is squarefree and $R = \mathbb{Z}[\sqrt{m}]$ then define the norm of an element $x = a + \sqrt{m}b$ by $N(x) = a^2 - mb^2$.

Theorem 24

(1) $N(x) = 0 \iff x = 0$,
(2) $N(xy) = N(x)N(y)$,
(3) x is a unit if and only if $N(x) = \pm 1$,
(4) If $N(x)$ is prime in $\mathbb{Z}$ then x is irreducible in $\mathbb{Z}[\sqrt{m}]$.

Example: $R = \mathbb{Z}[\sqrt{-5}]$

Irreducibles which are not primes and non unique factorizations

Firstly R is an integral domain inherited from $\mathbb{C}$.

$N(a+\sqrt{-5}b) = a^2+5b^2 = 1 \iff a+\sqrt{-5}$ is a unit of $R \iff a = \pm 1,\ b = 0$

Consider $14 = 2.7 = (3+\sqrt{-5})(3-\sqrt{-5})$.

Each of the factors $2,\ 3 \pm \sqrt{-5}$ is irreducible: $2 = xy \implies 4 = N(x)N(y)$ so $N(x) = 2,\ N(y) = 2$, but there is no integer solution to $a^2 + 5b^2 = 2$.

Similarly, $3 + \sqrt{-5} = xy \implies 14 = N(x)N(y)$ so again we need the impossible $2 = N(x)$.

If 2 were prime it would divide $3 + \sqrt{-5}$ or $3 - \sqrt{-5}$, suppose the former. Then $3 + \sqrt{-5} = 2(a + \sqrt{-5}b) \implies 3 = 2a,\ 1 = 2b$ with no integer solutions.

Primes vs irreducibles

Theorem 25

Let R be an integral domain. Then every prime p in R is irreducible.

Proof

If $p = xy$ then $p \mid xy$ so $p \mid x$ or $p \mid y$ say $p \mid x \implies x = pq$.

Then $p = xy = pqy \implies 1 = qy$ so y is a unit. Therefore p is irreducible.$\square$

Example: Gaussian Integers

in $\mathbb{Z}[i]$, 3, 7, 3i, 1+i, 1+2i are prime but 2, 5, 13, i, 1+3i are not.

Theorem 26: In a PID every irreducible is necessarily a prime

Proof

Let $a \mid bc$ and let a be irreducible. We need to show $a \mid b$ or $a \mid c$.

Define $A = \{ax + by : x, y \in R\}$. Then A is an ideal of R, a PID so $A = \langle \alpha \rangle$ for some $\alpha \in R$.

But $a \in A \implies a = \alpha\beta$ for some $\beta \in R$. Since a is irreducible either α or β must be a unit.

If β is a unit, $A = \langle \alpha \rangle = \langle a \rangle$ and $b \in A \implies a \mid b$.

If α is a unit, $A = R$ so $1 \in A \implies 1 = ax + by$ for some $x,\ y \in R$.

But then $c = axc + byc = axc + bcy$ and a divides both terms on the right, thus $a \mid c$.$\square$

Unique factorization into irreducibles

Definition

A unique factorization domain is an integral domain R in which every element which is not a unit can be written down as a product of irreducible elements of R, these factors being unique up to multiplication by associates and reordering.

Lemma

In a PID R any increasing chain of distinct ideals $A_1 \subset A_2 \subset \cdots$ is necessarily finite in length.

Proof

Let $A = \cup_j A_j$ be the union of all of the ideals in the ascending chain. Then $A \subset R$ is an ideal.

Since R is a PID, for some $\alpha \in A$ we have $A = \langle \alpha \rangle$. Since $A = \cup_j A_j$ there is a j_o such that $\alpha \in A_{j_o}$.

But then $A = \langle \alpha \rangle \subset A_{j_o}$ so $\cup_j A_j = \cup_{j=1}^{j_o} A_j$ which is of finite length.$\square$

Theorem 27: Each PID is a unique factorization domain

Proof: Step 1 - each a_0 has an irreducible factor

If a_0 is nonzero and not a unit but is irreducible this step is done, $a_0 = a_0$.
Else $a_0 = b_1 a_1$ where a_1 and b_1 are not units. If a_1 is irreducible we are done, else $a_1 = b_2 a_2$, and so on, $a_n = b_{n+1} a_{n+1}$ so $\langle a_n \rangle \subset \langle a_{n+1} \rangle$
We get a corresponding increasing chain of ideals $\langle a_0 \rangle \subset \langle a_1 \rangle \subset \cdots$, which by the above Lemma, must be finite meaning for some $r \in \mathbb{N}$, a_r is irreducible, giving an irreducible factor of a_0.

Step 2 - each a_0 can be written as a product of irreducibles

Now a_0 has an irreducible factor $a_0 = i_1 c_1$ where i_1 is irreducible. If c_1 is not a unit it too will have an irreducible factor $c_1 = i_2 c_2$, and so on. Again we get an ascending chain of ideals which must be finite: $\langle a_0 \rangle \subset \langle c_1 \rangle \subset \cdots \subset \langle c_s \rangle$ which means c_s is irreducible, so we can factor $a_0 = i_1 i_2 \cdots i_s c_s$, a product of irreducibles.

Step 3 - the product is unique up to reordering and associates

This uniqueness is very similar to that of Theorem 23 for $\mathbb{Z}[x]$, just replace the unit ± 1 by a unit u_i in R. $\square$

Examples

(1) We have seen that if F is a field then $F[x]$ is a principal ideal domain. Therefore, by Theorem 28, it is a unique factorization domain, and primes and irreducible elements coincide. Thus we could say the polynomial $x^2 + 1 \in \mathbb{Q}[x]$ was prime (but usually say it is irreducible over $\mathbb{Q}$).

(2) An example of an integral domain without unique factorization was given earlier: $\mathbb{Z}[\sqrt{-5}]$ where $14 = 2.7 = (3 - \sqrt{-5})(3 + \sqrt{-5})$ gives 2 different factorizations of 14 into irreducible factors. None of the factors can be prime.

Euclidean Domains

Definition

An integral domain R is called Euclidean if there is a function $d : R \to \mathbb{Z}_{\geq 0}$ such that
(1) for all $a,\ b \neq 0 \in R$, $d(a) \leq d(ab)$, and
(2) if $a,\ b \neq 0 \in R$ there exist $q,\ r \in R$ such that $a = bq + r$ with $r = 0$ or $d(r) < d(b)$.

Examples of Euclidean rings with their mappings d:

(1) In $\mathbb{Z}$, $d(x) := |x|$.

(2) In $F[x]$, $d(f(x)) := \deg f(x)$.

(3) In $\mathbb{Z}[i]$, $d(a + ib) = a^2 + b^2 = N(a + ib)$.

Theorem 28

Statement

If R is a Euclidean domain then R is a principal ideal domain.

Proof

Mimic the other PID proofs but use $d(x)$. If $\{0\} \neq A \subset R$ is an ideal, let $a \in A$ be an element such that $d(a)$ is a minimum.

Since R is Euclidean, given $b \in A$ there are elements $q,\ r \in R$ such that $b = qa + r$ and either $r = 0$ or $d(r) < d(a)$.

If $r = 0,\ b \in \langle a \rangle$.

If $d(r) < d(a)$ writing $r = b - qa$ we get an element of A with a strictly smaller value of $d(x)$, so this is not possible. Hence $A = \langle a \rangle$. $\square$

$$\text{ED} \implies \text{PID} \implies \text{UFD} \implies \text{ID} \implies \text{Commutative Ring} \implies \text{Ring}$$