Rings & Arithmetic 8: Euclidean Algorithm; polynomial rings

Thursday, 27 October 2005

Lectures for Part A of Oxford FHS in Mathematics and Joint Schools

- The euclidean algorithm
- A useful general fact
- The Remainder Theorem
- Roots of polynomials
- Factorising polynomials

The Euclidean Algorithm

Assume a Division Algorithm in R.

Input: elements a, b of euclidean ring R;

Output: hcf(a, b) .

Begin: while $b \neq 0$ do

$r := \text{res } a \pmod b$ [use Division Algorithm];

$a := b$;

$b := r$;

endwhile;

return a;

End.

Proof of correctness.

The Extended Euclidean Algorithm

Input: elements a, b of euclidean ring R;

Output: $\mathrm{hcf}(a, b)$ and
elements $u, v \in R$ such that $\mathrm{hcf}(a, b) = ua + vb$.

This is an interesting exercise for you.

A useful fact

Observation. *Let R be a euclidean ring (or, more generally, a PID) and $a \in R$. If a is irreducible in R then $R/(a)$ is a field.*

Proof.

Note: in particular, if f is irreducible in $F[x]$, where F is a field, then $F[x]/(f)$ is a field.

The Remainder Theorem

Theorem. *Let F be a field, let $f \in F[x]$, and let $\alpha \in F$. Then there exists $g \in F[x]$ such that*

$$f(x) = (x - \alpha)g(x) + f(\alpha)\,.$$

Proof.

Corollary. *If $f \in F[x]$ where F is a field, and $f(\alpha) = 0$ where $\alpha \in F$, then $(x - \alpha) | f(x)$ in $F[x]$.*

Roots of polynomials

Theorem. *Let F be a field and let $f \in F[x] \setminus \{0\}$. Suppose that f has k distinct roots in F. Then $k \leqslant \deg f$.*

Proof.

Note: The same holds if F is replaced by an integral domain R.

Note: An illuminating alternative proof uses the Vandermonde determinant.

Gauss's Lemma, I

Gauss's Lemma, Ver 1. *Polynomial* $c_0 + c_1x + c_2x^2 + \cdots + c_nx^n$ *in* $\mathbb{Z}[x] \setminus \{0\}$ *is said to be primitive if* $\mathsf{hcf}(c_0, c_1, c_2, \ldots, c_n) = 1$. *If* $f, g \in \mathbb{Z}[x] \setminus \{0\}$ *are primitive and* $h(x) = f(x)g(x)$ *then* h *is primitive.*

Proof.

Gauss's Lemma, Ver 2. *For* $f \in \mathbb{Z}[x] \setminus \{0\}$ *define the content by*

$c(f) := \mathsf{hcf}(c_0, c_1, \ldots, c_n)$ *where* $f(x) = c_0 + c_1x + \cdots + c_nx^n$.

If $f, g \in \mathbb{Z}[x] \setminus \{0\}$ *then* $c(fg) = c(f)c(g)$.

Proof.

Gauss's Lemma, II

Gauss's Lemma, Version 3. *Let $f \in \mathbb{Z}[x] \setminus \{0\}$. Then f can be factorised as a product of polynomials of degrees r, s in $\mathbb{Q}[x]$ if and only if f can be factorised as a product of polynomials of degrees r, s in $\mathbb{Z}[x]$.*

Proof.

Note: All these versions of Gauss's Lemma work for an arbitrary field F and integral domain R of which F is the field of fractions, so $F = \{a/b \mid a \in R,\ b \in R \setminus \{0\}\}$.

Practical factorisation of polynomials, I

Given $f \in F[x]$, how can we factorise f? **With difficulty.**

Note: If $\deg f$ is 2 or 3 then f is reducible in $F[x]$ if and only if it has a root in F.

Note: If F is finite and small then it is not unreasonable to use trial division. *E.g.*

$$\begin{aligned} x^7 - 1 &= (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) \\ &= \end{aligned}$$

in $\mathbb{Z}_2[x]$.

Practical factorisation of polynomials, I

Given $f \in F[x]$, how can we factorise f? With difficulty.

Note: If $\deg f \leqslant 3$ then f is reducible in $F[x]$ if and only if it has a root in F.

Note: If F is finite and small then it is not unreasonable to use trial division. *E.g.*

$$\begin{aligned} x^7 - 1 &= (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) \\ &= (x-1)(x^3 + x^2 + 1)(x^3 + x + 1) \end{aligned}$$

in $\mathbb{Z}_2[x]$.

Practical Factorisation of polynomials, II

Note: In $\mathbb{Q}[x]$ we find Gauss's Lemma helps greatly.

E.g. Since $x^2 - 2$ is irreducible in $\mathbb{Z}[x]$ (easy!), it is irreducible in $\mathbb{Q}[x]$, so $\sqrt{2}$ is irrational.

E.g. Challenge: $x^9 + x^3 + 1$ is irreducible in $\mathbb{Z}[x]$, therefore in $\mathbb{Q}[x]$ [See Herstein, *Topics in Algebra* (1st Ed.), p. 186].