Rings & Arithmetic 6: factorisation

Friday, 21 October 2005

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

- Highest common factor
- Irreducible and prime elements
- An example
- Euclidean rings
- Commentary.

Highest common factors, I

Definition. Element b divides element a in R (and we write $b|a$) if $\exists c \in R : a = bc$.

Definition. Elements a, b are said to be associates (and we write $a \sim b$) if $\exists u \in U(R) : a = ub$.

Note: $a \sim b$ if and only if $a|b$ & $b|a$.
Also $a \sim b$ if and only if $(a) = (b)$.

Definition: A highest common factor (also known as greatest common divisor) of elements a, b of R is an element d with the properties:

(1) $d|a$ & $d|b$ and (2) $c|a$ & $c|b \Rightarrow c|d$.

Highest common factors, II

Note: This general definition is different from the classical definition in $\mathbb{N}$. You should think why they come to essentially the same thing in $\mathbb{N}$.

Note: Highest common factor of a, b is not unique. If d is a highest common factor of a, b then so is any associate of d; conversely, if d_1, d_2 are highest common factors of a, b then $d_1 \sim d_2$.

Note: Nevertheless, we write $d = \mathrm{hcf}(a, b)$.

Note: Highest common factor of a, b does not necessarily exist. Example later.

Irreducible elements, primes

Let R be a commutative ring with 1.

Definition: An element $a \in R$ is said to be irreducible if $a \neq 0$, $a \notin U(R)$, and $a = bc \Rightarrow b \in U(R)$ or $c \in U(R)$.

Definition: An element $a \in R$ is said to be prime if $a \neq 0$, $a \notin U(R)$, and $a|bc \Rightarrow a|b$ or $a|c$.

Important note: In an integral domain primes are always irreducible.

Important note: In many integral domains, but not in all, irreducible elements are prime. Example to come.

An example

Example. Let $R := \mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. Note that $R \leqslant \mathbb{C}$, so R is an integral domain. In R

- there are irreducible elements that are not prime,
- there are elements a, b for which $\mathrm{hcf}(a, b)$ does not exist.

Euclidean rings

Definition: A euclidean ring is an integral domain R equipped with a function $v : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$ such that

(1) $v(ab) \geqslant v(a)$ for all $a, b \in R \setminus \{0\}$, and

(2) for all $a, b \in R$, if $b \neq 0$ then there exist $q, r \in R$ such that $a = qb + r$ and either $r = 0$ or $v(r) < v(b)$.

Note: Thus a euclidean ring has division with remainder.

Examples of euclidean rings

Example 1: $R = \mathbb{Z}$ with $v(a) = |a|$.

Note: To prove division with remainder we use subtraction, but to **find** the quotient q and remainder r we use long division.

Example 2: $R = F[x]$ where F is a field, with $v(f) = \deg f$.

Note: To prove division with remainder and to **find** the quotient q and remainder r we use the Division Algorithm for polynomials (which is a version of long division).

Example 3: R is a field with $v(a) = 0$ for all $a \in R^\times$.

Simple facts about euclidean rings R

Fact 1: *Define* $v_0 := v(1)$. *Then*

(1) $v_0 \leqslant v(a)$ *for all* $a \in R \setminus \{0\}$, *and*

(2) $v(a) = v_0$ *if and only if* $a \in U(R)$.

Proof.

Fact 2: *Let* $b, c \in R$. *If* $c \notin U(R)$ *then* $v(bc) > v(b)$.

Proof.

Fact 2: *Let* $a \in R$. *If* $a \neq 0$ *and* $a \notin U(R)$ *then there exist irreducible elements* $a_1, a_2, \ldots, a_k$ *in* R *such that* $a = a_1\, a_2 \cdots a_k$.

Proof.