Rings & Arithmetic 2: Integral domains and fields

Thursday, 13 October 2005

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

- Units in a ring
- Integral domains; examples
- Fields; examples
- Characteristic of an integral domain
- Field of fractions of an integral domain

Units in a ring

Definition: Let R be a ring (commutative with 1). Element $u \in R$ is said to be a unit if $(\exists v \in R) : uv = 1$.

Note: The set of units of R forms a group under multiplication. It is denoted $U(R)$ (or, sometimes, $R^{\times}$).

Example: $U(\mathbb{Z}) = \{1, -1\}$.

Example: $U(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$.

Zero-divisors

Definition: Element a of ring R is said to be a zero-divisor if:

$$a \neq 0 \text{ and } (\exists b \in R \setminus \{0\}) : ab = 0\,.$$

Example: Let S be a ring (commutative, with 1) and let $R := S \times S$. Elements of the form $(s, 0)$, where $s \in S \setminus \{0\}$, are zero-divisors. Likewise elements of the form $(0, t)$ with $t \neq 0$ are zero-divisors.

Integral domains

Definition: An integral domain is a commutative ring with 1 satisfying

$$
\begin{array}{ll}
(8') & ab = 0 \Rightarrow a = 0 \text{ or } b = 0 \\
(10) & 1 \neq 0
\end{array}
$$

Note: So R is an integral domain if and only if $1 \neq 0$ and there are NO divisors of zero.

Note: Axiom (8′) is equivalent to

$$(8'') \qquad (a \neq 0 \text{ and } ab = ac) \Rightarrow b = c \qquad \text{[cancellation]}.$$

Examples of integral domains

- $\mathbb{Z}$ is an integral domain [the prototype];

- any subring of $\mathbb{Q}$, of $\mathbb{R}$, or of $\mathbb{C}$ is an integral domain;

- if R is an integral domain then so is the polynomial ring $R[x]$ [see Sheet 1, Qn 4(a)];

- the ring $S \times S$ is never an integral domain.

Fields

Definition: A field is a commutative ring F with 1 in which

$$
\begin{array}{rl}
(8) & (\forall a \neq 0)(\exists b \in F)(ab = 1) \\
(10) & 1 \neq 0
\end{array}
$$

Examples: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Note: A ring F (commutative with 1) is a field if and only if $U(F) = F \setminus \{0\}$.

Note: A field is an integral domain.

Note: Axioms (1) – (10) are the Axioms of Arithmetic.

Characteristic of an integral domain

Definition: Let R be an integral domain. Define

$$\operatorname{Char} R := \begin{cases} \text{additive order of 1 if this is finite,} \\ 0 \text{ otherwise.} \end{cases}$$

Theorem: *Let R be an integral domain and let $p := \operatorname{Char} R$.*

(1) *If $p \neq 0$ then p is prime.*

(2) *For all $a \in R \setminus \{0\}$ the additive order of a is p.*

Proof.

Fields of fractions

Observation: Any subring of a field is an integral domain.

Proposition: [Non-examinable, but informative and useful.] *Let R be an integral domain. Then there exists a field F such that $R \leqslant F$.*

Sketch Proof.