Rings & Arithmetic 1: Introduction

Monday, 10 October 2005

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

- Introduction
- Axioms for commutative rings with 1
- Comments and Examples
- New rings from old
- Some basic theorems
- Subrings

Welcome to Second-Year Algebra, I

Lecture plan: Lecture 1 – Lecture 8 = Rings;
Lecture 9 – Lecture 24 = Linear Algebra

Exercise-sheet publication plan:

Week published	for Week	
$\leqslant 1$	2 or 3	Rings & Arithmetic 1
$\leqslant 2$	3 or 4	Rings & Arithmetic 2
$\leqslant 3$	4 or 5	Linear Algebra 1
$\leqslant 4$	6	Linear Algebra 2
$\leqslant 5$	7	Linear Algebra 3
$\leqslant 6$	8	Linear Algebra 4

Welcome to Second-Year Algebra, II

- You = learner = thinker
- tutorial = primary learning and teaching opportunity
- book = main source of ideas and information
- lectures = oral supplement to books

Axioms for commutative rings with 1

Definition: A *commutative ring with unity* is a set R with distinguished elements 0, 1 and with two binary operations $+$ and $\times$ satisfying axioms below ('axioms of arithmetic').

Conventionally:

for the image of (a, b) under the function $+ : R \times R \to R$ we write $a + b$;

for the image of (a, b) under the function $\times : R \times R \to R$ we write ab;

and $x + yz$ means $x + (yz)$.

Some axioms of arithmetic

(1) $a + (b + c) = (a + b) + c$ [+ is associative]

(2) $a + b = b + a$ [+ is commutative]

(3) $a + 0 = a$

(4) $(\forall a \in R)(\exists b \in R)(a + b = 0)$

(5) $a(bc) = (ab)c$ [× is associative]

(6) $ab = ba$ [× is commutative]

(7) $a1 = 1a = a$

(9) $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$

[× distributes over +]

Commentary on the axioms

Note: axioms in the form of equations are to be read as having the appropriate universal quantifier, such as $\forall a, b, c \in R$, in front.

Note: 'closure' axioms have no place here.

Note: for the purposes of this lecture course **ring** will often be used as an abbreviation for **commutative ring with 1**.

Note: in fact, the term ring usually refers to a system satisfying all these axioms except for commutativity of multiplication. Hence the unnecessary clauses in Axioms (7) and (9).

Some examples

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$;

Rings of real-valued functions $\mathbb{R}^X$;

etc., etc., etc.

Non-examples: $2\mathbb{Z}$ [does not contain unit element]

$\mathbb{N}$ [does not contain negatives]

$\mathrm{M}_{n\times n}(\mathbb{R})$ for $n \geq 2$ [non-commutative]

New rings from old

Example: the polynomial ring $R[x]$ where R is a commutative ring with 1

Similarly $R[x_1, x_2, \ldots, x_d]$

Example: the direct product $R \times S$ where R, S are commutative rings with 1

Some basic theorems

(1) if $a + b = 0$ and $a + b' = 0$ then $b = b'$.

Proof

Thus additive inverses are unique: the notation $-a$ is sensible. Note the corollary that if $x + x = x$ then $x = 0$.

(2) $a0 = 0a = 0$ for all $a \in R$.

Proof

(3) $(-a)b = -(ab)$ for all $a, b \in R$.

Proof

Etc., etc., etc.

Subrings

Definition: A *subring* of a ring R (commutative, with 1) is a subset S such that

(i) $0 \in S,\ 1 \in S$;

(ii) $a, b \in S \Rightarrow a + b \in S,\ -a \in S$;

(iii) $a, b \in S \Rightarrow ab \in S$.

Thus a subring is required to be **closed** with respect to the operations of R. We write $S \leqslant R$.

Note: a subset S of a ring R is a subring if and only if $1 \in S$ and S satisfies (ii′) and (iii), where (ii′) says $a, b \in S \Rightarrow a - b \in S$.

Examples of subrings

$\mathbb{Z} \leqslant \mathbb{Q} \leqslant \mathbb{R} \leqslant \mathbb{C}$;

$R \leqslant R[x]$;

etc., etc., etc.