MAS 305 **Algebraic Structures II**

Notes 10 **Autumn 2006**

Ring Theory

A *ring* is a set R with two binary operations $+$ and $*$ satisfying

(a) $(R,+)$ is an Abelian group;

(b) R is closed under $*$;

(c) $*$ is associative;

(d) $*$ is distributive over $+$, which means that

$$(a+b)*c = a*c+b*c$$

and

$$c*(a+b) = c*a+c*b$$

for all a, b, c in R.

The identity for $(R,+)$is written 0_R or 0; the additive inverse of a is $-a$.
We usually write $a*b$ as ab.

Here are some simple consequences of the axioms:

(a) general associativity of multiplication: the product $a_1 * a_2 * \cdots * a_n$ is well defined without parentheses;

(b) $a0_R = 0_Ra = 0_R$ for all a in R (proof: exercise).

A ring R is

a ring with identity if R contains an element 1_R such that $1_R \neq 0_R$ and $a1_R = 1_R a = a$ for all a in R;

a division ring if R has an identity and $(R \setminus \{0_R\}, *)$ is a group;

commutative if $a * b = b * a$ for all a, b in R;

a field if R is a commutative division ring.

If R has an identity and $ab = 1_R$ then b is written a^{-1} and a is called a *unit*. The set of units in a ring with identity forms a group (proof: exercise).

If $ab = 0_R$ but $a \neq 0_R$ and $b \neq 0_R$ then a and b are called *zero-divisors*. A commutative ring with identity and no zero-divisors is an *integral domain*.

Examples

(a) $(\mathbb{Z}, +, \times)$ is an integral domain.

(b) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields.

(c) $\mathbb{Z}_p$ is a field if p is prime.

(d) $\mathbb{Z}_n$ is a commutative ring with identity for all n. If n is not prime then $\mathbb{Z}_n$ has zero-divisors. For example, in $\mathbb{Z}_6$ we have $[2] \times [3] = [0]$.

(e) If R is a ring then the *ring of polynomials* over R, written $R[x]$, is the set of all polynomials with coefficients in R, with the usual addition and multiplication of polynomials. When we need to be formal, we think of a polynomial as being an infinite sequence $(a_0, a_1, a_2, \ldots)$ of elements of R, with the property that there is some n such that $a_j = 0$ if $j > n$. For example, the informal polynomial $2 - x + 5x^2 + 8x^3$ in $\mathbb{Z}[x]$ is the sequence $(2, -1, 5, 8, 0, 0, \ldots)$.

(f) This can be extended to the ring of polynomials in n variables x_1, …, x_n by putting $R[x_1, x_2] = (R[x_1])[x_2]$, …, $R[x_1, \ldots, x_n] = (R[x_1, \ldots, x_{n-1}])[x_n]$.

(g) If $(G, +)$ is any Abelian group then we can turn G into a *zero ring* by putting $g * h = 0_G$ for all g, h in G.

(h) If R is a ring then $M_n(R)$ is the ring of all $n \times n$ matrices with entries in R, with the usual addition and multiplication of matrices. If $n \geqslant 2$ then $M_n(R)$ is not commutative (unless R is a zero ring) and $M_n(R)$ contains zero-divisors.

Sums

If a is an element of a ring R and m is a positive integer then

$$\begin{array}{rcl} ma & \text{denotes} & \underbrace{a+a+\cdots+a}_{m \text{ times}} \\ (-m)a & \text{denotes} & -(ma). \end{array}$$

Then $na+ma=(n+m)a$ for all integers n, m.

Subrings and ideals

Definition A subset S of a ring R is a *subring* of R if it is a ring under the same operations. We write $S \leqslant R$.

The Subring Test If R is a ring and $S \subseteq R$ then S is a subring of R if

(a) $(S,+)$ is a subgroup of $(R,+)$, and

(b) $s*t \in S$ for all s, t in S.

If S is a subring of R then $0_S = 0_R$; but if R has an identity 1_R then S might contain no identity or S might have an identity 1_S different from 1_R.

Example Put $R = M_2(\mathbb{Z})$ and

$$S = \left\{ \begin{bmatrix} n & 0 \\ 0 & 0 \end{bmatrix} : n \in \mathbb{Z} \right\}.$$

Then $S \leqslant R$, $1_R = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \notin S$ and $1_S = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$.

Definition A subset S of a ring R is an *ideal* of R if S is a subring of R and $s*r \in S$ and $r*s \in S$ for all s in S and all r in R. We write $S \trianglelefteq R$.

$\{0_R\}$ is an ideal of R.
R is an ideal of itself.
If R has an identity 1_R and S is an ideal of R and $1_R \in S$ then $S = R$.

If R is commutative with an identity and $a \in R$ then $\{ar : r \in R\}$ is an ideal of R, called aR. It is the smallest ideal of R containing a, so it is also written $\langle a \rangle$.

In a general ring, the *principal ideal* $\langle a \rangle$ is

$$\left\{ na + r_0a + as_0 + \sum_{i=1}^{m} r_i a s_i : n, m \in \mathbb{Z},\ m \geqslant 0,\ r_i, s_i \in R \right\}.$$

Example $\mathbb{Z}$ is a commutative ring with identity. $2\mathbb{Z}$ is a principal ideal of $\mathbb{Z}$; it has no identity. The integer 4 is in $2\mathbb{Z}$ and $4\mathbb{Z}$ is a principal ideal of $2\mathbb{Z}$ but $4(2\mathbb{Z}) = 8\mathbb{Z} \neq 4\mathbb{Z}$.

Example For any integer m, $m\mathbb{Z} \trianglelefteq \mathbb{Z}$ and $M_2(m\mathbb{Z}) \trianglelefteq M_2(\mathbb{Z})$.

Lemma If I and J are ideals of a ring R, then so is $I \cap J$. In fact, the intersection of any non-empty collection of ideals of R is itself an ideal of R.

Proof Exercise.

If $A \subseteq R$ then R is an ideal containing A. By the lemma, the intersection of all the ideals containing A is itself an ideal—the smallest ideal containing A. It is written $\langle A \rangle$ (or (A) in some books).

Quotient rings

If S is a subring of R then it is a subgroup under addition, so it has cosets. Because addition is commutative, right cosets are the same as left cosets. The coset containing the element a is $\{s+a : s \in S\}$, which is written $S+a$. We know that we can define addition on cosets by

$$(S+a)+(S+b) = S+(a+b).$$

This makes the set of cosets into an Abelian group. Now we want to define multiplication of cosets in such a way that the cosets form a ring.

Theorem If S is an ideal of R, then we can define multiplication of cosets of S by

$$(S+a)*(S+b) = S+ab.$$

This is well defined, and makes the set of cosets into a ring, called the *quotient ring* R/S.

Proof Suppose that $S+a_1 = S+a_2$ and $S+b_1 = S+b_2$. Then $a_2 - a_1 = s_1 \in S$ and $b_2 - b_1 = s_2 \in S$, and

$$a_2b_2 = (s_1+a_1)(s_2+b_1) = s_1s_2 + a_1s_2 + s_1b_1 + a_1b_1.$$

The first three terms are in S, so so is their sum, so $a_2b_2 - a_1b_1 \in S$ and therefore $S + a_2b_2 = S + a_1b_1$. So multiplication is well defined, and the set of cosets is closed under multiplication.

For a, b, c in R:

$$\begin{aligned}((S+a)*(S+b))*(S+c) &= (S+ab)*(S+c)\\ &= S+(ab)c\\ &= S+a(bc)\\ &= (S+a)*(S+bc)\\ &= (S+a)*((S+b)*(S+c)),\end{aligned}$$

so multiplication is associative.

Moreover,

$$\begin{aligned}((S+a)+(S+b))*(S+c) &= (S+(a+b))*(S+c)\\ &= S+(a+b)c\\ &= S+(ac+bc)\\ &= (S+ac)+(S+bc)\\ &= (S+a)*(S+c)+(S+b)*(S+c),\end{aligned}$$

and, similarly,

$$(S+c)*((S+a)+(S+b)) = (S+c)*(S+a)+(S+c)*(S+b),$$

so multiplication is distributive over addition.

Therefore R/S is a ring. $\square$

Example Given m in $\mathbb{Z}$ with $m > 0$, we get $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$.

Ideals in matrix rings

Theorem Let R be a ring.

(a) If I is an ideal of R then $M_n(I)$ is an ideal of $M_n(R)$.

(b) If R has an identity and J is an ideal of $M_n(R)$ then there is some ideal I of R such that $J = M_n(I)$.

Proof (a) (i) Every ideal I contains 0_R, so the zero matrix is in $M_n(I)$ for every ideal I; in particular, $M_n(I)$ is not empty.

(ii) If A and B are in $M_n(I)$ with $A = [a_{ij}]$ and $B = [b_{ij}]$ then $a_{ij} \in I$ and $b_{ij} \in I$ so $a_{ij} - b_{ij} \in I$ for $1 \leqslant i, j \leqslant n$ and so $A - B \in I$.

(iii) If $C \in M_n(R)$ and $A \in M_n(I)$ then every entry of CA has the form $\sum_j c_{ij}a_{jk}$. Each term $c_{ij}a_{jk}$ is in I, because $c_{ij} \in R$ and $a_{ij} \in I$. The sum of elements of I is itself an element of I, so every entry of CA is in I: hence $CA \in M_n(I)$. Similarly, every entry of AC is in I, and so $AC \in M_n(I)$.

(b) Let E_{ij} be the matrix in $M_n(R)$ with (i,j)-th entry equal to 1_R and all other entries equal to 0_R. If $A = [a_{ij}]$ then

$$E_{ki}A = \begin{array}{cl} \begin{bmatrix} 0 & \dots & 0 \\ 0 & \dots & 0 \\ \vdots & \vdots & \vdots \\ \multicolumn{3}{c}{i\text{-th row of } A} \\ \vdots & \vdots & \vdots \\ 0 & \dots & 0 \end{bmatrix} & \begin{array}{l} \\ \\ \\ \leftarrow \text{row } k \\ \\ \\ \end{array} \end{array}$$

so

$$E_{ki}AE_{jl} = \begin{array}{cl} \begin{bmatrix} 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & \dots & 0 & a_{ij} & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 \end{bmatrix} & \begin{array}{l} \\ \\ \\ \leftarrow \text{row } k \\ \\ \\ \\ \end{array} \\ \begin{array}{ccccccc} & & & \uparrow & & & \\ & & & \text{column } l & & & \end{array} & \end{array} = a_{ij}E_{kl}.$$

Let $J \trianglelefteq M_n(R)$, and put

$$I = \{a \in R : a \text{ is an entry in any matrix in } J\}.$$

Then $J \subseteq M_n(I)$, and $I \neq \emptyset$.

If $A \in J$ then $E_{ki}AE_{jl} \in J$ so if $a \in I$ then $aE_{kl} \in J$ for $1 \leqslant k, l \leqslant n$. In particular, $aE_{11} \in J$. If a and b are in I then $aE_{11} \in J$ and $bE_{11} \in J$, so $aE_{11} - bE_{11} \in J$ so $(a-b)E_{11} \in J$ so $a - b \in I$; and if $r \in R$ then $(rE_{11})(aE_{11}) \in J$ so $raE_{11} \in J$ so $ra \in I$, and $(aE_{11})(rE_{11}) \in J$ so $arE_{11} \in J$ so $ar \in I$. Hence $I \trianglelefteq R$.

If $A = [a_{ij}]$ with each a_{ij} in I then $a_{ij}E_{ij} \in J$ for $1 \leqslant i, j \leqslant n$, but $A = \sum_i \sum_j a_{ij}E_{ij}$ so $A \in J$, so $M_n(I) \subseteq J$. Therefore $J = M_n(I)$. $\square$

Simple rings

Definition A ring R is *simple* if

(a) $\{rs : r \in R,\ s \in R\} \neq \{0_R\}$ and

(b) the only ideals of R are $\{0_R\}$ and R.

If R has an identity then (a) is always satisfied.
If R is a field (or a division ring) then R is simple.

Corollary to preceding Theorem If R is a simple ring with identity then $M_n(R)$ is simple. In particular, if F is a field then $M_n(F)$ is simple.