Algebraic Terminology

UCSD Math 15A, CSE 20 (S. Gill Williamson)

Contents

1 Semigroup

We use the notation $\mathbb{N} = \{1, 2, \ldots, \}$ for the positive integers. Let $\mathbb{N}_0 = \{0, 1, 2, \ldots, \}$ denote the nonnegative integers, and let $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ denote the set of all integers. Let $\times^n S$ (n-fold Cartesian product of S) be the set of n-tuples from a nonempty set S. We also write S^n for this product.

Semigroup→Monoid→Group: a set with one binary operation

A function $w : S^2 \to S$ is called a *binary operation*. It is sometimes useful to write $w(x, y)$ in a simpler form such as $x\,w\,y$ or simply $x \cdot y$ or even just xy. To tie the binary operation w to S explicitly, we write (S, w) or $(S, \cdot)$.

Definition 1.1 (Semigroup). Let $(S, \cdot)$ be a nonempty set S with a binary operation "$\cdot$" . If $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, for all $x, y, z \in S$, then the binary operation "$\cdot$" is called *associative* and $(S, \cdot)$ is called a *semigroup*. If two elements, $s, t \in S$ satisfy $s \cdot t = t \cdot s$ then we say s and t *commute*. If for all $x, y \in S$ we have $x \cdot y = y \cdot x$ then $(S, \cdot)$ is a *commutative* (or *abelian*) semigroup.

Remark 1.2 **(Semigroup).** Let $S = \mathbf{M}_{2,2}(\mathbb{Z}_e)$ be the set of 2×2 matrices with entries in $\mathbb{Z}_e = \{0, \pm 2, \pm 4, \ldots\}$, the set of even integers. Define $w(X, Y) = XY$ to be the standard multiplication of matrices (which is associative). Then (S, w) is a semigroup. This semigroup is not commutative. The semigroup of even integers, $(\mathbb{Z}_e, \cdot)$, where "$\cdot$" denotes multiplication of integers, is commutative.

Associative* + *Identity* = *Monoid

2 Monoid

Definition 2.1 (Monoid). Let $(S, \cdot)$ be a semigroup. If there exists an element $e \in S$ such that for all $x \in S$, $e \cdot x = x \cdot e = x$, then e is called an *identity* for the semigroup. A semigroup with an identity is called a *monoid*. If $x \in S$ and there is a $y \in S$ such that $x \cdot y = y \cdot x = e$ then y is called an *inverse* of x.

Remark 2.2 **(Monoid).** The identity is unique (i.e., if e and e' are both identities then $e = e \cdot e' = e'$). Likewise, if y and y' are inverses of x, then $y' = y' \cdot e = y' \cdot (x \cdot y) = (y' \cdot x) \cdot y = e \cdot y = y$ so the inverse of x is unique. The 2×2 matrices, $\mathbf{M}_{2,2}(\mathbb{Z})$, with matrix multiplication form a monoid (identity I_2, the 2×2 identity matrix).

Associative* + *Identity* + *Inverses* = *Group

3 Group

Definition 3.1 (Group). Let $(S, \cdot)$ be a monoid with identity e and let $x \in S$. If there is a $y \in S$ such that $x \cdot y = y \cdot x = e$ then y is called an *inverse* of x (see 2.1). A monoid in which every element has an inverse is a *group*.

Remark 3.2 **(Group).** The mathematical study of groups is a vast subject. Commutative groups, $x \cdot y = y \cdot x$ for all x and y, play an important role. They are also called *abelian* groups. Note that the inverse of an element x in a group is unique: if y and y' are inverses of x, then $y' = y' \cdot e = y' \cdot (x \cdot y) = (y' \cdot x) \cdot y = e \cdot y = y$ (see 2.2).

Ring: one set with two intertwined binary operations

4 Ring and Field

Definition 4.1 (Ring and Field). A *ring*, $(S, +, \cdot)$, is a set with two binary operations such that $(S, +)$ is an abelian group ("$+$" is called "addition") and $(S - \{0\}, \cdot)$ is a semigroup ("$\cdot$" is called "multiplication"). The two operations are related by distributive rules which state that for all x, y, z in S:

$$\textbf{(left)} \quad z \cdot (x + y) = z \cdot x + z \cdot y \quad \text{and} \quad (x + y) \cdot z = x \cdot z + y \cdot z \quad \textbf{(right)}.$$

Remark 4.2 **(Notation and special rings)**. The identity of the abelian group $(S,+)$ is denoted by "0" and is called the *zero* of the ring $(S,+,\cdot)$. If $(S-\{0\},\cdot)$ is a monoid then $(S,+,\cdot)$ is a *ring with identity*. If $(S-\{0\},\cdot)$ is commutative then $(S,+,\cdot)$ is *a commutative ring*. If $(S-\{0\},\cdot)$ is a group then the ring is called a *skew-field* or *division ring*. If this group is *abelian* then the ring is called a *field*.

Remark 4.3 **(Basic ring identities)**. We have taken the point of view that a semigroup, $(S,\cdot)$, has S nonempty (1.1). Thus, the semigroup $(S-\{0\},\cdot)$ of a ring (4.1) has $S-\{0\}$ nonempty. If r,s,t are in a ring $(S,+,\cdot)$ then the following basic identities (in braces, plus hints for proof) hold:

(1) $\{r\cdot 0 = 0\cdot r = 0\}$: If $x+x=x$ then $x=0$. Take $x=r\cdot 0$ and $x=0\cdot r$.

(2) $\{(-r)\cdot s = r\cdot(-s) = -(r\cdot s)\}$: $r\cdot s+(-r)\cdot s = 0 \implies (-r)\cdot s = -(r\cdot s)$.

(3) $\{(-r)\cdot(-s) = r\cdot s\}$: Replace r by $-r$ in **(2)**. Note that $-(-r)=r$.

Using the identities of Remark 4.3, you can show that if $(S-\{0\},\cdot)$ has an identity e, then $(-e)\cdot a = -a$ for any $a\in S$ and, taking $a=-e$, $(-e)\cdot(-e)=e$. It is convenient to define $r-s=r+(-s)$. Then we have $t\cdot(r-s)=t\cdot r-t\cdot s$ and $(r-s)\cdot t = r\cdot t - s\cdot t$.

A field is a ring $(S,+,\cdot)$ ***where*** $(S-\{0\},\cdot)$ ***is an abelian group***

Remark 4.4 **(Ring and Field)**. The 2×2 matrices over the even integers, $\mathbf{M}_{2,2}(\mathbb{Z}_e)$, with the usual multiplication and addition of matrices, is a noncommutative ring *without an identity*. The matrices, $\mathbf{M}_{2,2}(\mathbb{Z})$, over all integers, is a noncommutative ring *with identity*. The ring of 2×2 matrices of the form $\begin{pmatrix} x & y \\ -\overline{y} & \overline{x} \end{pmatrix}$ where x and y are complex numbers is a skew-field but not a field. This skew-field is equivalent to (i.e, a "matrix representation of") the *skew field of quaternions* (see Wikipedia article on quaternions). The most important fields for us will be the fields of real and complex numbers.

5 Ideal

Definition 5.1 (Ideal). Let $(R,+,\cdot)$ be a ring and let $A\subseteq R$ be a nonempty subset of R. If $(A,+,\cdot)$ is a ring, then it is called a *subring* of $(R,+,\cdot)$. A subring $(A,+,\cdot)$ is a *left ideal* if for every $x\in R$ and $y\in A$, $xy\in A$. A *right ideal* is similarly defined. If $(A,+,\cdot)$ is both a left and right ideal then it is a *two-sided ideal* or, simply, an *ideal*. Note that if $(R,+,\cdot)$ is commutative then all ideals are two sided.

Remark 5.2 **(Ideal)**. The set of all matrices of the form $a = \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}$ is a subring of $\mathbf{M}_{2,2}(\mathbb{Z})$. This subring, which has no identity element, is a right ideal but not a left ideal. It also has *zero divisors* - elements $a \neq 0$ and $b \neq 0$ such that $a \cdot b = 0$. Another example of an ideal is the set of even integers, $\mathbb{Z}_e$, which is a subring of the ring of integers, $\mathbb{Z}$ (which, it is worth noting, has *no zero divisors*). The subring, $\mathbb{Z}_e$, is an ideal (two-sided) in $\mathbb{Z}$. Given any integer $n \neq 0$, the set $\{k \cdot n \mid k \in \mathbb{Z}\}$ of multiples of n, is an ideal of the ring $\mathbb{Z}$ which we denote by $(n) = n\mathbb{Z} = \mathbb{Z}n$. Such an ideal (i.e., generated by a single element, n) in $\mathbb{Z}$ is called a *principal ideal*. It is easy to see that all ideals in $\mathbb{Z}$ are principal ideals. Another nice property of integers is that they *uniquely factor* into primes (up to order and sign).

6 Integral domain

Algebraists have defined a number of important abstractions of the ring of integers, $\mathbb{Z}$. We next discuss four such abstractions: integral domain, principal ideal domain (PID), unique factorization domain (UFD), and Euclidean domains - each more restrictive than the other.

$$\boxed{\textit{Euclidean Domain} \implies \textit{PID} \implies \textit{UFD}}$$

Definition 6.1 (Integral domain). An *integral domain* is a commutative ring with identity, $(R, +, \cdot)$, with no zero divisors (5.2). We denote the identity of $(R - \{0\}, \cdot)$ by 1_R or, simply, 1.

Definition 6.2 (Characteristic of a ring). Let R be a ring. Given $a \in R$ and an integer $n > 0$, define $na \equiv a + a + \cdots a$ where there are n terms in the sum. If there is an integer $n > 0$ such that $na = 0$ for all $a \in R$ then the *characteristic* of R is the least such n. If no such n exists, then R has *characteristic zero*.

Remark 6.3 **(Divisors, associates and primes)**. If b, c and a are elements of an integral domain R such that $a \neq 0$ and $b = a \cdot c$ then we say that a *divides* b (written $a \mid b$) or a *is a divisor of* b. An element u in $R - \{0\}$ is an *invertible element* or a *unit of* R if u has an inverse in $(R - \{0\}, \cdot)$. Two elements, a and b, of R are *associates in* R if $a = b \cdot u$ where u is a unit. An element p in $R - \{0\}$ is *irreducible* if $p = a \cdot b$ implies that either a or b is invertible and *prime* if $p \mid a \cdot b$ implies $p \mid a$ or $p \mid b$. For unique factorization domains (6.4), p is irreducible if and only if it is prime. In the ring $\mathbb{Z}$, the only invertible elements are $\{+1, -1\}$. The only associates of an integer $n \neq 0$ are $+n$ and $-n$. The integer $12 = 3 \cdot 4$ is the product of two non-invertible elements so 12 is not irreducible (i.e., reducible) or, equivalently in this case, not a prime. The integer 13 is a prime with the two associates +13 and −13. A field is an integral domain in which every nonzero element is invertible. In a field,

if $0 \neq p = a\dot{b}$ then *both* a and b are nonzero and hence both are invertible (and "at least one is invertible" is satisfied) which implies that every nonzero element in a field is irreducible.

Definition 6.4 (Unique factorization domain). An integral domain R is a *unique factorization domain* (UFD) if

(1) Every nonzero and non-invertible $a \in R$ can be factored into a finite product of irreducibles (6.3).

(2) If $a = p_1 \cdots p_r$ and $a = q_1 \cdots q_s$ are two such factorizations then $r = s$ and the q_i can be reindexed so that p_i and q_i are associates for $i = 1, \ldots, s$.

Remark 6.5 **(Unique factorization domains).** The integers, $\mathbb{Z}$, are a unique factorization domain. Every field is also a unique factorization domain ($r = s = 1$ in (2) of 6.4). If R is a UFD then so are the polynomial rings $R[x]$ and $R[x_1, \ldots, x_n]$. If $a_1, \ldots, a_n$ are nonzero elements of a UFD, then there exists a greatest common divisor $d = \gcd(a_1, \ldots, a_n)$ which is unique up to multiplication by units.

Definition 6.6 (Principal ideal domain). An integral domain R is a *principal ideal domain* (PID) if every ideal in R is a principal ideal (5.2).

Remark 6.7 **(Principal ideal domains).** We noted in Remark 5.2 that every ideal in $\mathbb{Z}$ is a principal ideal. If $(F, +, \cdot)$ is a field, then any subring, $(A, +, \cdot)$, contains a nonzero and hence invertible element a. The ideal $(a) = F$. There is only one ideal in a field and that is a principal ideal that equals F. Thus, any field F is a PID. Let $a_1, \ldots, a_n$ be nonzero elements of a PID, R. It can be shown that if $d = \gcd(a_1, \ldots, a_n)$ in R then there exists $r_1, \ldots, r_n$ in R such that $r_1 a_1 + \cdots + r_n a_n = d$. The ring of polynomials in two variables (or more) over a field, $F[x_1, \ldots x_n]$, is not a PID. Also, the ring of polynomials with integral coefficients, $Z[x]$, is not a PID.

7 Euclidean domain

Definition 7.1 (Euclidean valuation). A function ν from the nonzero elements of an integral domain R to the nonnegative integers, N_0, is a *valuation* on R if

(1) For all $a, b \in R$ with $b \neq 0$, there exist q and r in R such that $a = b \cdot q + r$ where either $r = 0$ or $\nu(r) < \nu(b)$.

(2) For all $a, b \in R$ with $a \neq 0$ and $b \neq 0$, $\nu(a) \leq \nu(a \cdot b)$.

Definition 7.2 (Euclidean domain). An integral domain R is a *Euclidean domain* if there exists a Euclidean valuation on R (see 7.1)

Remark 7.3 **(Euclidean domains)**. For the three integral domain types just discussed, it can be shown that every Euclidian domain is a principal ideal domain and every principal ideal domain is a unique factorization domain. The integers $\mathbb{Z}$ are a Euclidean domain with $\nu(n) = |n|$. The polynomials with real numbers as coefficients, $\mathbb{R}[x]$, form a Euclidean domain with $\nu(p(x))$ the degree of $p(x)$. Any field $(F, +, \cdot)$ is a Euclidean domain with $\nu(x) = 1$ for all nonzero x. But, the ring of polynomials with integral coefficients, $\mathbb{Z}[x]$, is not a PID (6.7) and thus not a Euclidean domain. Likewise, the ring of polynomials in n variables, $n > 1$, over a field F, $F[x_1, \ldots, x_n]$, is not a PID (6.7) and hence not a Euclidean domain. Rings that are PIDs but not Euclidean domains are rarely discussed (the ring $\mathbb{Z}[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Z},\ \alpha = (1 + (19)^{1/2}i)\}$ is an example).

We now combine a ring with an abelian group to get a module.

8 Module

Definition 8.1 (Module). Let $(R, +, \cdot)$ be a ring with identity 1_R. Let $(M, \oplus)$ be an abelian group. We define an operation with domain $R \times M$ and range M which for each $r \in R$ and $x \in M$ takes (r, x) to rx (juxtaposition of r and x). This operation, called *scalar multiplication*, defines a *left R-module M* if the following hold for every $r, s \in R$ and $x, y \in M$:

(1) $r(x \oplus y) = rx \oplus ry$ (2) $(r + s)x = rx \oplus sx$ (3) $(r \cdot s)x = r(sx)$ (4) $1_R x = x$.

Usually, we simply say "M is an R-module," the "left" being understood. We also use "+" for the addition in both abelian groups and replace "$\cdot$" with juxtaposition. Thus, we have: (2) $(r + s)x = rx + sx$ (3) $(rs)x = r(sx)$.

What we call a "module" is sometimes called a "unitary module." In that case, a "module" does not need to have an identity, 1_R.

Remark 8.2 **(Module).** Let R be the ring of 2×2 matrices over the integers, $\mathbf{M}_{2,2}(\mathbb{Z})$. Let M be the abelian group, $\mathbf{M}_{2,1}(\mathbb{Z})$, of 2×1 matrices under addition. Then (1) and (2) correspond to the distributive law for matrix multiplication, (3) is the associative law, and (4) is multiplication on the left by the 2×2 identity matrix. Thus, $\mathbf{M}_{2,1}(\mathbb{Z})$ is an $\mathbf{M}_{2,2}(\mathbb{Z})$-module.

9 Vector space and algebra

Definition 9.1 (Vector space and algebra). If an abelian group $(M, +)$ is an F-module where F is a field (4.4), then we say $(M, +)$ (or, simply, M) is a *vector space over F* (or M is an F *vector space*). Suppose $(M, +, \cdot)$ is a ring where $(M, +)$ is a vector space over F and where the following "scalar rule" holds,

scalar rule: for all $\alpha \in F$, $a, b \in M$ we have $\alpha(a \cdot b) = (\alpha a) \cdot b = a \cdot (\alpha b)$.

Then $(M, +, \cdot)$ is an *algebra over* F (or M is an F *algebra*).

Remark 9.2 (**Complex matrix algebra**). Let $\mathbb{C}$ be the field of complex numbers and let M be $\mathbf{M}_{2,2}(\mathbb{C})$, the additive abelian group of 2×2 matrices with complex entries. Conditions (1) to (4) of 8.1 are familiar properties of multiplying matrices by scalars (complex numbers). Thus, M is a complex vector space or, alternatively, M is a vector space over the field of complex numbers, $\mathbb{C}$. If we regard M as the ring, $\mathbf{M}_{2,2}(\mathbb{C})$, of 2×2 complex matrices using the standard multiplication of matrices, then it follows from the definitions of matrix multiplication and multiplication by scalars that the scalar rule of 9.1 holds, and $\mathbf{M}_{2,2}(\mathbb{C})$ is an algebra over $\mathbb{C}$.

10 Notational conventions

Remark 10.1 (**Special notation**). Let $\mathbb{K} \in \{\mathbb{Z}, \mathbb{F}[x]\}$ where $\mathbb{Z}$ denotes the integers and $\mathbb{F}[x]$ the polynomials over a field $\mathbb{F}$ which will be either $\mathbb{Q}$ (rational numbers), $\mathbb{R}$ (real numbers) or $\mathbb{C}$ (complex numbers). Thus, $\mathbb{F} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. Note that $\mathbb{K}$ is a Euclidean domain. A general theorem in algebra says that any integral domain can, like the integers, be extended to a quotient field. For $\mathbb{Z}$, the quotient field is the rational numbers, $\mathbb{Q}$. For the Euclidean domains $\mathbb{F}[x]$, the quotient field is all rational functions over $\mathbb{F}$ (ratios of polynomials with coefficients in $\mathbb{F}$) which we denote by $\mathbb{F}(x)$ (parentheses instead of $\mathbb{F}[x]$).