MAT 511 **Notes on rings, modules, and representations**
November 16, 2017

# 1 Rings and fields

**Definition 1.1.** A *ring* is a triple $(R, +, \cdot)$ consisting of a set $R$ and two binary operations $+$ and $\cdot$ on $R$, such that (i) $(R, +)$ is an abelian group (with identity element $0_R$); (ii) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in R$; (iii) $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(x + y) \cdot z = x \cdot z + y \cdot z$ for all $x, y, z \in R$. $R$ is a *ring with* 1 if there is an element $1_R \in R$ such that $1_R \cdot x = x = x \cdot 1_R$ for all $x \in R$. $R$ is *commutative* if $x \cdot y = y \cdot x$ for all $x, y \in R$. $\square$

We will assume all rings have 1, unless otherwise stated. It is easily proven from the axioms that $1_R$ is unique, $0_R \cdot x = 0_R = x \cdot 0_R$ and $-x = (-1_R) \cdot x$ for all $x \in R$. We usually assume without mention that $0_R \neq 1_R$, which is the case unless $R = \{0_R\}$. We will usually drop the $\cdot$ and write $xy$ for $x \cdot y$.

**Definition 1.2.** An element $x \in R$ is a *unit* if there exists $y \in R$ such that $xy = yx = 1_R$. $\square$

The set of units of $R$ is denoted $U(R)$; it is a group under $\cdot$. $0_R$ is not a unit (assuming $0_R \neq 1_R$). If $x \in U(R)$, the element $y$ satisfying $xy - 1_R = yx$ is unqiuely determined by $x$, and is deonted $x^{-1}$.

**Definition 1.3.** A *division ring* is a ring satisfying $U(R) = R - \{0_R\}$. A *field* is a commutative division ring. $\square$

Examples of rings:

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, the usual addition and multiplication; the latter three are fields.
- $\mathbb{Z}_n$ under addition and multiplication modulo $n$; these are commutative rings; $U(\mathbb{Z}_n)$ consists of the residue classes $k$ for which $k$ and $n$ are relatively prime, hence $\mathbb{Z}_n$ is a field if and only if $n$ is prime.
- the set $M_n(R)$ of all $n \times n$ matrices with entries in a ring $R$, with addition and multiplication of such $n \times n$ matrices defined using the usual formulas for matrices with real entries - this is a non-commutative ring, even if $R$ is commutative. The group of units $U(M_n(R))$ consists of the invertible $n \times n$ matrices with entries in $R$, and is denoted $\mathrm{GL}_n(R)$, called the *general linear group* of $R$.
- the set $R[x]$ of polynomials in one variable $x$ and coefficients in a ring $R$; if $R$ is commutative this is a commutative ring.
- the set $R[x_1, \ldots, x_n]$ of polynomials in variables $x_1, \ldots, x_n$ and coefficients in a ring $R$; if $R$ is commutative this is a commutative ring.

- the set $\mathbb{C}z$ of convergent power series in one complex variable $z$ is a ring under addition and multiplication of power series. This is a commutative ring.

There is a famous division ring called *the quaternions*[1] $\mathbb{H}$, (for W.R. Hamilton, who invented or discovered them), consisting of the vector space $\mathbb{R}^4$ with basis labelled 1, $i$, $j$, $k$ and multiplication defined as in the quaternion group $Q_8$, and extended linearly. In particular $ij = k = -ji$ so $\mathbb{H}$ is not a field. A well-known theorem of Wedderburn states that any finite division ring is a field.

**Definition 1.4.** Let $R$ be a ring and $G$ a group. The *group ring* of $G$ over $R$ is the set $R[G]$ of finite "linear combinations" $\sum_{g\in G} gc_g$, where $c_g \in R$ for $g \in G$ (and $c_g = 0_R$ for all but finitely many $g$), with addition defined by "combining like terms" and multiplication defined using the multiplication in $G$ and extending linearly. $\square$

The group ring $R[G]$ is a ring with 1, which is commutative if and only if $G$ is abelian. A more formal definition of $R[G]$ will be given in the next section.

**Definition 1.5.** Let $R$ be a ring. The *trace* of a matrix $A = \left[a_{ij}\right] \in M_n(R)$ is $\operatorname{tr}(A) := \sum_{i=1}^n a_{ii}$. $\square$

**Theorem 1.6.** *Suppose $R$ is commutative. For any $A, B \in M_n(R)$, $\operatorname{tr}(AB) = \operatorname{tr}(BA)$.*

*Proof.* By definition of matrix multiplication, the $(i, j)$ entry of $AB$ is $\sum_{k=1}^n a_{ik}b_{kj}$. Then

$$\begin{aligned}\operatorname{tr}(AB) &= \sum_{i=1}^n \sum_{k=1}^n a_{ik}b_{ki} \\ &= \sum_{k=1}^n \sum_{i=1}^n b_{ki}a_{ik} \\ &= \sum_{i=1}^n \sum_{k=1}^n b_{ik}a_{ki} \\ &= \operatorname{tr}(BA),\end{aligned}$$

by interchange of the order of summation (and re-indexing). $\square$

**Corollary 1.7.** *Suppose $R$ is commutative. If $A \in M_n(R)$ and $P \in M_n(R)$ is a unit, then $\operatorname{tr}(A) = \operatorname{tr}(P^{-1}AP)$.*

*Proof.* By the previous theorem,

$$\begin{aligned}\operatorname{tr}(P^{-1}AP) &= \operatorname{tr}\left(P^{-1}(AP)\right) \\ &= \operatorname{tr}\left((AP)P^{-1})\right) \\ &= \operatorname{tr}(A).\end{aligned}$$

$\square$

[1] see https://en.wikipedia.org/wiki/History_of_quaternions

**Definition 1.8.** Let $R$ be a ring. A *subring* of $R$ is an additive subgroup $S$ of $R$ satisfying $xy \in S$ for all $x, y \in S$. A *right ideal* of $R$ is a subring $I$ satisfying the stronger requirement $xr \in I$ for all $x \in I$ and $r \in R$. A *(two-sided) ideal* of $R$ is a right ideal $I$ of $R$ that satisties the additional requirement $rx \in I$ for all $x \in I$ and $r \in R$.

Examples of subrings and ideals:

- $\mathbb{Z}$ is a subring of $\mathbb{Q}$ is a subring of $\mathbb{R}$ is a subring of $\mathbb{C}$. None of these are (right) ideals.
- for any $n \in \mathbb{Z}$, the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$ is an ideal.
- if $S$ is a subring (resp., ideal) of $R$, then $M_n(S)$ is a subring (resp., ideal) of $M_n(R)$.

**Definition 1.9.** Let $R$ and $S$ be rings. A *ring homomorphism* of $R$ to $S$ is a homomorphism $\varphi\colon R \to S$ of the underlying abelian groups that satisfies $(xy)\varphi = (x)\varphi(y)\varphi$ for all $x, y \in R$.

**Theorem 1.10.** *If $\varphi\colon R \to S$ is a ring homomorphism, then $\ker(\varphi)$ is a two-sided ideal of $R$ and $\operatorname{im}(\varphi)$ is a subring of $S$.* □

Let $R$ be a ring and let $I$ be a two-sided ideal of $R$. Then the quotient abelian group $R/I$ has a well-defined multiplication defined by $(I + x)(I + y) := I + xy$, making $R/I$ into a ring, called the *quotient of $R$ by $I$.*

**Theorem 1.11.** *($1^{st}$ isomorphism theorem for rings) If $\varphi\colon R \to S$ is a ring homomorphism, then $\varphi$ induces an isomorphism $\bar{\varphi}\colon R/\ker(\varphi) \to \operatorname{im}(\varphi)$.* □

## 2 Modules and vector spaces

Let $R$ be a ring (with 1).

**Definition 2.1.** A *(right) $R$-module* is an abelian group $M$ equipped with a "scalar" multiplication operation $\cdot\colon M \times R \to M$, denoted $(x, r) \mapsto x \cdot r$, satisfying (i) $(x + y) \cdot r = x \cdot r + y \cdot r$, (ii) $x \cdot (r + s) = x \cdot r + x \cdot s$, and (iii) $(x \cdot r) \cdot s = x \cdot (rs)$, for all $x, y \in M$ and $r, s \in R$. $M$ is *unital* if, in addition, (iv) $x \cdot 1_R = x$ for all $x \in M$. If $R$ is a field, a unital (right) $R$-module is called a (right) *$R$-vector space.* □

Examples of $R$-modules:

- every abelian group $M$ has a natural structure as a $\mathbb{Z}$-module, with $x \cdot n$ defined to equal $nx$, for $x \in M$ and $n \in \mathbb{Z}$.
- if $R$ is a ring, then the cartesian product $R^n$ has a natural structure as an $R$-module, with addition and scalar multiplication defined coordinate-wise just as in the familiar special case of the real vector space $\mathbb{R}^n$. This is called the *free $R$-module of rank $n$.*
- if $G$ is a group, $\Bbbk$ is a field, and $\mathcal{X}\colon G \to \mathrm{GL}_n(\Bbbk); g \mapsto (g)\mathcal{X}$ is a homomorphism (i.e., $\mathcal{X}$ is a $\Bbbk$-*representation* of $G$), then the $\Bbbk$-vector space $\Bbbk^n$ has the structure of a $\Bbbk[G]$-module, with scalar multiplication defined by

$$v \cdot (\sum_{g \in G} g c_g) = \sum_{g \in G} v\left((g)\mathcal{X} c_g\right),$$

for $v \in \Bbbk^n$ identified with a $1 \times n$ (row) matrix with entries in $\Bbbk$. Conversely, any $\Bbbk[G]$-module structure on $\Bbbk^n$ determines a $\Bbbk$-representation of $G$, using the fact that $\mathrm{GL}_n(\Bbbk)$ is a subset of the ring $M_n(\Bbbk)$, via

$$(g)\mathcal{X} = \begin{bmatrix} e_1 \cdot g \\ \hline \vdots \\ \hline e_n \cdot g \end{bmatrix},$$

where $e_i$ is the row matrix with 1 in the $i^{\text{th}}$ column and 0's elsewhere. Here we use the ring structure The defining properties of the module structure are equivalent to the homomorphism property of $\mathcal{X}$ together with the distributive and associative properties of matrix multiplication.

**Exercise 2.2.** Assume $\mathcal{X}$ is a $\Bbbk$-representation of $G$ and prove that $\Bbbk^n$ is a $\Bbbk[G]$-module under the scalar multiplication defined above.

**Definition 2.3.** Let $\Bbbk$ be a field. A $\Bbbk$-*algebra* is a $\Bbbk$-vector space $A$ which also has the structure of a ring, satisfying (i) $(v \cdot \lambda)w = (vw) \cdot \lambda$ and (ii) $v(w \cdot \lambda) = (vw) \cdot \lambda$, for all $v, w \in A$ and $\lambda \in \Bbbk$.

If