Basic Terminology and Results for Rings

Revised October 31, 2013

Let R be a set. A *binary operation on* R is a function that takes ordered pairs of elements of R, to elements of R. For example, addition, subtraction and multiplication are binary operations on $\mathbb{R}$. Exponentiation is a binary operation on the positive reals, taking (a, b) to a^b. Division is also a binary operation on the nonzero reals, taking (a, b) to $\frac{a}{b}$. Addition, multiplication and exponentiation are binary operations on $\mathbb{N} = \{1, 2, 3, \ldots\}$ but subtraction and division are not binary operations on $\mathbb{N}$. In order to have a binary operation on R, we require that R be *closed* under the operation; i.e. the values of the operation actually lie in R.

The word 'binary' refers to the operation having two inputs. By contrast, a *unary operation on* R takes a single element of R to an element of R. For example, $x \mapsto -x$ is a unary operation on $\mathbb{R}$, or on $\mathbb{Q}$, or on $\mathbb{Z}$, but not on $\mathbb{N}$. The operation $x \mapsto x^{-1} = \frac{1}{x}$ is a unary operation on $\mathbb{R}^\times$, the set of nonzero real numbers. More generally, an *n-ary operation on* R takes an ordered n-tuple from R, to an element of R. The most important n-ary operations are those for $n = 1, 2$.

A *ring* is a set R with two binary operations called *addition* and *multiplication*, such that the following properties hold:

(i) $a + b = b + a$ for all $a, b \in R$;

(ii) $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$;

(iii) There exists an element in R which (if we denote this element by $0 \in R$) satisfies $a + 0 = a$ for all $a \in R$;

(iv) Every element in R has an additive inverse, i.e. for every $a \in R$ there exists $x \in R$ such that $a + x = 0$;

(v) $a(bc) = (ab)c$ for all $a, b, c \in R$; and

(vi) $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ for all $a, b, c \in R$.

Note that a ring is more than just a set; it is a set together with two binary operations. (Actually a ring is a set together with two binary operations and a designated element 0.)

Proposition 1. Let R be any ring. Then

(a) the 'zero element' (i.e. additive identity) of R is unique; and

(b) for each $a \in R$, the additive inverse of a is unique.

Proof. Suppose 0 and $0'$ are additive identity elements in R, both satisfying (iii). Then $0 = 0 + 0' = 0' + 0 = 0'$ using (i) and the fact that both 0 and $0'$ are additive identity elements. So actually the additive identity element of R is unique; henceforth it will be called *the zero element of* R (note: 'the' rather than 'a' zero element).

Let $a \in R$, and suppose $a + x = a + x' = 0$ for some $x, x' \in R$. Then

$$x = x + 0 = x + (a + x') = (x + a) + x' = (a + x) + x' = 0 + x' = x' + 0 = x'$$

so actually the additive inverse of a is unique. □

We write $-a$ for the additive inverse of $a \in R$. Since it is uniquely determined by a, there is no ambiguity in this definition.

Proposition 2. For all $a \in R$, we have $0a = a0 = 0$.

Proof. Note that $0a = (0 + 0)a = 0a + 0a$. Adding $-0a$ to both sides,

$$0 = 0a + (-0a) = (0a + 0a) + (-0a) = 0a + \big(0a + (-0a)\big) = 0a + 0 = 0a.$$

A similar argument shows that $a0 = 0$. □

Proposition 3. For all $a, b \in R$, we have

(a) $-(a + b) = (-a) + (-b)$;
(b) $-(-a) = a$;
(c) $-(ab) = (-a)b = a(-b)$;
(d) $(-a)(-b) = ab$.

Proof. Use (i) and (ii) multiple times, we get

$$(a + b) + \big((-a) + (-b)\big) = \cdots = \big(a + (-a)\big) + \big(b + (-b)\big) = 0 + 0 = 0$$

which proves (a). By the definition of $-a$, we have $(-a) + a = a + (-a) = 0$ which forces $-(-a) = a$, so (b) follows.

Using (vi) and Proposition 3, $ab + (-a)b = \big(a + (-a)\big)b = 0b = 0$ which shows that $-ab = (-a)b$. A similar argument (using the right distributive law rather than the left distributive law) shows that $-ab = a(-b)$. Finally, (d) follows by combining (b) and (c) as follows: $(-a)(-b) = -(-a)b = \big(-(-a)\big)b = ab$. □

In any ring R, we define a new binary operation called subtraction by $a-b = a+(-b)$. We define positive powers recursively by $a^1 = a$ and $a^{k+1} = a^k a$ for all $k \geq 1$. We define integer multiples of ring elements by

$$ka = \begin{cases} \underbrace{a+a+\cdots+a}_{k \text{ times}}, & \text{for } k = 1, 2, 3, \ldots; \\ 0, & \text{if } k = 0; \text{ and} \\ -|k|a, & \text{for } k = -1, -2, -3, \ldots. \end{cases}$$

It is then straightforward to check that $(k\ell)a = k(\ell a)$ and $(k+\ell)a = ka+\ell a$ for all $k, \ell \in \mathbb{Z}$ and $a \in R$. This requires a straightforward check. (It does not follow from the ring axioms (v) and (vi) since here we are talking not about products of elements of R, but rather integer multiples of ring elements.)

If a ring R satisfies $ab = ba$ for all $a, b \in R$, then we say R is *commutative*. (Note that here we are describing multiplication as commutative. When we speak of a commutative ring, it should be clear that we are referring to the commutativity of multiplication since the corresponding property for addition holds in all cases by axiom (i).) For example, the rings $\mathbb{Z}$, $\mathbb{Z}_5$ and $\mathbb{R}[t]$ are commutative, but the ring $M_2(\mathbb{R})$ is noncommutative.

We say that a ring R *has identity* if there exists a nonzero element $e \in R$ such that $ea = ae = a$ for all $a \in R$. Again, 'identity' refers to multiplicative identity, since the additive identity exists in all cases by (iii). For example, the rings $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{R}[t]$ have identity 1. The ring $M_2(\mathbb{R})$ has identity $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. The set $\{0, 2, 4\}$ with addition and multiplication mod 6, is a commutative ring with identity $e = 4$. The set of all even integers, with the usual addition and multiplication of integers, is a commutative ring without identity. Most of the time, we will simply denote the identity by $e = 1$, if this does not create any confusion. A proof similar to the one given for Proposition 1, shows that if R has an identity, then this identity is unique.

Warning: Some textbooks restrict attention to commutative rings with identity; and they often use the term 'ring' to refer to such structures (i.e. what we call commutative rings with identity). Accordingly, some books refer to a *rng* as a ring but possibly without identity. Somewhat less typically, certain books throw away certain of our ring axioms; thus for example a nonassociative ring is one where (v) does not necessarily hold. When referring to other sources, always be careful to check the fine print, sometimes in the introduction, to see what is assumed by the term 'ring'!

Let R be a ring with identity 1. A *unit in* R is an element $u \in R$ such that $uv = vu = 1$ for some $v \in R$. Thus a unit is the same thing as an invertible element, i.e. an element

having a (multiplicative) inverse. If an inverse of u exists, then it is unique; and so we may denote it by u^{-1}. More generally, for $k \in \mathbb{Z}$ the kth power of u is defined by

$$u^k = \begin{cases} \underbrace{uuu\cdots u}_{k \text{ times}}, & \text{if } k \geq 1; \\ 1, & \text{if } k = 0; \\ (u^{-1})^{|k|}, & \text{if } k < 0. \end{cases}$$

(Of course u^k is not defined for $k < 0$ unless u is a unit.) The set of units in R is denoted by $R^\times$; for example, $\mathbb{Z}^\times = \{1, -1\}$, $\mathbb{Z}_9^\times = \{1, 2, 4, 5, 7, 8\}$. For all $u, v \in R^\times$, we have $uv \in R^\times$ since $(uv)^{-1} = v^{-1}u^{-1}$. The set of units $R^\times$ is an example of a *group* (meaning that it is a set with one binary operation, in this case multiplication, which contains 1 and is closed under products and inverses). The second course of this sequence, Algebra II, is devoted to the study of groups; but for now, we may remark that many natural examples of groups arise as the set of units in a ring.

A *field* is a commutative ring with identity, in which *every* nonzero element is a unit. In any field F, division is defined as follows: if $b \neq 0$ then $\frac{a}{b}$ is defined as ab^{-1} (which agrees with $b^{-1}a$ only because F is commutative).

Let R and R' be rings. An *isomorphism from R to R'* is a bijection $\theta : R \to R'$ such that $\theta(a + b) = \theta(a) + \theta(b)$ and $\theta(ab) = \theta(a)\theta(b)$ for all $a, b \in R$. If there exists an isomorphism from R to R', we say that the rings R and R' are *isomorphic* and we write $R \cong R'$ in this case. If two rings are isomorphic, then all their *intrinsic* properties are the same, i.e. any differences between the two rings are due to the differences in names for the elements only; after all, an isomorphism $\theta : R \to R'$ may be regarded as a renaming of the elements, which preserves their basic properties under the binary operations. For example, the set $R = \{0, 2, 4\}$ with addition and multiplication mod 6, is a ring isomorphic to $\mathbb{Z}_3$. In this case, the map $\theta : R \to \mathbb{Z}_3$ given by $0 \mapsto 0$, $2 \mapsto 2$, $4 \mapsto 1$ is an isomorphism.

Assume R and R' are two sets, each with binary operations of addition and multiplication. If $\theta : R \to R'$ is an isomorphism (i.e. θ is a bijection satisfying $\theta(a+b) = \theta(a)+\theta(b)$ and $\theta(ab) = \theta(a)\theta(b)$), then R and R' have all the same intrinsic properties. So if R is a ring, then automatically so is R'. If R is commutative, then R' is too. If R has an identity, then so does R'. If R is a field, then so is R'. The two sets have the same number of elements, the same number of units, and so forth.

In any commutative ring R, we say that a divides b, or b is a multiple of a, if $b = ma$ for some $m \in R$. In this case we write $a \,\big|\, b$. In a trivial sense, every element divides 0, since for every $a \in R$ we have $0 = 0a$. However, we shall refer to a *zero divisor* as a *nonzero* element $a \in R$ such that $0 = ab$ for some *nonzero* $b \in R$. (Without these restrictions, every element would be a zero divisor for trivial reasons.) For example in $\mathbb{Z}_6$, the zero divisors are the elements $2, 3, 4$ since $2 \cdot 3 = 3 \cdot 4 = 0$. A zero divisor cannot be a unit; for suppose

$u \in R$ is both a zero divisor and a unit. There exists $v \in R$ such that $uv = 1$; also there exists a nonzero element $r \in R$ such that $ru = 0$. Then $r = r1 = r(uv) = (ru)v = 0v = v$, a contradiction.

An *integral domain* is a commutative ring with identity, which has no zero divisors. Note that every field is an integral domain; however, not every integral domain is a field. For example, $\mathbb{Z}$, $\mathbb{Z}[t]$ and $\mathbb{R}[t]$ are integral domains but not fields. Some integral domains (such as $\mathbb{Z}$, $\mathbb{Z}[\sqrt{2}$, $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{R}[t]$) have unique factorization; others (such as $\mathbb{Z}[\sqrt{23}]$ and $\mathbb{Z}[\sqrt{-5}]$) do not. In the case of $\mathbb{R}[t]$, unique factorization holds because there is a notion of degree of a ring element, satisfying the conditions of the division algorithm: given $f(t), d(t)$ with $d(t) \neq 0$, we obtain $f(t) = q(t)d(t) + r(t)$ where the remainder $r(t)$ has degree less than the degree of $d(t)$. Any integral domain having a notion of degree with this property, is called a *Euclidean domain*. The ring of integers is also a Euclidean domain, where the degree of $d \in \mathbb{Z}$ is understood to be $|d|$. One proves (just as we did with $\mathbb{Z}$ or with $\mathbb{R}[t]$) that every Euclidean ring has unique factorization.

By (iii), every ring has at least one element, namely 0. A ring with *only* one element is called a trivial ring. We speak of *the* trivial ring $\{0\}$ since it is, up to isomorphism, the *unique* ring with only one element. A situation *almost* as trivial is a ring in which all products are zero, i.e. $ab = 0$ for all $a, b \in R$. This cannot happen in a ring with identity, because of the requirement that $1 \neq 0$.

Let S be a subset of a ring R. We say that S is a *subring* of R if S is also a ring, using the same binary operations as in R (but restricted to S). Thus for example, $\mathbb{Z}$ is a subring of $\mathbb{Q}$, which is a subring of $\mathbb{R}$, which is a subring of $\mathbb{C}$. Note that $\mathbb{Z}_5$ is *not* a subring of $\mathbb{Z}$ since the operation of addition in $\mathbb{Z}_3$ does not agree with the operation of addition in $\mathbb{Z}$: we have $2 + 2 = 1$ in $\mathbb{Z}_3$, but this does not agree with the result in $\mathbb{Z}$. In order for a subset $S \subseteq R$ to be a subring, it must be nonempty (at least it must contain a zero element, and this must be the same as the zero element of R); and it must be closed under addition, subtraction, and multiplication. To check the remaining properties (i.e. (i), (ii), etc.) for S does not present any problem; since these properties hold universally in R, they must also hold in S. So we obtain

Proposition 4. Let S be a nonempty subset of a ring R. Suppose that S contains the zero element of R; and that $a + b$, $a - b$, $ab \in S$ whenever $a, b \in S$. Then S is a subring of R (and in particular, S is itself a ring).

Instead of checking for closure under the three binary operations stated above (addition, subtraction, and multiplication), it suffices to check for closure under just subtraction and multiplication, since this implies closure under addition. Alternatively, it suffices to check for closure under addition and multiplication, and under the unary operation $a \mapsto -a$.

For example, let S be the set of all rational numbers of the form $\frac{a}{b}$ where a, b are integers with b odd. Then $0 = \frac{0}{1} \in S$; and S is closed under addition, subtraction and multiplication. (Here we make use of the familiar rules for addition and subtraction of fractions, using a common denominator; also the rule for multiplying fractions.) Thus S is a ring (in this case, a subring of $\mathbb{Q}$.)

In Linear Algebra, there is a well-known theorem that is completely analogous to Proposition 4. Linear Algebra is the study of algebraic structures known as vector spaces; and in a vector space V, a *subspace* is by definition a subset $U \subseteq V$ which is also a vector space (using the same operations as in V, just restricted to U). The comparable theorem is that a subset $U \subset V$ is a subspace iff U contains the zero vector, and U is closed under vector addition and scalar multiplication (equivalently, U is closed under taking linear combinations). This is an example of a large number of connections between abstract algebra and linear algebra; and we will highlight such connections from time to time.

An *integral domain* is a commutative ring with identity, which has no zero divisors. Note that every field is an integral domain; however, not every integral domain is a field. For example, $\mathbb{Z}$, $\mathbb{Z}[t]$ and $\mathbb{R}[t]$ are integral domains but not fields. What is special about integral domains, is stated in the following:

Theorem 5. Let R be an integral domain. Then R is a subring of its *quotient field* F which consists of the 'fractions' of the form $\frac{a}{b}$ where $a, b \in R$ with $b \neq 0$.

Familiar examples of this process include the following: From the integral domain $\mathbb{Z}$, one obtains $\mathbb{Q}$ as the field of fractions of $\mathbb{Z}$. From the integral domain $\mathbb{R}[x]$ (the ring of polynomials in x with real coefficients), we obtain $\mathbb{R}(x)$, the field of rational functions in x with real coefficients. From the integral domain $\mathbb{Z}[\sqrt{2}]$, we obtain the field $\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} \,:\, a, b \in \mathbb{Q}\right\}$ as its quotient field. In order for the ring R to have a quotient field, it really needs to be an integral domain; for example quotients of elements of $\mathbb{Z}_6$ do not form a field with addition and multiplication mod 6, since the expression $\frac{1}{3} \cdot \frac{5}{4} = \frac{5}{12} = \frac{5}{0}$ would of course be meaningless. Here of course the problem with $\mathbb{Z}_6$ is that it has zero divisors.

A *real quaternion* is an expression of the form $z = a + bi + cj + dk$ where $a, b, c \in \mathbb{R}$. Here the fixed symbols i, j, k satisfy

$$i^2 = j^2 = k^2 = -1$$

$$\begin{array}{lll} ij = k & jk = i & ki = j \\ ji = -k & kj = -i & ik = -j \end{array}$$

The set of all real quaternions, denoted by $\mathbb{H}$, is a noncommutative ring with identity 1. The *conjugate* of a real quaternion $z = a+bi+cj+dk \in \mathbb{H}$ is defined as $\overline{z} = a-bi-cj-dk$. It satisfies

$$\overline{z+w} = \overline{z} + \overline{w}\,, \qquad \overline{zw} = \overline{w}\,\overline{z}$$

for all $z, w \in \mathbb{H}$. The *norm* of $z = a+bi+cj+dk \in \mathbb{H}$ is $|z|^2 = z\overline{z} = \overline{z}z = a^2+b^2+c^2+d^2$. We have $|zw|^2 = (zw)(\overline{zw}) = zw\overline{w}\,\overline{z} = z|w|^2\overline{z} = z\overline{z}|w|^2 = |z|^2|w|^2$ since real numbers commute with every quaternion. In particular, $|zw| = |z||w|$. Furthermore, if $z \neq 0$ then $|z| \neq 0$ so

$$z \cdot \tfrac{1}{|z|^2}\overline{z} = \frac{z\overline{z}}{|z|^2} = 1$$

and so every nonzero element $z \in \mathbb{H}$ is a unit, with $z^{-1} = \frac{1}{|z|^2}\overline{z}$. So $\mathbb{H}$ is almost a field; the only thing lacking is commutativity. It fits into a very natural sequence $\mathbb{R} \subset \mathbb{C} \subset \mathbb{H} \subset \mathbb{O}$ of dimensions 1, 2, 4 and 8 respectively. These are division rings, except for $\mathbb{O}$ (the *ring of octonions*) which is actually a *nonassociative* division ring. The rings $\mathbb{H}$ and $\mathbb{O}$ have been intensively studied, primarily by physicists.

A *skewfield*, or *division ring*, is a ring with identity, in which every nonzero element is a unit. A skewfield is a *proper skewfield* if it is noncommutative; it is of course a field if it is commutative. Examples of proper skewfields take some effort to construct, and $\mathbb{H}$ is our first example of this (probably our only example in this course). A famous theorem of Wedderburn says that every finite skewfield is commutative, hence a field; so every proper skewfield must be infinite.

Note that the polynomial t^2+1 has many roots in $\mathbb{H}$: clearly at least six roots $\pm i, \pm j, \pm k$, and actually there are infinitely many roots in $\mathbb{H}$. So the fact (valid for any field F) that any polynomial $f(t) \in F[t]$ of degree n has at most n roots in F, is not true more generally for skewfields.