Rings having some of the same characteristics as the integers $\mathbb{Z}$ are given a name:

Definition. A commutative ring with identity $1 \neq 0$ is called an *integral domain* if it has no zero divisors.

The absence of zero divisors in integral domains give these rings a cancellation property:

Proposition 2. Assume a, b and c are elements of any ring with a not a zero divisor. If $ab = ac$, then either $a = 0$ or $b = c$ (i.e., if $a \neq 0$ we can cancel the a's). In particular, if a, b, c are any elements in an integral domain and $ab = ac$, then either $a = 0$ or $b = c$.

Proof: If $ab = ac$ then $a(b - c) = 0$ so either $a = 0$ or $b - c = 0$. The second statement follows from the first and the definition of an integral domain.

Corollary 3. Any finite integral domain is a field.

Proof: Let R be a finite integral domain and let a be a nonzero element of R. By the cancellation law the map $x \mapsto ax$ is an injective function. Since R is finite this map is also surjective. In particular, there is some $b \in R$ such that $ab = 1$, i.e., a is a unit in R. Since a was an arbitrary nonzero element, R is a field.

A remarkable result of Wedderburn is that a finite division ring is necessarily commutative, i.e., is a field. A proof of this theorem is outlined in the exercises at the end of Section 13.6.

In Section 5 we study the relation between zero divisors and units in greater detail. We shall see that every nonzero element of a commutative ring that is not a zero divisor has a multiplicative inverse in some larger ring. This gives another perspective on the cancellation law in Proposition 2.

Having defined the notion of a ring, there is a natural notion of a subring.

Definition. A *subring* of the ring R is a subgroup of R that is closed under multiplication.

In other words, a subset S of a ring R is a subring if the operations of addition and multiplication in R when restricted to S give S the structure of a ring. To show that a subset of a ring R is a subring it suffices to check that it is *nonempty* and *closed under subtraction and under multiplication.*

Examples

A number of the examples above were also subrings.

(1) $\mathbb{Z}$ is a subring of $\mathbb{Q}$ and $\mathbb{Q}$ is a subring of $\mathbb{R}$. The property "is a subring of" is clearly transitive.

(2) $2\mathbb{Z}$ is a subring of $\mathbb{Z}$, as is $n\mathbb{Z}$ for any integer n. The ring $\mathbb{Z}/n\mathbb{Z}$ is not a subring (or a subgroup) of $\mathbb{Z}$ for any $n \geq 2$.

(3) The ring of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$ is a subring of the ring of all functions from $\mathbb{R}$ to $\mathbb{R}$. The ring of all differentiable functions from $\mathbb{R}$ to $\mathbb{R}$ is a subring of both of these.

(4) $S = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$, the *integral* Quaternions, form a subring of either the real or the rational Quaternions — it is easy to check that multiplying two such quaternions together gives another quaternion with integer coefficients. This ring (which is not a division ring) can be used to give proofs for a number of results in number theory.

(5) If R is a subring of a field F that contains the identity of F then R is an integral domain. The converse of this is also true, namely any integral domain is contained in a field (cf. Section 5).

Example: (Quadratic Integer Rings)

Let D be a squarefree integer. It is immediate from the addition and multiplication that the subset $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}$ forms a subring of the quadratic field $\mathbb{Q}(\sqrt{D})$ defined earlier. If $D \equiv 1 \bmod 4$ then the slightly larger subset

$$\mathbb{Z}[\frac{1+\sqrt{D}}{2}] = \{a + b\frac{1+\sqrt{D}}{2} \mid a, b \in \mathbb{Z}\}$$

is also a subring: closure under addition is immediate and $(a + b\frac{1+\sqrt{D}}{2})(c + d\frac{1+\sqrt{D}}{2}) = (ac + bd\frac{D-1}{4}) + (ad + bc + bd)\frac{1+\sqrt{D}}{2}$ together with the congruence on D shows closure under multiplication.

Define

$$\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\},$$

where

$$\omega = \begin{cases} \sqrt{D}, & \text{if } D \equiv 2, 3 \bmod 4 \\ \dfrac{1+\sqrt{D}}{2}, & \text{if } D \equiv 1 \bmod 4, \end{cases}$$

called the *ring of integers* in the quadratic field $\mathbb{Q}(\sqrt{D})$. The terminology comes from the fact that the elements of the subring $\mathcal{O}$ of the field $\mathbb{Q}(\sqrt{D})$ have many properties analogous to those of the subring of integers $\mathbb{Z}$ in the field of rational numbers $\mathbb{Q}$ (and are the *integral closure* of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{D})$ as explained in Section 15.3).

In the special case when $D = -1$ we obtain the ring $\mathbb{Z}[i]$ of *Gaussian integers*, which are the complex numbers $a + bi \in \mathbb{C}$ with a and b both *integers*. These numbers were originally introduced by Gauss around 1800 in order to state the biquadratic reciprocity law which deals with the beautiful relations that exist among fourth powers modulo primes. We shall shortly see another useful application of the algebraic structure of this ring to number theoretic questions.

Define the *field norm* $N : \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}$ by

$$N(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2 \in \mathbb{Q},$$

which, as previously mentioned, is nonzero if $a + b\sqrt{D} \neq 0$. This norm gives a measure of "size" in the field $\mathbb{Q}(\sqrt{D})$. For instance when $D = -1$ the norm of $a + bi$ is $a^2 + b^2$, which is the square of the length of this complex number considered as a vector in the complex plane. We shall use the field norm in this and subsequent examples to establish many properties of the rings $\mathcal{O}$.

It is easy to check that N is *multiplicative*, i.e., that $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$. On the subring $\mathcal{O}$ it is also easy to see that the field norm is given by

$$N(a+b\omega) = (a+b\omega)(a+b\overline{\omega}) = \begin{cases} a^2 - Db^2, & \text{if } D \equiv 2, 3 \bmod 4 \\ a^2 + ab + \dfrac{1-D}{4}b^2, & \text{if } D \equiv 1 \bmod 4 \end{cases}$$

where

$$\overline{\omega} = \begin{cases} -\sqrt{D}, & \text{if } D \equiv 2, 3 \bmod 4 \\ \dfrac{1-\sqrt{D}}{2}, & \text{if } D \equiv 1 \bmod 4. \end{cases}$$

It follows that $N(\alpha)$ is in fact an *integer* for every $\alpha \in \mathcal{O}$.

We may use this norm to characterize the units in $\mathcal{O}$. If $\alpha \in \mathcal{O}$ has field norm $N(\alpha) = \pm 1$, the previous formula shows that $(a+b\omega)^{-1} = \pm(a+b\overline{\omega})$, which is again an element of $\mathcal{O}$ and so α is a unit in $\mathcal{O}$. Suppose conversely that α is a unit in $\mathcal{O}$, say $\alpha\beta = 1$ for some $\beta \in \mathcal{O}$. Then the multiplicative property of the field norm implies that $N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$. Since both $N(\alpha)$ and $N(\beta)$ are integers, each must be ± 1. Hence,

the element α is a unit in $\mathcal{O}$ if and only if $N(\alpha) = \pm 1$.

In particular the determination of the integer solutions to the equation $x^2 - Dy^2 = \pm 1$ (called *Pell's equation* in elementary number theory) is essentially equivalent to the determination of the units in the ring $\mathcal{O}$.

When $D = -1$, the units in the Gaussian integers $\mathbb{Z}[i]$ are the elements $a + bi$ with $a^2 + b^2 = \pm 1$, $a, b \in \mathbb{Z}$, so the group of units consists of $\{\pm 1, \pm i\}$. When $D = -3$, the units in $\mathbb{Z}[(1+\sqrt{-3})/2]$ are determined by the integers a, b with $a^2 + ab + b^2 = \pm 1$, i.e., with $(2a+b)^2 + 3b^2 = \pm 4$, from which it is easy to see that the group of units is a group of order 6 given by $\{\pm 1, \pm\rho, \pm\rho^2\}$ where $\rho = (-1+\sqrt{-3})/2$. For any other $D < 0$ it is similarly straightforward to see that the only units are $\{\pm 1\}$.

By contrast, when $D > 0$ it can be shown that the group of units $\mathcal{O}^\times$ is always infinite. For example, it is easy to check that $1 + \sqrt{2}$ is a unit in the ring $\mathcal{O} = \mathbb{Z}[\sqrt{2}]$ (with field norm -1) and that $\{\pm(1+\sqrt{2})^n \mid n \in \mathbb{Z}\}$, is an infinite set of distinct units (in fact the full group of units in this case, but this is harder to prove).

EXERCISES

Let R be a ring with 1.

1. Show that $(-1)^2 = 1$ in R.
2. Prove that if u is a unit in R then so is $-u$.
3. Let R be a ring with identity and let S be a subring of R containing the identity. Prove that if u is a unit in S then u is a unit in R. Show by example that the converse is false.
4. Prove that the intersection of any nonempty collection of subrings of a ring is also a subring.
5. Decide which of the following (a) – (f) are subrings of $\mathbb{Q}$:
   (a) the set of all rational numbers with odd denominators (when written in lowest terms)
   (b) the set of all rational numbers with even denominators (when written in lowest terms)
   (c) the set of nonnegative rational numbers
   (d) the set of squares of rational numbers
   (e) the set of all rational numbers with odd numerators (when written in lowest terms)

(f) the set of all rational numbers with even numerators (when written in lowest terms).

6. Decide which of the following are subrings of the ring of all functions from the closed interval [0,1] to $\mathbb{R}$:
(a) the set of all functions $f(x)$ such that $f(q) = 0$ for all $q \in \mathbb{Q} \cap [0, 1]$
(b) the set of all polynomial functions
(c) the set of all functions which have only a finite number of zeros, together with the zero function
(d) the set of all functions which have an infinite number of zeros
(e) the set of all functions f such that $\lim_{x \to 1^-} f(x) = 0$
(f) the set of all rational linear combinations of the functions $\sin nx$ and $\cos mx$, where $m, n \in \{0, 1, 2, \ldots\}$.

7. The *center* of a ring R is $\{z \in R \mid zr = rz \text{ for all } r \in R\}$ (i.e., is the set of all elements which commute with every element of R). Prove that the center of a ring is a subring that contains the identity. Prove that the center of a division ring is a field.

8. Describe the center of the real Hamilton Quaternions $\mathbb{H}$. Prove that $\{a + bi \mid a, b \in \mathbb{R}\}$ is a subring of $\mathbb{H}$ which is a field but is not contained in the center of $\mathbb{H}$.

9. For a fixed element $a \in R$ define $C(a) = \{r \in R \mid ra = ar\}$. Prove that $C(a)$ is a subring of R containing a. Prove that the center of R is the intersection of the subrings $C(a)$ over all $a \in R$.

10. Prove that if D is a division ring then $C(a)$ is a division ring for all $a \in D$ (cf. the preceding exercise).

11. Prove that if R is an integral domain and $x^2 = 1$ for some $x \in R$ then $x = \pm 1$.

12. Prove that any subring of a field which contains the identity is an integral domain.

13. An element x in R is called *nilpotent* if $x^m = 0$ for some $m \in \mathbb{Z}^+$.
(a) Show that if $n = a^k b$ for some integers a and b then $\overline{ab}$ is a nilpotent element of $\mathbb{Z}/n\mathbb{Z}$.
(b) If $a \in \mathbb{Z}$ is an integer, show that the element $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent if and only if every prime divisor of n is also a divisor of a. In particular, determine the nilpotent elements of $\mathbb{Z}/72\mathbb{Z}$ explicitly.
(c) Let R be the ring of functions from a nonempty set X to a field F. Prove that R contains no nonzero nilpotent elements.

14. Let x be a nilpotent element of the commutative ring R (cf. the preceding exercise).
(a) Prove that x is either zero or a zero divisor.
(b) Prove that rx is nilpotent for all $r \in R$.
(c) Prove that $1 + x$ is a unit in R.
(d) Deduce that the sum of a nilpotent element and a unit is a unit.

15. A ring R is called a *Boolean ring* if $a^2 = a$ for all $a \in R$. Prove that every Boolean ring is commutative.

16. Prove that the only Boolean ring that is an integral domain is $\mathbb{Z}/2\mathbb{Z}$.

17. Let R and S be rings. Prove that the direct product $R \times S$ is a ring under componentwise addition and multiplication. Prove that $R \times S$ is commutative if and only if both R and S are commutative. Prove that $R \times S$ has an identity if and only if both R and S have identities.

18. Prove that $\{(r, r) \mid r \in R\}$ is a subring of $R \times R$.

19. Let I be any nonempty index set and let R_i be a ring for each $i \in I$. Prove that the direct