valuation on K and let R be the valuation ring of ν. For each integer $k \geq 0$ define $A_k = \{r \in R \mid \nu(r) \geq k\} \cup \{0\}$.

(a) Prove that A_k is a principal ideal and that $A_0 \supseteq A_1 \supseteq A_2 \supseteq \cdots$.

(b) Prove that if I is any nonzero ideal of R, then $I = A_k$ for some $k \geq 0$. Deduce that R is a local ring with unique maximal ideal A_1.

40. Assume R is commutative. Prove that the following are equivalent: (see also Exercises 13 and 14 in Section 1)

(i) R has exactly one prime ideal

(ii) every element of R is either nilpotent or a unit

(iii) $R/\eta(R)$ is a field (cf. Exercise 29, Section 3).

41. A proper ideal Q of the commutative ring R is called *primary* if whenever $ab \in Q$ and $a \notin Q$ then $b^n \in Q$ for some positive integer n. (Note that the symmetry between a and b in this definition implies that if Q is a primary ideal and $ab \in Q$ with *neither* a nor b in Q, then a positive power of a and a positive power of b both lie in Q.) Establish the following facts about primary ideals.

(a) The primary ideals of $\mathbb{Z}$ are 0 and (p^n), where p is a prime and n is a positive integer.

(b) Every prime ideal of R is a primary ideal.

(c) An ideal Q of R is primary if and only if every zero divisor in R/Q is a nilpotent element of R/Q.

(d) If Q is a primary ideal then $\operatorname{rad}(Q)$ is a prime ideal (cf. Exercise 30).

7.5 RINGS OF FRACTIONS

Throughout this section R is a commutative ring. Proposition 2 shows that if a is not zero nor a zero divisor and $ab = ac$ in R then $b = c$. Thus a nonzero element that is not a zero divisor enjoys some of the properties of a unit without necessarily possessing a multiplicative inverse in R. On the other hand, we saw in Section 1 that a zero divisor a cannot be a unit in R and, by definition, if a is a zero divisor we cannot always cancel the a's in the equation $ab = ac$ to obtain $b = c$ (take $c = 0$ for example). The aim of this section is to prove that a commutative ring R is always a subring of a larger ring Q in which every nonzero element of R that is not a zero divisor is a unit in Q. The principal application of this will be to integral domains, in which case this ring Q will be a field — called its *field of fractions* or *quotient field*. Indeed, the paradigm for the construction of Q from R is the one offered by the construction of the field of rational numbers from the integral domain $\mathbb{Z}$.

In order to see the essential features of the construction of the field $\mathbb{Q}$ from the integral domain $\mathbb{Z}$ we review the basic properties of fractions. Each rational number may be represented in many different ways as the quotient of two integers (for example, $\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \ldots$, etc.). These representations are related by

$$\frac{a}{b} = \frac{c}{d} \qquad \text{if and only if} \qquad ad = bc.$$

In more precise terms, the fraction $\frac{a}{b}$ is the equivalence class of ordered pairs (a, b) of integers with $b \neq 0$ under the equivalence relation: $(a, b) \sim (c, d)$ if and only if

$ad = bc$. The arithmetic operations on fractions are given by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \qquad \text{and} \qquad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

These are well defined (independent of choice of representatives of the equivalence classes) and make the set of fractions into a commutative ring (in fact, a field), $\mathbb{Q}$. The integers $\mathbb{Z}$ are identified with the subring $\{\frac{a}{1} \mid a \in \mathbb{Z}\}$ of $\mathbb{Q}$ and every nonzero integer a has an inverse $\frac{1}{a}$ in $\mathbb{Q}$.

It seems reasonable to attempt to follow the same steps for any commutative ring R, allowing arbitrary denominators. If, however, b is zero or a zero divisor in R, say $bd = 0$, and if we allow b as a denominator, then we should expect to have

$$d = \frac{d}{1} = \frac{bd}{b} = \frac{0}{b} = 0$$

in the "ring of fractions" (where, for convenience, we have assumed R has a 1). Thus if we allow zero or zero divisors as denominators there must be some collapsing in the sense that we cannot expect R to appear naturally as a subring of this "ring of fractions." A second restriction is more obviously imposed by the laws of addition and multiplication: if ring elements b and d are allowed as denominators, then bd must also be a denominator, i.e., the set of denominators must be closed under multiplication in R. The main result of this section shows that these two restrictions are sufficient to construct a ring of fractions for R. Note that this theorem includes the construction of $\mathbb{Q}$ from $\mathbb{Z}$ as a special case.

Theorem 15. Let R be a commutative ring. Let D be any nonempty subset of R that does not contain 0, does not contain any zero divisors and is closed under multiplication (i.e., $ab \in D$ for all $a, b \in D$). Then there is a commutative ring Q with 1 such that Q contains R as a subring and every element of D is a unit in Q. The ring Q has the following additional properties.

(1) every element of Q is of the form rd^{-1} for some $r \in R$ and $d \in D$. In particular, if $D = R - \{0\}$ then Q is a field.

(2) (uniqueness of Q) The ring Q is the "*smallest*" ring containing R in which all elements of D become units, in the following sense. Let S be any commutative ring with identity and let $\varphi : R \to S$ be any injective ring homomorphism such that $\varphi(d)$ is a unit in S for every $d \in D$. Then there is an injective homomorphism $\Phi : Q \to S$ such that $\Phi|_R = \varphi$. In other words, any ring containing an isomorphic copy of R in which all the elements of D become units must also contain an isomorphic copy of Q.

Remark: In Section 15.4 a more general construction is given. The proof of the general result is more technical but relies on the same basic rationale and steps as the proof of Theorem 15. Readers wishing greater generality may read the proof below and the beginning of Section 15.4 in concert.

Proof: Let $\mathcal{F} = \{(r, d) \mid r \in R,\ d \in D\}$ and define the relation $\sim$ on $\mathcal{F}$ by

$$(r, d) \sim (s, e) \qquad \text{if and only if} \qquad re = sd.$$

It is immediate that this relation is reflexive and symmetric. Suppose $(r, d) \sim (s, e)$ and $(s, e) \sim (t, f)$. Then $re - sd = 0$ and $sf - te = 0$. Multiplying the first of these equations by f and the second by d and adding them gives $(rf - td)e = 0$. Since $e \in D$ is neither zero nor a zero divisor we must have $rf - td = 0$, i.e., $(r, d) \sim (t, f)$. This proves $\sim$ is transitive, hence an equivalence relation. Denote the equivalence class of (r, d) by $\frac{r}{d}$:

$$\frac{r}{d} = \{(a, b) \mid a \in R,\ b \in D \text{ and } rb = ad\}.$$

Let Q be the set of equivalence classes under $\sim$. Note that $\frac{r}{d} = \frac{re}{de}$ in Q for all $e \in D$, since D is closed under multiplication.

We now define an additive and multiplicative structure on Q:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \text{and} \qquad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

In order to prove that Q is a commutative ring with identity there are a number of things to check:

(1) these operations are well defined (i.e., do not depend on the choice of representatives for the equivalence classes),

(2) Q is an abelian group under addition, where the additive identity is $\frac{0}{d}$ for any $d \in D$ and the additive inverse of $\frac{a}{d}$ is $\frac{-a}{d}$,

(3) multiplication is associative, distributive and commutative, and

(4) Q has an identity ($= \frac{d}{d}$ for any $d \in D$).

These are all completely straightforward calculations involving only arithmetic in R and the definition of $\sim$. Again we need D to be closed under multiplication for addition and multiplication to be defined.

For example, to check that addition is well defined assume $\frac{a}{b} = \frac{a'}{b'}$ (i.e., $ab' = a'b$) and $\frac{c}{d} = \frac{c'}{d'}$ (i.e., $cd' = c'd$). We must show that $\frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'}$, i.e.,

$$(ad + bc)(b'd') = (a'd' + b'c')(bd).$$

The left hand side of this equation is $ab'dd' + cd'bb'$ substituting $a'b$ for ab' and $c'd$ for cd' gives $a'bdd' + c'dbb'$, which is the right hand side. Hence addition of fractions is well defined. Checking the details in the other parts of (1) to (4) involves even easier manipulations and so is left as an exercise.

Next we embed R into Q by defining

$$\iota : R \to Q \qquad \text{by} \qquad \iota : r \mapsto \frac{rd}{d} \quad \text{where } d \text{ is any element of } D.$$

Since $\frac{rd}{d} = \frac{re}{e}$ for all $d, e \in D$, $\iota(r)$ does not depend on the choice of $d \in D$. Since D is closed under multiplication, one checks directly that ι is a ring homomorphism.

Furthermore, ι is injective because

$$\iota(r) = 0 \Leftrightarrow \frac{rd}{d} = \frac{0}{d} \Leftrightarrow rd^2 = 0 \Leftrightarrow r = 0$$

because d (hence also d^2) is neither zero nor a zero divisor. The subring $\iota(R)$ of Q is therefore isomorphic to R. We henceforth identify each $r \in R$ with $\iota(r)$ and so consider R as a subring of Q.

Next note that each $d \in D$ has a multiplicative inverse in Q: namely, if d is represented by the fraction $\frac{de}{e}$ then its multiplicative inverse is $\frac{e}{de}$. One then sees that every element of Q may be written as $r \cdot d^{-1}$ for some $r \in R$ and some $d \in D$. In particular, if $D = R - \{0\}$, every nonzero element of Q has a multiplicative inverse and Q is a field.

It remains to establish the uniqueness property of Q. Assume $\varphi : R \to S$ is an injective ring homomorphism such that $\varphi(d)$ is a unit in S for all $d \in D$. Extend φ to a map $\Phi : Q \to S$ by defining $\Phi(rd^{-1}) = \varphi(r)\varphi(d)^{-1}$ for all $r \in R$, $d \in D$. This map is well defined, since $rd^{-1} = se^{-1}$ implies $re = sd$, so $\varphi(r)\varphi(e) = \varphi(s)\varphi(d)$, and then

$$\Phi(rd^{-1}) = \varphi(r)\varphi(d)^{-1} = \varphi(s)\varphi(e)^{-1} = \Phi(se^{-1}).$$

It is straightforward to check that Φ is a ring homomorphism — the details are left as an exercise. Finally, Φ is injective because $rd^{-1} \in \ker\Phi$ implies $r \in \ker\Phi \cap R = \ker\varphi$; since φ is injective this forces r and hence also rd^{-1} to be zero. This completes the proof.

Definition. Let R, D and Q be as in Theorem 15.

(1) The ring Q is called the *ring of fractions* of D with respect to R and is denoted $D^{-1}R$.

(2) If R is an integral domain and $D = R - \{0\}$, Q is called the *field of fractions* or *quotient field* of R.

If A is a subset of a field F (for example, if A is a subring of F), then the intersection of all the subfields of F containing A is a subfield of F and is called the subfield *generated* by A. This subfield is the smallest subfield of F containing A (namely, any subfield of F containing A contains the subfield generated by A).

The next corollary shows that the smallest field containing an integral domain R is its field of fractions.

Corollary 16. Let R be an integral domain and let Q be the field of fractions of R. If a field F contains a subring R' isomorphic to R then the subfield of F generated by R' is isomorphic to Q.

Proof: Let $\varphi : R \cong R' \subseteq F$ be a (ring) isomorphism of R to R'. In particular, $\varphi : R \to F$ is an injective homomorphism from R into the field F. Let $\Phi : Q \to F$ be the extension of φ to Q as in the theorem. By Theorem 15, Φ is injective, so $\Phi(Q)$ is an isomorphic copy of Q in F containing $\varphi(R) = R'$. Now, any subfield of F containing $R' = \varphi(R)$ contains the elements $\varphi(r_1)\varphi(r_2)^{-1} = \varphi(r_1 r_2^{-1})$ for all $r_1, r_2 \in R$. Since