for the product IJ of two nonprincipal ideals I and J to be principal, for example the ideals $(3, 1+\sqrt{-5})$ and $(3, 1-\sqrt{-5})$ are both nonprincipal and their product is the principal ideal generated by 3, i.e., $(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) = (3)$ (cf. Exercise 5 and the example preceding Proposition 12 below).

It is not true that every Principal Ideal Domain is a Euclidean Domain. We shall prove below that the quadratic integer ring $\mathbb{Z}[(1+\sqrt{-19})/2]$, which was shown not to be a Euclidean Domain in the previous section, nevertheless is a P.I.D.

From an ideal-theoretic point of view Principal Ideal Domains are a natural class of rings to study beyond rings which are fields (where the ideals are just the trivial ones: (0) and (1)). Many of the properties enjoyed by Euclidean Domains are also satisfied by Principal Ideal Domains. A significant advantage of Euclidean Domains over Principal Ideal Domains, however, is that although greatest common divisors exist in both settings, in Euclidean Domains one has an *algorithm* for computing them. Thus (as we shall see in Chapter 12 in particular) results which depend on the existence of greatest common divisors may often be proved in the larger class of Principal Ideal Domains although computation of examples (i.e., concrete applications of these results) are more effectively carried out using a Euclidean Algorithm (if one is available).

We collect some facts about greatest common divisors proved in the preceding section.

Proposition 6. Let R be a Principal Ideal Domain and let a and b be nonzero elements of R. Let d be a generator for the principal ideal generated by a and b. Then

(1) d is a greatest common divisor of a and b

(2) d can be written as an *R-linear combination* of a and b, i.e., there are elements x and y in R with

$$d = ax + by$$

(3) d is unique up to multiplication by a unit of R.

Proof: This is just Propositions 2 and 3.

Recall that maximal ideals are always prime ideals but the converse is not true in general. We observed in Section 7.4, however, that every nonzero prime ideal of $\mathbb{Z}$ is a maximal ideal. This useful fact is true in an arbitrary Principal Ideal Domain, as the following proposition shows.

Proposition 7. Every nonzero prime ideal in a Principal Ideal Domain is a maximal ideal.

Proof: Let (p) be a nonzero prime ideal in the Principal Ideal Domain R and let $I = (m)$ be any ideal containing (p). We must show that $I = (p)$ or $I = R$. Now $p \in (m)$ so $p = rm$ for some $r \in R$. Since (p) is a prime ideal and $rm \in (p)$, either r or m must lie in (p). If $m \in (p)$ then $(p) = (m) = I$. If, on the other hand, $r \in (p)$ write $r = ps$. In this case $p = rm = psm$, so $sm = 1$ (recall that R is an integral domain) and m is a unit so $I = R$.

As we have already mentioned, if F is a field, then the polynomial ring $F[x]$ is a Euclidean Domain, hence also a Principal Ideal Domain (this will be proved in the next chapter). The converse to this is also true. Intuitively, if I is an ideal in R (such as the ideal (2) in $\mathbb{Z}$) then the ideal (I, x) in $R[x]$ (such as the ideal $(2, x)$ in $\mathbb{Z}[x]$) requires one more generator than does I, hence in general is not principal.

Corollary 8. If R is any commutative ring such that the polynomial ring $R[x]$ is a Principal Ideal Domain (or a Euclidean Domain), then R is necessarily a field.

Proof: Assume $R[x]$ is a Principal Ideal Domain. Since R is a subring of $R[x]$ then R must be an integral domain (recall that $R[x]$ has an identity if and only if R does). The ideal (x) is a nonzero prime ideal in $R[x]$ because $R[x]/(x)$ is isomorphic to the integral domain R. By Proposition 7, (x) is a maximal ideal, hence the quotient R is a field by Proposition 12 in Section 7.4.

The last result in this section will be used to prove that not every P.I.D. is a Euclidean Domain and relates the principal ideal property with another weakening of the Euclidean condition.

Definition. Define N to be a *Dedekind–Hasse norm* if N is a positive norm and for every nonzero $a, b \in R$ either a is an element of the ideal (b) or there is a nonzero element in the ideal (a, b) of norm strictly smaller than the norm of b (i.e., either b divides a in R or there exist $s, t \in R$ with $0 < N(sa - tb) < N(b)$).

Note that R is Euclidean with respect to a positive norm N if it is always possible to satisfy the Dedekind–Hasse condition with $s = 1$, so this is indeed a weakening of the Euclidean condition.

Proposition 9. The integral domain R is a P.I.D. if and only if R has a Dedekind–Hasse norm.[2]

Proof: Let I be any nonzero ideal in R and let b be a nonzero element of I with $N(b)$ minimal. Suppose a is any nonzero element in I, so that the ideal (a, b) is contained in I. Then the Dedekind–Hasse condition on N and the minimality of b implies that $a \in (b)$, so $I = (b)$ is principal. The converse will be proved in the next section (Corollary 16).

[2] That a Dedekind–Hasse norm on R implies that R is a P.I.D. (and is equivalent when R is a ring of algebraic integers) is the classical *Criterion of Dedekind and Hasse*, cf. *Über eindeutige Zerlegung in Primelemente oder in Primhauptideale in Integritätsbereichen*, Jour. für die Reine und Angew. Math., 159(1928), pp. 3–12. The observation that the converse holds generally is more recent and due to John Greene, *Principal Ideal Domains are almost Euclidean*, Amer. Math. Monthly, 104(1997), pp. 154–156.

Example

Let $R = \mathbb{Z}[(1+\sqrt{-19})/2]$ be the quadratic integer ring considered at the end of the previous section. We show that the positive field norm $N(a + b(1 + \sqrt{-19})/2) = a^2 + ab + 5b^2$ defined on R is a Dedekind–Hasse norm, which by Proposition 9 and the results of the previous section will prove that R is a P.I.D. but not a Euclidean Domain.

Suppose α, β are nonzero elements of R and $\alpha/\beta \notin R$. We must show that there are elements $s, t \in R$ with $0 < N(s\alpha - t\beta) < N(\beta)$, which by the multiplicativity of the field norm is equivalent to

$$0 < N(\frac{\alpha}{\beta}s - t) < 1. \tag{$*$}$$

Write $\dfrac{\alpha}{\beta} = \dfrac{a + b\sqrt{-19}}{c} \in \mathbb{Q}[\sqrt{-19}]$ with integers a, b, c having no common divisor and with $c > 1$ (since β is assumed not to divide α). Since a, b, c have no common divisor there are integers x, y, z with $ax + by + cz = 1$. Write $ay - 19bx = cq + r$ for some quotient q and remainder r with $|r| \leq c/2$ and let $s = y + x\sqrt{-19}$ and $t = q - z\sqrt{-19}$. Then a quick computation shows that

$$0 < N(\frac{\alpha}{\beta}s - t) = \frac{(ay - 19bx - cq)^2 + 19(ax + by + cz)^2}{c^2} \leq \frac{1}{4} + \frac{19}{c^2}$$

and so $(*)$ is satisfied with this s and t provided $c \geq 5$.

Suppose that $c = 2$. Then one of a, b is even and the other is odd (otherwise $\alpha/\beta \in R$), and then a quick check shows that $s = 1$ and $t = \dfrac{(a-1) + b\sqrt{-19}}{2}$ are elements of R satisfying $(*)$.

Suppose that $c = 3$. The integer $a^2 + 19b^2$ is not divisible by 3 (modulo 3 this is $a^2 + b^2$ which is easily seen to be 0 modulo 3 if and only if a and b are both 0 modulo 3; but then a, b, c have a common factor). Write $a^2 + 19b^2 = 3q + r$ with $r = 1$ or 2. Then again a quick check shows that $s = a - b\sqrt{-19}$, $t = q$ are elements of R satisfying $(*)$.

Finally, suppose that $c = 4$, so a and b are not both even. If one of a, b is even and the other odd, then $a^2 + 19b^2$ is odd, so we can write $a^2 + 19b^2 = 4q + r$ for some $q, r \in \mathbb{Z}$ and $0 < r < 4$. Then $s = a - b\sqrt{-19}$ and $t = q$ satisfy $(*)$. If a and b are both odd, then $a^2 + 19b^2 \equiv 1 + 3 \bmod 8$, so we can write $a^2 + 19b^2 = 8q + 4$ for some $q \in \mathbb{Z}$. Then $s = \dfrac{a - b\sqrt{-19}}{2}$ and $t = q$ are elements of R that satisfy $(*)$.

EXERCISES

1. Prove that in a Principal Ideal Domain two ideals (a) and (b) are comaximal (cf. Section 7.6) if and only if a greatest common divisor of a and b is 1 (in which case a and b are said to be *coprime* or *relatively prime*).
2. Prove that any two nonzero elements of a P.I.D. have a least common multiple (cf. Exercise 11, Section 1).
3. Prove that a quotient of a P.I.D. by a prime ideal is again a P.I.D.
4. Let R be an integral domain. Prove that if the following two conditions hold then R is a Principal Ideal Domain:

   (i) any two nonzero elements a and b in R have a greatest common divisor which can be written in the form $ra + sb$ for some $r, s \in R$, and