Proof: The first statement in the corollary was proved above. Assume now that $b_1, \ldots, b_s$ are all even. For each prime p_i congruent to 1 modulo 4 write $p_i = \pi_i\overline{\pi_i}$ for $i = 1, 2, \ldots, r$, where π_i and $\overline{\pi_i}$ are irreducibles as in (2)(c) of Proposition 18. If $N(A + Bi) = n$ then examining norms we see that, up to units, the factorization of $A + Bi$ into irreducibles in $\mathbb{Z}[i]$ is given by

$$A + Bi = (1 + i)^k(\pi_1^{a_{1,1}}\overline{\pi_1}^{a_{1,2}}) \ldots (\pi_r^{a_{r,1}}\overline{\pi_r}^{a_{r,2}})q_1^{b_1/2} \ldots q_s^{b_s/2}$$

with nonnegative integers $a_{i,1}, a_{i,2}$ satisfying $a_{i,1} + a_{i,2} = a_i$ for $i = 1, 2, \ldots, r$. Since $a_{i,1}$ can have the values $0, 1, \ldots, a_i$ (and then $a_{i,2}$ is determined), there are a total of $(a_1 + 1)(a_2 + 1) \cdots (a_r + 1)$ distinct elements $A + Bi$ in $\mathbb{Z}[i]$ of norm n, up to units. Finally, since there are four units in $\mathbb{Z}[i]$, the second statement in the corollary follows.

Example

Since $493 = 17 \cdot 29$ and both primes are congruent to 1 modulo 4, $493 = A^2 + B^2$ is the sum of two integer squares. Since $17 = (4 + i)(4 - i)$ and $29 = (5 + 2i)(5 - 2i)$ the possible factorizations of $A + Bi$ in $\mathbb{Z}[i]$ up to units are $(4 + i)(5 + 2i) = 18 + 13i$, $(4 + i)(5 - 2i) = 22 - 3i$, $(4 - i)(5 - 2i) = 22 + 3i$, and $(4 - i)(5 - 2i) = 18 - 13i$. Multiplying by -1 reverses both signs and multiplication by i interchanges the A and B and introduces one sign change. Then $493 = (\pm 18)^2 + (\pm 13)^2 = (\pm 22)^2 + (\pm 3)^2$ with all possible choices of signs give 8 of the 16 possible representations of 493 as the sum of two squares; the remaining 8 are obtained by interchanging the two summands.

Similarly, the integer $58000957 = 7^6 \cdot 17 \cdot 29$ can be written as a sum of two squares in precisely 16 ways, obtained by multiplying each of the integers A, B in $493 = A^2 + B^2$ above by 7^3.

Summary

In summary, we have the following inclusions among classes of commutative rings with identity:

$$\textit{fields} \subset \textit{Euclidean Domains} \subset \textit{P.I.D.s} \subset \textit{U.F.D.s} \subset \textit{integral domains}$$

with all containments being proper. Recall that $\mathbb{Z}$ is a Euclidean Domain that is not a field, the quadratic integer ring $\mathbb{Z}[(1 + \sqrt{-19})/2]$ is a Principal Ideal Domain that is not a Euclidean Domain, $\mathbb{Z}[x]$ is a Unique Factorization Domain (Theorem 7 in Chapter 9) that is not a Principal Ideal Domain and $\mathbb{Z}[\sqrt{-5}]$ is an integral domain that is not a Unique Factorization Domain.

EXERCISES

1. Let $G = \mathbb{Q}^\times$ be the multiplicative group of nonzero rational numbers. If $\alpha = p/q \in G$, where p and q are relatively prime integers, let $\varphi : G \to G$ be the map which interchanges the primes 2 and 3 in the prime power factorizations of p and q (so, for example, $\varphi(2^4 3^{11} 5^1 13^2) = 3^4 2^{11} 5^1 13^2$, $\varphi(3/16) = \varphi(3/2^4) = 2/3^4 = 2/81$, and φ is the identity on all rational numbers with numerators and denominators relatively prime to 2 and to 3).

(a) Prove that φ is a group isomorphism.

(b) Prove that there are infinitely many isomorphisms of the group G to itself.

(c) Prove that none of the isomorphisms above can be extended to an isomorphism of the *ring* $\mathbb{Q}$ to itself. In fact prove that the identity map is the only ring isomorphism of $\mathbb{Q}$.

2. Let a and b be nonzero elements of the Unique Factorization Domain R. Prove that a and b have a least common multiple (cf. Exercise 11 of Section 1) and describe it in terms of the prime factorizations of a and b in the same fashion that Proposition 13 describes their greatest common divisor.

3. Determine all the representations of the integer $2130797 = 17^2 \cdot 73 \cdot 101$ as a sum of two squares.

4. Prove that if an integer is the sum of two rational squares, then it is the sum of two integer squares (for example, $13 = (1/5)^2 + (18/5)^2 = 2^2 + 3^2$).

5. Let $R = \mathbb{Z}[\sqrt{-n}]$ where n is a squarefree integer greater than 3.

(a) Prove that 2, $\sqrt{-n}$ and $1 + \sqrt{-n}$ are irreducibles in R.

(b) Prove that R is not a U.F.D. Conclude that the quadratic integer ring $\mathcal{O}$ is not a U.F.D. for $D \equiv 2, 3 \bmod 4$, $D < -3$ (so also not Euclidean and not a P.I.D.). [Show that either $\sqrt{-n}$ or $1 + \sqrt{-n}$ is not prime.]

(c) Give an explicit ideal in R that is not principal. [Using (b) consider a maximal ideal containing the nonprime ideal $(\sqrt{-n})$ or $(1 + \sqrt{-n})$.]

6. (a) Prove that the quotient ring $\mathbb{Z}[i]/(1 + i)$ is a field of order 2.

(b) Let $q \in \mathbb{Z}$ be a prime with $q \equiv 3 \bmod 4$. Prove that the quotient ring $\mathbb{Z}[i]/(q)$ is a field with q^2 elements.

(c) Let $p \in \mathbb{Z}$ be a prime with $p \equiv 1 \bmod 4$ and write $p = \pi\bar{\pi}$ as in Proposition 18. Show that the hypotheses for the Chinese Remainder Theorem (Theorem 17 in Section 7.6) are satisfied and that $\mathbb{Z}[i]/(p) \cong \mathbb{Z}[i]/(\pi) \times \mathbb{Z}[i]/(\bar{\pi})$ as rings. Show that the quotient ring $\mathbb{Z}[i]/(p)$ has order p^2 and conclude that $\mathbb{Z}[i]/(\pi)$ and $\mathbb{Z}[i]/(\bar{\pi})$ are both fields of order p.

7. Let π be an irreducible element in $\mathbb{Z}[i]$.

(a) For any integer $n \geq 0$, prove that $(\pi^{n+1}) = \pi^{n+1}\mathbb{Z}[i]$ is an ideal in $(\pi^n) = \pi^n\mathbb{Z}[i]$ and that multiplication by π^n induces an isomorphism $\mathbb{Z}[i]/(\pi) \cong (\pi^n)/(\pi^{n+1})$ as additive abelian groups.

(b) Prove that $|\mathbb{Z}[i]/(\pi^n)| = |\mathbb{Z}[i]/(\pi)|^n$.

(c) Prove for any nonzero α in $\mathbb{Z}[i]$ that the quotient ring $\mathbb{Z}[i]/(\alpha)$ has order equal to $N(\alpha)$. [Use (b) together with the Chinese Remainder Theorem and the results of the previous exercise.]

8. Let R be the quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$ and define the ideals $I_2 = (2, 1 + \sqrt{-5})$, $I_3 = (3, 2 + \sqrt{-5})$, and $I_3' = (3, 2 - \sqrt{-5})$.

(a) Prove that 2, 3, $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are irreducibles in R, no two of which are associate in R, and that $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$ are two distinct factorizations of 6 into irreducibles in R.

(b) Prove that I_2, I_3, and I_3' are prime ideals in R. [One approach: for I_3, observe that $R/I_3 \cong (R/(3))/(I_3/(3))$ by the Third Isomorphism Theorem for Rings. Show that $R/(3)$ has 9 elements, $(I_3/(3))$ has 3 elements, and that $R/I_3 \cong \mathbb{Z}/3\mathbb{Z}$ as an additive abelian group. Conclude that I_3 is a maximal (hence prime) ideal and that $R/I_3 \cong \mathbb{Z}/3\mathbb{Z}$ as rings.]

(c) Show that the factorizations in (a) imply the equality of ideals $(6) = (2)(3)$ and $(6) = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Show that these two ideal factorizations give the same factorization of the ideal (6) as the product of prime ideals (cf. Exercise 5 in Section 2).

9. Suppose that the quadratic integer ring $\mathcal{O}$ is a P.I.D. Prove that the absolute value of the field norm N on $\mathcal{O}$ (cf. Section 7.1) is a Dedekind–Hasse norm on $\mathcal{O}$. Conclude that if the quadratic integer ring $\mathcal{O}$ possesses *any* Dedekind–Hasse norm, then in fact the absolute value of the field norm on $\mathcal{O}$ already provides a Dedekind–Hasse norm on $\mathcal{O}$. [If $\alpha, \beta \in \mathcal{O}$ then $(\alpha, \beta) = (\gamma)$ for some $\gamma \in \mathcal{O}$. Show that if β does not divide α then $0 < |N(\gamma)| < |N(\beta)|$ — use the fact that the units in $\mathcal{O}$ are precisely the elements whose norm is ± 1.]

Remark: If $\mathcal{O}$ is a Euclidean Domain with respect to some norm it is not necessarily true that it is a Euclidean Domain with respect to the absolute value of the field norm (although this is true for $D < 0$, cf. Exercise 8 in Section 1). An example is $D = 69$ (cf. D. Clark, *A quadratic field which is Euclidean but not norm-Euclidean*, Manuscripta Math., 83(1994), pp. 327–330).

10. (*k-stage Euclidean Domains*) Let R be an integral domain and let $N : R \to \mathbb{Z}^+ \cup \{0\}$ be a norm on R. The ring R is Euclidean with respect to N if for any $a, b \in R$ with $b \neq 0$, there exist elements q and r in R with

$$a = qb + r \qquad \text{with } r = 0 \text{ or } N(r) < N(b).$$

Suppose now that this condition is weakened, namely that for any $a, b \in R$ with $b \neq 0$, there exist elements q, q' and r, r' in R with

$$a = qb + r, \quad b = q'r + r' \qquad \text{with } r' = 0 \text{ or } N(r') < N(b),$$

i.e., the remainder after two divisions is smaller. Call such a domain a *2-stage Euclidean Domain.*

(a) Prove that iterating the divisions in a 2-stage Euclidean Domain produces a greatest common divisor of a and b which is a linear combination of a and b. Conclude that every *finitely generated* ideal of a 2-stage Euclidean Domain is principal. (There are 2-stage Euclidean Domains that are *not* P.I.D.s, however.) [Imitate the proof of Theorem 4.]

(b) Prove that a 2-stage Euclidean Domain in which every nonzero nonunit can be factored into a finite number of irreducibles is a Unique Factorization Domain. [Prove first that irreducible elements are prime, as follows. If p is irreducible and $p \mid ab$ with p not dividing a, use part (a) to write $px + ay = 1$ for some x, y. Multiply through by b to conclude that $p \mid b$, so p is prime. Now follow the proof of uniqueness in Theorem 14.]

(c) Make the obvious generalization to define the notion of a k-stage Euclidean Domain for any integer $k \geq 1$. Prove that statements (a) and (b) remain valid if "2-stage Euclidean" is replaced by "k-stage Euclidean."

Remarks: There are examples of rings which are 2-stage Euclidean but are not Euclidean. There are also examples of rings which are not Euclidean with respect to a given norm but which are k-stage Euclidean with respect to the norm (for example, the ring $\mathbb{Z}[\sqrt{14}]$ is not Euclidean with respect to the usual norm $N(a+b\sqrt{14}) = |a^2 - 14b^2|$, but is 2-stage Euclidean with respect to this norm). The k-stage Euclidean condition is also related to the question of whether the group $GL_n(R)$ of invertible $n \times n$ matrices with entries from R is generated by elementary matrices (matrices with 1's along the main diagonal, a single 1 somewhere off the main diagonal, and 0's elsewhere).

11. (*Characterization of P.I.D.s*) Prove that R is a P.I.D. if and only if R is a U.F.D. that is also a Bezout Domain (cf. Exercise 7 in Section 2). [One direction is given by Theorem 14. For the converse, let a be a nonzero element of the ideal I with a minimal number of irreducible factors. Prove that $I = (a)$ by showing that if there is an element $b \in I$ that is not in (a) then $(a, b) = (d)$ leads to a contradiction.]