Remark: Given any integer $d \in \mathbb{Z}$ such that $d \neq 0, 1$ and d does not have any square factor greater than one, the *quadratic field* $\mathbb{Q}(\sqrt{d})$ is the field consisting of all complex numbers of the form $a + ib\sqrt{-d}$ if $d < 0$, and of all the real numbers of the form $a + b\sqrt{d}$ if $d > 0$, with $a, b \in \mathbb{Q}$. The subring of $\mathbb{Q}(\sqrt{d})$ consisting of all elements as above for which $a, b \in \mathbb{Z}$ is denoted by $\mathbb{Z}[\sqrt{d}]$. We define the *ring of integers* of the field $\mathbb{Q}(\sqrt{d})$ as the subring of $\mathbb{Q}(\sqrt{d})$ consisting of the following elements:

(1) If $d \equiv 2 \pmod 4$ or $d \equiv 3 \pmod 4$, then all elements of the form $a + ib\sqrt{-d}$ (if $d < 0$) or all elements of the form $a + b\sqrt{d}$ (if $d > 0$), with $a, b \in \mathbb{Z}$;

(2) If $d \equiv 1 \pmod 4$, then all elements of the form $(a + ib\sqrt{-d})/2$ (if $d < 0$) or all elements of the form $(a + b\sqrt{d})/2$ (if $d > 0$), with $a, b \in \mathbb{Z}$ and with a, b either both even or both odd.

Observe that when $d \equiv 2 \pmod 4$ or $d \equiv 3 \pmod 4$, the ring of integers of $\mathbb{Q}(\sqrt{d})$ is equal to $\mathbb{Z}[\sqrt{d}]$.

It can be shown that the rings of integers of the fields $\mathbb{Q}(\sqrt{-d})$ where $d = 19$, 43, 67, 163 are PID's, but not Euclidean rings. The proof is hard and long. First, it can be shown that these rings are UFD's (refer to Definition 32.2), see Stark [164] (Chapter 8, Theorems 8.21 and 8.22). Then, we use the fact that the ring of integers of the field $\mathbb{Q}(\sqrt{d})$ (with $d \neq 0, 1$ any square-free integers) is a certain kind of integral domain called a Dedekind ring; see Atiyah-MacDonald [8] (Chapter 9, Theorem 9.5) or Samuel [143] (Chapter III, Section 3.4). Finally, we use the fact that if a Dedekind ring is a UFD then it is a PID, which follows from Proposition 32.13.

Actually, the rings of integers of $\mathbb{Q}(\sqrt{d})$ that are Euclidean domains are completely determined but the proof is quite difficult. It turns out that there are twenty one such rings corresponding to the integers: $-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57$ and 73, see Stark [164] (Chapter 8). For more on quadratic fields and their rings of integers, see Stark [164] (Chapter 8) or Niven, Zuckerman and Montgomery [132] (Chapter 9).

It is possible to characterize a larger class of rings (in terms of ideals), *factorial rings (or unique factorization domains)*, for which unique factorization holds (see Section 32.1). We now consider zeros (or roots) of polynomials.

30.6 Roots of Polynomials

We go back to the general case of an arbitrary ring for a little while.

Definition 30.11. Given a ring A and any polynomial $f \in A[X]$, we say that some $\alpha \in A$ is *a zero of f, or a root of f*, if $f(\alpha) = 0$. Similarly, given a polynomial $f \in A[X_1, \ldots, X_n]$, we say that $(\alpha_1, \ldots, \alpha_n) \in A^n$ is a *a zero of f, or a root of f*, if $f(\alpha_1, \ldots, \alpha_n) = 0$.

When $f \in A[X]$ is the null polynomial, every $\alpha \in A$ is trivially a zero of f. This case being trivial, we usually assume that we are considering zeros of nonnull polynomials.