Chapter 6. Quadratic Rings

6.1 Note: Recall that an **integral domain** is a commutative ring with no zero divisors. Note that if u is a unit in a commutative ring R then u cannot be a zero divisor because for all $b\in R$, if $ub=0$ then we have $b=1\cdot b=(u^{-1}u)b=u^{-1}(ub)=u^{-1}\cdot 0=0$. It follows that every field F is an integral domain and hence that every ring R which is a subring of a field F is an integral domain.

6.2 Example: Let $d\in\mathbb{Z}$ with d not a square. When $d>0$ the **real quadratic ring** $\mathbb{Z}[\sqrt{d}\,]$ is an integral domain which is a subring of the field $\mathbb{Q}[\sqrt{d}\,]\subseteq\mathbb{R}$. When $d<0$ $\big($and we write $\sqrt{d}=\sqrt{|d|}\,i\in\mathbb{C}\big)$, the **complex quadratic ring** $\mathbb{Z}[\sqrt{d}\,]$ is an integral domain which is a subring of the field $\mathbb{Q}[\sqrt{d}\,]\subseteq\mathbb{C}$.

6.3 Remark: In most books which define real and complex quadratic rings, they are defined differently. For reasons we shall not delve into here, the quadratic ring in $\mathbb{Q}[\sqrt{d}\,]$ is usually defined to be the set of all elements in $\mathbb{Q}[\sqrt{d}\,]$ which are roots of monic quadratic polynomials over $\mathbb{Z}$. Using this definition, one can show that when d is square-free with $d=3$ mod 4 the quadratic ring in $\mathbb{Q}[\sqrt{d}\,]$ is equal to the ring $\mathbb{Z}[\sqrt{d}\,]$ (in agreement with our definition) but when d is square-free with $d=1$ mod 4 the quadratic ring in $\mathbb{Q}[\sqrt{d}\,]$ is equal to the ring $\mathbb{Z}\big[\frac{1+\sqrt{d}}{2}\big]$ (which properly contains the ring $\mathbb{Z}[\sqrt{d}\,]$).

6.4 Definition: Let $d\in\mathbb{Z}$, with d not a perfect square. For $u\in\mathbb{Q}[\sqrt{d}\,]$ given by $u=x+y\sqrt{d}$ with $x,y\in\mathbb{Q}$, we define the **conjugate** of u in $\mathbb{Q}[\sqrt{d}\,]$ to be the element

$$\overline{u}=x-y\sqrt{d}\in\mathbb{Q}[\sqrt{d}\,].$$

Note that when $d<0$, the conjugate of u in $\mathbb{Q}[\sqrt{d}\,]$ is equal to the complex conjugate of u in $\mathbb{C}$, but when $d>0$ the conjugate of u in $\mathbb{Q}[\sqrt{d}\,]$ is not equal to the complex conjugate of u (which is simply equal to u). The **field norm** in $\mathbb{Q}[\,\sqrt{d}\,]$ is the map $N:\mathbb{Z}[\sqrt{d}\,]\to\mathbb{Q}$ given by $N(u)=u\,\overline{u}$, so for $u=x+y\sqrt{d}$ with $x,y\in\mathbb{Q}$, we have

$$N(u)=u\,\overline{u}=x^2-d\,y^2.$$

Note that when $d<0$, the field norm of u in $\mathbb{Q}[\sqrt{d}\,]$ is equal to the square of the complex norm of u in $\mathbb{C}$, that is we have $N(u)=\|u\|^2$, but when $d>0$ the field norm of u in $\mathbb{Q}[\sqrt{d}\,]$ is not the square of the complex norm, indeed the field norm can take negative values.

6.5 Theorem: *(Properties of the Field Norm) Let N be the field norm in $\mathbb{Q}[\sqrt{d}\,]$ where $d\in\mathbb{Z}$ is not a perfect square. Then*
(1) For all $u,v\in\mathbb{Q}[\sqrt{d}\,]$ we have $\overline{uv}=\overline{u}\,\overline{v}$ and $N(uv)=N(u)N(v)$,
(2) for all $u\in\mathbb{Q}[\sqrt{d}\,]$ we have $N(u)=0\iff u=0$,
(3) for all $u\in\mathbb{Z}[\sqrt{d}\,]$, $N(u)\in\mathbb{Z}$ and we have $N(u)=\pm1\iff u$ is a unit.

Proof: To prove Part 1, note that for $u=r+s\sqrt{d}$ and $v=x+y\sqrt{d}$ wiuth $r,s,x,y\in\mathbb{Q}$ we have

$$uv=(r+s\sqrt{d})(x+y\sqrt{d})=(rx+syd)+(ry+sx)\sqrt{d}\,,\text{ so}$$

$$\overline{u}\,\overline{v}=(r-s\sqrt{d})(x-y\sqrt{d})=(rx+syd)+-(ry+sx)\sqrt{d})=\overline{uv},$$

and hence $N(uv)=uv\,\overline{uv}=uv\,\overline{u}\,\overline{v}=u\overline{u}\,v\overline{v}=N(u)N(v)$.

To prove Part 2, suppose $x+y\sqrt{d}=0$ with $x,y\in\mathbb{Q}$. If $x=0$ then $y\sqrt{d}=-x=0$ hence $y=0$ (since $d\neq 0$). If $y=0$ then $x=-y\sqrt{d}=0$. If $x\neq 0$ and $y\neq 0$ then we have $x=-t\sqrt{d}$ hence $x^2=y^2d$, but this is not possible since d is not a square. Indeed if we let p be a prime factor of d which occurs with an odd exponent in d, then the exponent of p in the rational number x^2 is even (possibly zero or negative if it occurs in the denominator) but the exponent of p in the rational number $-y^2d$ is odd.

To prove part 3, first note that if $u\in\mathbb{Z}[\sqrt{d}\,]$, say $u=a+b\sqrt{d}$ with $a,b\in\mathbb{Z}$, then we have $N(u)=a^2-b^2d\in\mathbb{Z}$. If u is a unit then we can choose $v\in\mathbb{Z}[\sqrt{d}\,]$ such that $uv=1$ and then, by Part 1, we have $N(u)N(v)=N(uv)=N(1)=1$ and so (since $N(u)\in\mathbb{Z}$ and $N(v)\in\mathbb{Z}$) we must have $N(u)=N(v)=1$ or $N(u)=N(v)=-1$. Conversely, if $N(u)=\pm1$ then we have $u\,\overline{u}=N(u)=\pm1$ and so u is a unit with inverse $\pm\,\overline{u}$.

6.6 Theorem: *(Units in Complex Quadratic Rings)*
(1) The units in the ring of Gaussian integers $\mathbb{Z}[\sqrt{-1}]$ are ±1 and $\pm i$.
(2) When $d\in\mathbb{Z}$ with $d<-1$, the only units in the ring $\mathbb{Z}[\sqrt{d}\,]$ are ±1.

Proof: The proof is left as an exercise (use the fact that for $d<0$ the units $u\in\mathbb{Z}[\sqrt{d}\,]$ are the elements with $N(u)=\|u\|^2=\pm1$).

6.7 Remark: The problem of determining the units in real quadratic rings is considerably more difficult than for complex quadratic rings, and we shall make use of the following theorem about using rational numbers to approximate irrational numbers.

6.8 Theorem: *(Dirichlet's Approximation Theorem) Let $x\in\mathbb{R}\setminus\mathbb{Q}$.*
(1) For every $n\in\mathbb{Z}^+$ there exist $p,q\in\mathbb{Z}$ with $1\leq q\leq n$ such that $|qx-p|<\frac{1}{n}$.
(2) There exist infinitely many pairs (p,q) with $p\in\mathbb{Z}$ and $q\in\mathbb{Z}^+$ such that $\left|x-\frac{p}{q}\right|<\frac{1}{q^2}$.

Proof: Let us prove Part 1. When $n=1$ we can take $q=1$ and $p=\lfloor x\rfloor$. Let $2\leq n\in\mathbb{Z}$ and let $\langle x\rangle=x-\lfloor x\rfloor$. Since $[0,1]$ is the union of the n intervals $\left[\frac{k-1}{n},\frac{k}{n}\right]$ with $1\leq k\leq n$, it follows that some two of the $n+1$ numbers $0,1,\langle x\rangle,\langle 2x\rangle,\cdots,\langle(n-1)x\rangle$ must lie in the same interval. Thus either there exists an index k such that $\langle kx\rangle\leq\frac{1}{n}$ or there exists an index k such that $1-\langle kx\rangle\leq\frac{1}{n}$ or there exist indices $k<\ell$ such that $\big|\langle\ell x\rangle-\langle kx\rangle\big|\leq\frac{1}{n}$. In the case that $\langle kx\rangle\leq\frac{1}{n}$ we can choose $q=k$ and $p=\lfloor kx\rfloor$ to get $|qx-p|=\big|kx-\lfloor kx\rfloor\big|=\langle kx\rangle\leq\frac{1}{n}$. In the case that $1-\langle kx\rangle\leq\frac{1}{n}$ we can choose $q=k$ and $p=\lfloor kx\rfloor+1$ to get $\big|qx-p\big|=\big|kx-(\lfloor kx\rfloor+1)\big|=1-\langle kx\rangle\leq\frac{1}{n}$. In the case that $k<\ell$ and $\big|\langle\ell x\rangle-\langle kx\rangle\big|\leq\frac{1}{n}$, we can choose $q=\ell-k$ and $p=\lfloor\ell x\rfloor-\lfloor kx\rfloor$ to get

$$\big|qx-p\big|=\big|(\ell-k)x-(\lfloor\ell x\rfloor-\lfloor kx\rfloor)\big|=\big|\big(\ell x-\lfloor\ell x\rfloor\big)-\big(kx-\lfloor kx\rfloor\big)\big|=\big|\langle\ell x\rangle-\langle kx\rangle\big|\leq\tfrac{1}{n}.$$

In all cases we can choose $p,q\in\mathbb{Z}$ such that $|qx-p|\leq\frac{1}{n}$. Finally, note that the inequality must be strict because $x\notin\mathbb{Q}$.

Part 2 follows easily from Part 1. We begin by choosing $n_1\in\mathbb{Z}^+$ and $p_1,q_1\in\mathbb{Z}$ with $1\leq q_1\leq n_1$ such that $|q_1x-p_1|<\frac{1}{n_1}$. Dividing by q_1 gives $\left|x-\frac{p_1}{q_1}\right|<\frac{1}{q_1n_1}\leq\frac{1}{{q_1}^2}$. Then we choose $n_2\in\mathbb{Z}^+$ with $\frac{1}{n_2}\leq|q_1x-p_1|$ and we choose $p_2,q_2\in\mathbb{Z}$ with $1\leq q_2\leq n_2$ such that $|q_2x-p_2|<\frac{1}{n_2}$. Dividing by q_2 gives $\left|x-\frac{p_2}{q_2}\right|<\frac{1}{q_2n_2}\leq\frac{1}{{q_2}^2}$. We note that since $|q_2x-p_2|<\frac{1}{n_2}\leq|q_1x-p_1|$ we cannot have $(p_1,q_1)=(p_2,q_2)$. We then repeat the procedure.

6.9 Remark: Dirichlet's Approximation Theorem can also be proven using properties of continued fractions. Indeed Theorem 7.5 shows that an irrational number x is closely approximated by each of the convergents $\frac{p_n}{q_n}$ of its continued fraction, with $\left|x-\frac{p_n}{q_n}\right|<\frac{1}{{q_n}^2}$.

6.10 Theorem: *(Units in Real Quadratic Rings) Let $d \in \mathbb{Z}^+$ be a non-square.*
(1) For a unit $u = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}\,]$, with $a, b \in \mathbb{Z}$, we have $u > 1 \iff \big(a > 0$ and $b > 0\big)$.
(2) There exists a unique smallest unit $u \in \mathbb{Z}[\sqrt{d}\,]$ with $u > 1$, and the set of all units in $\mathbb{Z}[\sqrt{d}\,]$ is equal to the set $\mathbb{Z}[\sqrt{d}\,]^* = \big\{\pm u^k \big| k \in \mathbb{Z}\big\}$.

Proof: To prove Part 1, let $u \in \mathbb{Z}[\sqrt{d}\,]$ be a unit and say $u = a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$. If $a > 0$ and $b > 0$ then $u = a + b\sqrt{d} \geq 1 + \sqrt{d} > 1$. Suppose, conversely that $u > 1$. Note that $a \neq 0$ (since $N(0 + b\sqrt{d}) = b^2 d$ which cannot be equal to ± 1 because $b \in \mathbb{Z}$ and $d \geq 2$) and $b \neq 0$ since if $b = 0$ then $u = a$ and $N(u) = a^2 = \pm 1$ so that $u = a = \pm 1$. Let $v = |a| + |b|\sqrt{d}$ and note that $v > 1$, that is $v \in (1, \infty)$. Note that the four elements $\pm v$ and $\pm\frac{1}{v}$ are all units with $v \in (1, \infty)$, $\frac{1}{v} \in (0, 1)$, $-\frac{1}{v} \in (-1, 0)$ and $-v \in (-\infty, -1)$. Also note that the four elements $\pm v$ and $\pm\overline{v}$ (that is the four elements $\pm|a| \pm |b|\sqrt{d}$) are also all units because $N(\pm|a| \pm |b|\sqrt{d}) = a^2 - b^2 d = N(u) = \pm 1$. Since $\frac{1}{v} = \frac{1}{|a|+|b|\sqrt{d}} = \frac{|a|-|b|\sqrt{d}}{a^2-b^2d} = \frac{\overline{v}}{N(v)} = \pm\,\overline{v}$ we see that the two elements $\pm\,\overline{v}$ are equal to the two elements $\pm\frac{1}{v}$. Thus the four units $\pm\, v, \pm\,\overline{v}$ (in some order) are equal to the four units $\pm\, v, \pm\,\frac{1}{v}$ and each of these four lies in a different one of the four intervals $(-\infty, -1)$, $(-1, 0)$, $(0, 1)$, $(1, \infty)$. Since $u = a + b\sqrt{d} > 1$, it follows that u is the only one of the four elements $\pm\, v, \pm\,\overline{v}$ which lies in the interval $(1, \infty)$, so we must have $u = v$, that is $a = |a| > 0$ and $b = |b| > 0$.

Next, we shall use Dirichlet's Approximation Theorem to prove that there exists at least one unit $w \in \mathbb{Z}[\sqrt{d}\,]$ with $w > 1$. By Dirichlet's Theorem, there exist infinitely many pairs (p, q) with $p \in \mathbb{Z}$ and $q \in \mathbb{Z}^+$ such that $\left|\frac{p}{q} - \sqrt{d}\right| < \frac{1}{q^2}$. For such pairs we have $\sqrt{d} - \frac{1}{q^2} < \frac{p}{q} < \sqrt{d} + \frac{1}{q^2}$ so that $2\sqrt{d} - \frac{1}{q^2} < \frac{p}{q} + \sqrt{d} < 2\sqrt{d} + \frac{1}{q^2}$, hence $\left|\frac{p}{q} + \sqrt{d}\right| < 2\sqrt{d} + \frac{1}{q^2} \leq 2\sqrt{d} + 1$, and so

$$\big|N(p + q\sqrt{d})\big| = \big|p^2 - q^2 d\big| = q^2\big|\tfrac{p}{q} - \sqrt{d}\big|\big|\tfrac{p}{q} + \sqrt{d}\big| < q^2 \cdot \tfrac{1}{q^2} \cdot (2\sqrt{d} + 1) = 2\sqrt{d} + 1.$$

It follows that we can choose $m \in \mathbb{Z}$ with $|m| \leq 2\sqrt{d} + 1$ such that there exists infinitely many pairs (p, q) with $p \in \mathbb{Z}$, $q \in \mathbb{Z}^+$ such that $N(p + q\sqrt{d}) = m$. We note that $m \neq 0$ since there is only one pair (p, q) with $N(p + q\sqrt{d}) = 0$, namely $(p, q) = (0, 0)$. Next we choose $r, s \in \mathbb{Z}_m$ such that there exist infinitely many pairs (p, q) with $p \in \mathbb{Z}$, $q \in \mathbb{Z}^+$ such that $N(p + q\sqrt{d}) = m$ and $p = r \bmod m$ and $q = s \bmod m$. Let (p_1, q_1) and (p_2, q_2) be any two such pairs and let $u_1 = p_1 + q_1\sqrt{d}$ and $u_2 = p_2 + q_2\sqrt{d}$. Then we have $0 \neq u_1, u_2 \in \mathbb{Z}[\sqrt{d}\,]$ and $N(u_1) = N(u_2) = m$ and $p_1 = p_2 = r \bmod m$ and $q_1 = q_2 = s \bmod m$. Working in the field $\mathbb{Q}[\sqrt{d}\,]$ (where u_2 is invertible) we have $N(u_2)N\big(\frac{1}{u_2}\big) = N\big(u_2 \cdot \frac{1}{u_2}\big) = N(1) = 1$ so that $N\big(\frac{1}{u_2}\big) = \frac{1}{N(u_2)}$, and hence

$$N\big(\tfrac{u_1}{u_2}\big) = N\big(u_1 \cdot \tfrac{1}{u_2}\big) = N(u_1)N\big(\tfrac{1}{u_2}\big) = \tfrac{N(u_1)}{N(u_2)} = \tfrac{m}{m} = 1.$$

Also note that the element $\frac{u_1}{u_2} \in \mathbb{Q}[\sqrt{d}\,]$ actually lies in $\mathbb{Z}[\sqrt{d}\,]$ because we have $p_1 = p_2 \bmod m$ and $q_1 = q_2 \bmod m$ and

$$\tfrac{u_1}{u_2} = 1 + \tfrac{u_1 - u_2}{u_2} = 1 + \tfrac{u_1 - u_2}{u_2\,\overline{u_2}}\,\overline{u_2} = 1 + \tfrac{(p_1 + q_1\sqrt{d}) - (p_2 + q_2\sqrt{d})}{m}\,\overline{u_2} = 1 + \Big(\tfrac{p_1 - p_2}{m} + \tfrac{q_1 - q_2}{m}\sqrt{d}\Big)\overline{u_2}.$$

Thus the element $\frac{u_1}{u_2}$ is a unit in $\mathbb{Z}[\sqrt{d}\,]$. Since for each choice of u_2 there are infinitely many choices of u_1, this proves that there exist infinitely many units in $\mathbb{Z}[\sqrt{d}\,]$. If we let $v \in \mathbb{Z}[\sqrt{d}\,]$ be any unit with $v \neq \pm 1$ then, as in the proof of Part 1, each of the four units $\pm\, v$, $\pm\frac{1}{v}$ lies in a different one of the four intervals $(-\infty, -1)$, $(-1, 0)$, $(0, 1)$ and $(1, \infty)$. In particular, there exists at least one unit $w \in \mathbb{Z}[\sqrt{d}\,]$ with $w > 1$.

Since there exists at least one unit $w \in \mathbb{Z}[\sqrt{d}\,]$ with $w > 1$, it is easy to see that there is a unique smallest unit $u \in \mathbb{Z}[\sqrt{d}\,]$ with $u > 1$. Fix one particular unit $w \in \mathbb{Z}[\sqrt{d}\,]$ with $w > 1$. For $a, b \in \mathbb{Z}$, if $u = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}\,]$ is a unit with $1 < u \leq w$ then (by Part 1) we must have $0 < a \leq u \leq w$ and $0 < b < b\sqrt{d} \leq u \leq w$ so there are only finitely many choices for a and b. Thus there are only finitely many units $u \in \mathbb{Z}[\sqrt{d}\,]$ with $1 < u \leq w$.

Finally we claim that when u is the smallest unit in $\mathbb{Z}[\sqrt{d}\,]$ with $u > 1$, the set of all units in $\mathbb{Z}[\sqrt{d}\,]$ is equal to the set $\big\{ \pm\, u^k \big| k \in \mathbb{Z} \big\}$. Since u is a unit it follows that $\pm\, u^k$ is a unit for all $k \in \mathbb{Z}$, indeed the inverse of u^k is equal to u^{-k} and the inverse of $-u^k$ is equal to $-u^{-k}$. We need to show that every unit in $\mathbb{Z}[\sqrt{d}\,]$ is equal to $\pm u^k$ for some $k \in \mathbb{Z}$. Let v be any unit in $\mathbb{Z}[\sqrt{2}]$. Suppose first that $v > 0$. Since $u > 1$ we have $\cdots u^{-2} < u^{-1} < u^0 < u^1 < u^2 < \cdots$ with $u^k \to \infty$ and $u^{-k} \to 0$ as $k \to \infty$, and so we can choose $k \in \mathbb{Z}$ so that $u^k \leq v < u^{k+1}$. We claim that $u^k = v$. Suppose, for a contradiction, that $u^k < v < u^{k+1}$. Then we have $1 < \frac{v}{u^k} < u$. This is not possible since $\frac{v}{u^k}$ is a unit (since v and u are units) but u is the smallest unit with $u > 1$. Thus we have $u^k = v$, as claimed. Now suppose that $v < 0$. Then since $-v$ is a unit witth $-v > 0$, as we just showed we can choose $k \in \mathbb{Z}$ so that $-v = u^k$ and then we have $v = -u^k$.

6.11 Note: Given a non-square $d \in \mathbb{Z}^+$, we can find the smallest unit $u = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}\,]$ with $u > 1$ as follows. Since we need to have $N(u) = a^2 - b^2 d = \pm 1$ we can try values $b = 1, 2, 3, \cdots$ until we find the smallest $b \in \mathbb{Z}^+$ such that $b^2 d$ differs from a square by ± 1, that is such that $b^2 d = a^2 \pm 1$ for some $a \in \mathbb{Z}^+$. Then $u = a + b\sqrt{d}$ is the smallest possible unit $u \in \mathbb{Z}[\sqrt{d}\,]$ with $u > 1$. Indeed if $v = r + s\sqrt{d}$ is a unit with $r, s \in \mathbb{Z}^+$ and $s > b$ then, since $r^2 - s^2 d = N(v) = \pm 1$, we must have $r^2 = s^2 d \pm 1 \geq (b+1)^2 d - 1 > b^2 d + 1 \geq a^2$ and so we have $r > a$ and $s > b$ so that $v = r + s\sqrt{d} > a + b\sqrt{d} = u$.

6.12 Example: Find all of the units in the real quadratic ring $\mathbb{Z}[\sqrt{7}]$.

Solution: We have

b	1	2	3
$7b^2$	7	28	63

We see that the smallest value of $b \in \mathbb{Z}^+$ for which $7b^2$ differs from a square by ± 1 is $b = 3$ and, in this case, we have $7b^2 = 63 = a^2 - 1$ for $a = 8$. Thus the smallest unit $u \in \mathbb{Z}[\sqrt{7}]$ with $u > 1$ is $u = 8 + 3\sqrt{7}$. The set of all units in $\mathbb{Z}[\sqrt{7}]$ is the set $\big\{ \pm\, (8 + 3\sqrt{7})^k \big| k \in \mathbb{Z} \big\}$.

6.13 Remark: The method described in Note 6.11 (and used in Example 6.12) to find the smallest unit $u \in \mathbb{Z}[\sqrt{d}\,]$ with $u > 1$ can be quite tedious for large values of d. Another more efficient algorithm, which uses continued fractions, is described in the next chapter.

6.14 Definition: Let R be a commutative ring. Let $a, b \in R$. We say that a **divides** b (or a is a **divisor** or **factor** of b, or b is a **multiple** of a), and we write $a\big|b$, when $b = ar$ for some $r \in R$. We say that a and b are **associates**, and we write $a \sim b$, when $a\big|b$ and $b\big|a$. Note that association is an equivalence relation meaning that for all $a, b, c \in R$ we have $a \sim a$, and if $a \sim b$ then $b \sim a$, and if $a \sim b$ and $b \sim c$ then $a \sim c$. The equivalence classes are called **association classes**.

6.15 Example: In the ring $\mathbb{Z}$, for $a, b \in \mathbb{Z}$ we have $a \sim b \iff b = \pm a$.

6.16 Example: Verify that the association classes in the ring $\mathbb{Z}_{12}$ are $\{0\}$, $\{1, 5, 7, 11\}$, $\{2, 10\}$, $\{3, 9\}$, $\{4, 8\}$ and $\{6\}$.

6.17 Theorem: *Let R be a commutative ring. Let $a, b \in R$. Then*

(1) $a \sim b$ if and only if a and b have the same multiples and divisors,
(2) $a \sim 0$ if and only if $a = 0$,
(3) $a \sim 1$ if and only if a is a unit.
(4) if R is an integral domain then $a \sim b$ if and only if $b = au$ for some unit $u \in R$.

Proof: We prove Part 4 and leave the proofs of the other parts as an exercise. Note that if $b = au$ where u is a unit in R, then since $b = au$ we have $a\big|b$, and since $a = bu^{-1}$ we have $b\big|a$, and so $a \sim b$. Suppose that R is an integral domain and that $a \sim b$. Since $a\big|b$ we can choose $u \in R$ such that $b = au$, and since $b\big|a$ we can choose $v \in R$ so that $a = bv$. Then we have $b = au = bvu$ hence $b - bvu = 0$ and so $b(1 - vu) = 0$. Since R is an integral domain (so there are no zero divisors), it follows that either $b = 0$ or $vu = 1$. If $vu = 1$ then u (and also v) is a unit and we have $b = au$. If $b = 0$ then we also have $a = bu = 0 \cdot u = 0$ and so $b = a \cdot 1$.

6.18 Example: By Part 4 of the above theorem together with Theorem 6.6 (Units in Complex Quadratic Rings), the associates of an element $a \in \mathbb{Z}[\sqrt{-1}]$ are the elements $\pm a$ and $\pm i\, a$ and when $d \in \mathbb{Z}$ with $d < -1$ the associates of $a \in \mathbb{Z}[\sqrt{d}\,]$ are the elements $\pm a$. By Part 4 above together with Theorem 6.10 (Units in Real Quadratic Rings), when $d \in \mathbb{Z}^+$ is a non-square, the associates of an element $a \in \mathbb{Z}[\sqrt{d}\,]$ are the elements $\pm au^k$ with $k \in \mathbb{Z}$, where u is the smallest unit in $\mathbb{Z}[\sqrt{d}\,]$ with $u > 1$.

6.19 Definition: Let R be a commutative ring. Let $a \in R$ be a non-zero non-unit. We say that a is **reducible** when $a = bc$ for some non-units $b, c \in R$, and otherwise we say that a is **irreducible**. Note that if a is irreducible then the divisors of a are the units and the associates of a. We say that a is **prime** when for all $b, c \in R$, if $a\big|bc$ then either $a\big|b$ or $a\big|c$.

6.20 Example: In the ring $\mathbb{Z}$, for $a \in \mathbb{Z}$, a is irreducible if and only if a is prime if and only if $a = \pm p$ for some (positive) prime number p.

6.21 Example: As an exercise, verify that in the ring $\mathbb{Z}_{12}$, the irreducible elements are 2 and 10 and the prime elements are 2, 3, 9 and 10 (the element 3 is reducible because, for example, $3 = 3 \cdot 9 = 3 \cdot 3 \cdot 3$).

6.22 Theorem: *Let R be a commutative ring. Let $a, b \in R$ be non-zero non-units with $a \sim b$. Then*

(1) a is reducible if and only if b is reducible,
(2) a is irreducible if and only if b is irreducible,
(3) a is prime if and only if b is prime,
(4) if R is an integral domain and a is prime, then a is irreducible.

Proof: We prove Part 4 and leave the proofs of the other parts as an exercise. Suppose that R is an integral domain and that $a \in R$ is prime. Suppose that $a = bc$ where $b, c \in R$. Since $a = bc$ we have $a \big| bc$ and hence (since a is prime) either $a \big| b$ or $a \big| c$. Suppose that $a \big| b$, say $b = ad$ where $d \in R$. Then we have $a = bc = adc$ and so $a - adc = 0$ hence $a(1 - dc) = 0$. Since $a \neq 0$ and R is an integral domain (so there are no zero divisors) we must have $1 - dc = 0$, hence $dc = 1$. Thus c is a unit (with $c^{-1} = d$). Similarly, if $a \big| c$ then b is a unit.

6.23 Example: Show that in the ring $\mathbb{Z}[\sqrt{-3}]$, $1+\sqrt{-3}$ is irreducible but not prime.

Solution: Let N be the field norm in $\mathbb{Q}[\sqrt{3}\,i]$. Note that $N(1 + \sqrt{3}\,i) = 4$. If we had $1+\sqrt{3}\,i = uv$ for some non-units $u, v \in \mathbb{Z}[\sqrt{3}\,i]$ then we would have $N(u) > 1$ and $N(v) > 1$ and $N(u)N(v) = N(uv) = N(1 + \sqrt{3}\,i) = 4$, and hence we would have $N(u) = N(v) = 2$. But for $u = a + b\sqrt{3}\,i$ with $a, b \in \mathbb{Z}$ we have $N(u) = N(a + b\sqrt{3}\,i) = a^2 + 3b^2 = a^2 \bmod 3$ so that $N(u) \neq 2 \bmod 3$. Thus the element $1 + \sqrt{3}\,i$ is irreducible. On the other hand, $1 + \sqrt{3}\,i$ is not prime because $(1 + \sqrt{3}\,i)(1 - \sqrt{3}\,i) = 4 = 2^2$ so that $(1 + \sqrt{3}\,i)\big| 2^2$, but $(1 + \sqrt{3}\,i)\not\big| 2$ because, working in the field $\mathbb{Q}[\sqrt{3}\,i]$, we have $\frac{2}{1+\sqrt{3}\,i} = \frac{1-\sqrt{3}\,i}{2} \notin \mathbb{Z}[\sqrt{3}\,i]$.

6.24 Example: Use the method of the Sieve of Eratosthenes to find all irreducible elements $u \in \mathbb{Z}[i]$ with $N(u) \leq 50$.

Solution: Draw a grid of unit squares to represent $\mathbb{Z}[i\,]$ showing all the points $x + iy$ with $x^2 + y^2 \leq 50$. Cross off 0 and cross off the units $\pm 1, \pm i$. Circle the remaining elements of smallest norm, namely $\pm 1 \pm i$ (they are irreducible, and they are associates of each other). Cross off multiples of $1 + i$ in $\mathbb{Z}[i\,]$, that is cross off elements of the form $(1 + i)(a + bi)$ with $a, b \in \mathbb{Z}$ (note that these elements form a grid of squares of side length $\sqrt{2}$). Circle the remaining elements of smallest norm, namely the elements $\pm 2 \pm i$ and $\pm 1 \pm 2i$ (they are irreducible with 4 of them associate to $2 + i$ and the other 4 associate to $1 + 2i$). Cross off the multiples of $2 + i$ in $\mathbb{Z}[i]$, that is cross off the elements of the form $(2 + i)(a + bi)$ with $a, b \in \mathbb{Z}$ (note that these elements form a grid of squares of side length $\sqrt{5}$) and also cross off the multiples of $1 + 2i$ (these also form a grid of squares of side length $\sqrt{5}$). Circle the remaining elements of smallest norm, namely the elements $\pm 3, \pm 3i$ (they are irreducible, and they are associates). Cross off the multiples of 3 (actually you will find that you have already crossed off all the multiples of 3 which lie in the circle $x^2 + y^2 \leq 50$). At this stage, since $N(3) = 9 \geq \sqrt{50}$ we can circle all of the remaining elements (they are all irreducible). In order of increasing norm, the irreducible elements $u \in \mathbb{Z}[i\,]$ with $N(u) \leq 50$ are $\pm 1 \pm i$, $\pm 2 \pm i$, $\pm 1 \pm 2i$, ± 3, $\pm 3i$, $\pm 3 \pm 2i$, $\pm 2 \pm 3i$, $\pm 4 \pm i$, $\pm 1 \pm 4i$, $\pm 5 \pm 2i$, $\pm 2 \pm 5i$, $\pm 6 \pm, i$, $\pm 1 \pm 6i$, $\pm, 7$, $\pm 7i$.

6.25 Remark: We shall obtain a more complete description of the irreducible elements in $\mathbb{Z}[i]$ when we study sums of squares in the chapter on Diophantine equations.

6.26 Definition: A **Euclidean domain** (or ED) is an integral domain R together with a function $E : R \to \mathbb{N}$, called a **Euclidean norm**, such that

E1. for all $a \in R$ we have $E(a) = 0 \Longleftrightarrow a = 0$,
E2. for all $a \in R$ we have $E(a) = 1 \Longleftrightarrow a$ is a unit,
E3. for all $a, b \in R$, if $a \sim b$ then $E(a) = E(b)$,
E4. for all nonzero nonunits $a, b, c \in R$, if $a = bc$ then $E(b) < E(a)$ and $E(c) < E(a)$,
E5. for all $a, b \in R$ with $b \neq 0$ there exist $q, r \in R$ such that $a = qb + r$ and $E(r) < E(b)$.

6.27 Example: $\mathbb{Z}$ is a Euclidean domain using the Euclidean norm $E : \mathbb{Z} \to \mathbb{N}$ given by $E(a) = |a|$.

6.28 Example: Every field is a Euclidean domain, using the function $E : R \to \mathbb{N}$ given by $E(0) = 0$ and $E(a) = 1$ for all $a \neq 0$.

6.29 Example: If F is a field then the polynomial ring $F[x]$ is a Euclidean domain with Euclidean norm $E(f) = \deg(f) + 1$ (where we follow the convention that $\deg(0) = -1$ so that $E(0) = 0$).

6.30 Exercise: Show that for each $d \in \{-2, -1, 2, 3\}$ the ring $\mathbb{Z}\big[\sqrt{d}\,\big]$ is a Euclidean domain with Euclidean norm given by $E(u) = \big|N(u)\big|$, that is $E(a + b\sqrt{d}) = \big|a^2 - db^2\big|$.

6.31 Definition: Let R be a Euclidean domain with Euclidean norm E. For $a, b \in R$ with a and b not both zero, a **greatest common divisor** of a and b is an element $d \in R$ with $d\big|a$ and $d\big|b$ such that $E(d) \geq E(c)$ for every $c \in R$ with $c\big|a$ and $c\big|b$. Note that greatest common divisors are unique up to association, meaning that when d is one common divisor of a and b, the set of all common divisors of a and b is the set of associates of d. When d is one of the greatest common divisors of a and b we often write $d = \gcd(a, b)$. For convenience, we also write $0 = \gcd(0, 0)$.

6.32 Theorem: *(Bézout's Identity) Let R be a Euclidean domain with Euclidean norm E and let $a, b \in R$ with a and b not both zero. Then the Euclidean Algorithm, with Back Substitution, can be applied to find a greatest common divisor d of a and b, and to find elements $s, t \in R$ such that $as + bt = d$.*

Proof: The proof is almost identical to the proof of Bézout's Identity in $\mathbb{Z}$ (Theorem 1.7).

6.33 Corollary: *Let R be a Euclidean domain and let $a, b \in R$.*
(1) If $d = \gcd(a, b)$ and $c \in R$ with $c\big|a$ and $c\big|b$ then $c\big|d$.
(2) If $a\big|bc$ and $\gcd(a, b) = 1$ then $a\big|c$.
(3) For all $p \in R$, p is irreducible if and only if p is prime.

Proof: The proof is left as an exercise (imitate the proofs of Theorems 1.10 and 1.16).

6.34 Definition: A **unique factorization domain** (or UFD) is an integral domain R with the property that for every nonzero non-unit $a \in R$ we have
(1) $a = p_1 p_2 \cdots p_\ell$ for some $\ell \in \mathbb{Z}^+$ and some irreducible elements $p_i \in R$, and
(2) if $a = p_1 p_2 \cdots p_\ell = q_1 q_2 \cdots q_m$ where $\ell, m \in \mathbb{Z}^+$ and each p_i and q_j is irreducible, then $m = \ell$ and for some bijection $\sigma : \{1, 2, \cdots, \ell\} \to \{1, 2, \cdots, \ell\}$ we have $a_i \sim b_{\sigma(i)}$ for all i.

6.35 Theorem: *Every Euclidean domain is a unique factorization domain.*

Proof: The proof is left as an exercise (imitate the proof of unique factorization in $\mathbb{Z}$).

6.36 Exercise: Show that the rings $\mathbb{Z}\big[\sqrt{3}\,i\big]$ and $\mathbb{Z}\big[\sqrt{5}\,\big]$ are not unique factorization domains.