Notes on Quadratic Number Rings

1. Ideals.

Definition 1.1. A *quadratic number ring* is a subring of the complex numbers which is free of rank 2 as an abelian group.

Lemma 1.2. Let A be a free abelian group on 2 generators, and let $\alpha \in A$. Then A has a generating set $\{\alpha, \beta\}$ exactly when α is not *divisible*: that is, exactly when $n\gamma = \alpha$, for $n \in \mathbb{Z}, \gamma \in A$, implies that $n = \pm 1$.

Let A be a quadratic number ring. Suppose $\frac{1}{n} \in A$. Then all fractions of the form $\frac{m}{n^k}$ lie in A. But the set of such numbers forms an abelian group which is not finitely generated. The conclusion is that we may take 1 as one of the two abelian group generators of A.

If $\{1, \alpha\}$ generates A, then $\alpha^2 \in A$ implies that α satisfies a *monic* quadratic polynomial

$$x^2 + bx + c = 0.$$

If $\alpha \in \mathbb{Q}$, then the discriminant $d = b^2 - 4c$ is a square, so in fact $\alpha \in \mathbb{Z}$. In general, a number satisfying an equation of this form is a *quadratic integer*; a rational quadratic integer is an ordinary ("rational") integer.

Proposition 1.3. If α and β are two quadratic integers of discriminant d, then the quadratic number rings $\langle 1, \alpha \rangle$ and $\langle 1, \beta \rangle$ coincide.

This ring thus depends only on the discriminant d; write $A(d)$ for it, and call it the quadratic number ring of discriminant d. There is one for each *discriminant*, i.e., each nonsquare $d \equiv 0, 1 \pmod 4$. For example, let

$$\omega = \frac{\sqrt{d}}{2} \text{ if } d \equiv 0 \pmod 4, \quad \omega = \frac{1 + \sqrt{d}}{2} \text{ if } d \equiv 1 \pmod 4.$$

Then in either case the discriminant of ω is d, and in either case ω is a quadratic integer (being a root of $x^2 - \frac{d}{4} = 0$ or $x^2 - x - \frac{d-1}{4}$ respectively), so $A(d) = \langle 1, \omega \rangle$. (We use the notation $\langle \alpha, \beta \rangle$ to denote the free abelian group of rank 2 generated by α and β.)

Proposition 1.4. (a) $A(d) = \{\frac{t+u\sqrt{d}}{2} : t, u \in \mathbb{Z}, t \equiv du \pmod 2\}$.
(b) The map $\{(t, u) \in \mathbb{Z} \times \mathbb{Z} : t^2 - du^2 = \pm 4\} \to A(d)^*$ sending (t, u) to $\frac{t+u\sqrt{d}}{2}$ is bijective.

(b) is true because $N(\frac{t+u\sqrt{d}}{2}) = \frac{t^2-du^2}{2}$. This equation forces $t \equiv du \pmod 2$. And $\alpha \in A(d)$ is a unit if and only if its norm is ± 1.

Corollary 1.5. $A(d)$ consists of the rational integers together with the quadratic irrational integers of discriminant $f^2 d$ for $f \in \mathbb{N}$.

A discriminant d is *fundamental* if and only if it is not of the form $f^2\delta$, where f is an integer greater than 1 and δ is again a discriminant. (Warning: one fundamental discriminant may divide another: 12 divides 24, for example.) If d is a fundamental discriminant, then $A(d)$ is the set of all quadratic integers in the field $\mathbb{Q}(\sqrt{d})$. Any discriminant d factors uniquely as $f^2\delta$, where $f \in \mathbb{N}$ and δ is a fundamental discriminant. $A(d)$ is then a subring of $A(\delta)$. The positive integer f is the *conductor* of d or of $A(d)$.

Let $\mathfrak{a}$ be an ideal in $A = A(d)$. If $\mathfrak{a} \neq 0$, then for any nonzero $\alpha \in \mathfrak{a}$, the principal ideal (α) is a free abelian group of rank 2 inside $\mathfrak{a}$. $\mathfrak{a}$ thus has rank at least 2, and, since it in turn lies inside A, it must have rank exactly 2.

One way to generate such ideals is by means of a quadratic irrational $\alpha = \frac{-b+\sqrt{d}}{2a}$ of discriminant d. Let $\mathfrak{a} = \langle a, \frac{-b+\sqrt{d}}{2} \rangle$. We claim this is an ideal. In fact, for any subset X of $\mathbb{Q}(\sqrt{d})$, define

$$B(X) = \{\beta \in \mathbb{Q}(\sqrt{d}) : \beta X \subseteq X\}.$$

Proposition 1.6. With α and $\mathfrak{a}$ as above, $B(\mathfrak{a}) = A(d)$.

Proof. Clearly, $B(\zeta X) = B(X)$; so the Proposition is equivalent to the statement that

$$B(\langle 1, \alpha \rangle) = A(d),$$

Now $\beta \in B(\langle 1, \alpha \rangle)$ if and only if

$$\text{(i) } \beta \in \langle 1, \alpha \rangle, \quad \text{and} \quad \text{(ii) } \beta\alpha \in \langle 1, \alpha \rangle.$$

From (i), $\beta = m + n\alpha$. Then

$$\beta\alpha = m\alpha + n\alpha^2 = m\alpha + n(-\frac{b}{a}\alpha - \frac{c}{a}) = (m - \frac{nb}{a})\alpha - \frac{nc}{a}.$$

Now (ii) is equivalent to the requirement that nb and nc both be divisible by a. But $\gcd\{a, b, c\} = 1$ then forces $a|n$, so $\beta = m + ka\alpha$, $m, k \in \mathbb{Z}$. Since $a\alpha$ is a quadratic integer of discriminant d, this is equivalent to $\beta \in A(d)$. ∎

Corollary 1.7. Given d, and an irrational $\alpha \in \mathbb{Q}(\sqrt{d})$, $\langle 1, \alpha \rangle$ is a fractional ideal for $A(d)$ if and only if $d = u^2 D(\alpha)$ for some integer u; it is proper if and only if $D(\alpha) = d$.

Here: a *fractional ideal* for A is a subgroup $\mathfrak{b}$ of $\mathbb{Q}(\sqrt{d})$ such that there exists a number $\zeta \in \mathbb{Q}(\sqrt{d})^*$ and an ideal $\mathfrak{a}$ of A such that $\mathfrak{b} = \zeta\mathfrak{a}$; $D(\alpha)$ denotes the discriminant of α; and a fractional ideal $\mathfrak{a}$ for A is *proper* if and only if $B(\mathfrak{a}) = A$.

Corollary 1.8. If d is a fundamental discriminant, then every fractional ideal for $A(d)$ is proper.

For, any nonzero ideal $\mathfrak{a}$ has the form $\langle \alpha, \beta \rangle$, and then $B(\mathfrak{a}) = B(\langle 1, \frac{\beta}{\alpha} \rangle)$.

We have a map from the set $X(d)$ of quadratic irrationals of discriminant d to the set $I(d)$ of proper fractional ideals of $A(d)$, sending α to $\langle 1, \alpha \rangle$.

Definition 1.9. Two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ are *equivalent* if and only if there is $\zeta \in \mathbb{Q}(\sqrt{d})^*$ such that $\mathfrak{b} = \zeta\mathfrak{a}$.

Proposition 1.10. Let α and β be quadratic irrationals of discriminant d. Then $\alpha \sim \beta$ if and only if $\langle 1, \alpha \rangle \sim \langle 1, \beta \rangle$.

Proof. Say $\beta = \gamma\alpha$, $\gamma = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$. Then

$$\begin{pmatrix} \beta \\ 1 \end{pmatrix} = \frac{1}{r\alpha + s} \begin{pmatrix} p\alpha + q \\ r\alpha + s \end{pmatrix} = \frac{1}{r\alpha + s} \gamma \begin{pmatrix} \alpha \\ 1 \end{pmatrix}.$$

Thus the abelian group generated by 1 and β is the same as $\frac{1}{r\alpha+s}$ times the group generated by 1 and α, as desired. The converse is similar. ∎

Thus the map induces a monomorphism on the sets of equivalence classes, which the above work shows is in fact also surjective:

Corollary 1.11. (a) $X(d)/\sim \xrightarrow{\cong} I(d)/\sim$.
(b) $\psi : G_\alpha \xrightarrow{\cong} A(d)^*$, via $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \mapsto r\alpha + s$.

Proof of (b). We have seen that $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \mapsto r\alpha + s$ defines a map

$$\psi : G_\alpha \to \{\zeta \in \mathbb{Q}(\sqrt{d})^* : \zeta\mathfrak{a} = \mathfrak{a}\}$$

where $\mathfrak{a} = \langle 1, \alpha \rangle$. We claim that the target is A^*. Let $\zeta \in \mathbb{Q}(\sqrt{d})^*$ be such that $\zeta\mathfrak{a} = \mathfrak{a}$. Since $\mathfrak{a}$ is proper, $\zeta \in A$. On the other hand, $\zeta \neq 0$, and $\zeta^{-1}\mathfrak{a} \subseteq \mathfrak{a}$, so, again by the properness of $\mathfrak{a}$, $\zeta^{-1} \in A$: that is, $\zeta \in A^*$.

Now we construct an inverse. Given $r\alpha + s \in A^*$, we seek integers p, q such that $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \alpha = \alpha$. This is equivalent to $r\alpha^2 + (s-p)\alpha - q = 0$. This equation must be a multiple of the primitive equation for α: $r = ka, s - p = kb, q = -kc$. r and s clearly determine p and q, so ψ is monic. It remains only to check that $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$; but this follows from Lemma 2.2 below. ∎

Recall that we also know that $X(d)/\sim$ is bijective with the set of sign-equivalence classes of primitive quadratic forms of discriminant d.

2. Units.

We have four sets in bijection:

- $\{(t, u) \in \mathbb{Z} \times \mathbb{Z} : t^2 - du^2 = \pm 4\}$;
- $A(d)^*$;
- G_α; and
- $\mathrm{Aut}_s(f)$, where f is the primitive quadratic form corresponding to α and $\mathrm{Aut}_s(f)$ denotes the set of $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ such that $f\gamma = f$, using the signed action of $\mathrm{GL}_2(\mathbb{Z})$ on forms.

This works even if $d < 0$, and recovers a calculation we made in the course of establishing reduction theory for definite quadratic forms: the only definite forms admitting nontrivial automorphisms (i.e., different from changing the sign of both variables) are those of discriminant -3 and -4.

All but the first of these four sets carry natural group structures; and we claim that the bijections preserve this group structure. We have dealt already with the last pair.

Lemma 2.1. ψ is a homomorphism of groups.

Lemma 2.2. $\det \begin{pmatrix} p & q \\ r & s \end{pmatrix} = N(r\alpha + s)$, for $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in G_\alpha$.

In proving this it is useful to consider a general $\beta \in \mathbb{Q}(\sqrt{d})$; multiplication by β gives a linear operator on the 2-dimensional rational vector space $\mathbb{Q}(\sqrt{d})$, which we denote by m_β. Then (recalling the notation for the coefficients of the monic polynomial $x^2 - T(\beta)x + N(\beta) = 0$ satisfied by β):

Lemma 2.3. $N\beta = \det m_\beta$, and $T\beta = \operatorname{tr} m_\beta$.

We now describe the structure of this group. We will need to use problem 4b of problem set 6, extended and corrected slightly as follows.

Lemma 2.4. Let a, c be relatively prime integers, with $c > 0$, and let $\epsilon \in \{1, -1\}$. If $c > 1$, there is a unique matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ with determinant ϵ and $c \geq d \geq 0$; and in fact, $c > d > 0$. If $c = 1$, there are two such matrices, namely

$$\begin{pmatrix} a & -\epsilon \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} a & a - \epsilon \\ 1 & 1 \end{pmatrix}.$$

Proposition 2.5. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$, with $c \geq d \geq 0$. If $c = 1$, assume that $d = 1$ if $\det A = +1$, $d = 0$ if $\det A = -1$. Then there exists a unique sequence $q_0, \ldots q_n \in \mathbb{Z}$ with $q_i > 0$ for $i > 0$ such that

$$A = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix}.$$

Now let α be any reduced quadratic irrational of discriminant $d > 0$, and let $\langle q_0, q_1, \ldots \rangle$ be its continued fraction. Let the *minimal* period have length $n + 1$, so

$$\alpha = \langle q_0, \ldots, q_n, \alpha \rangle.$$

Let a_n, b_n have their usual meanings, so that for any x,

$$\langle q_0, \ldots, q_k, x \rangle = \begin{pmatrix} a_k & a_{k-1} \\ b_k & b_{k-1} \end{pmatrix}.$$

Then in particular $\sigma_0 \alpha = \alpha$ with $\sigma_0 = \begin{pmatrix} a_n & a_{n-1} \\ b_n & b_{n-1} \end{pmatrix}$. Let

$$\epsilon = b_n \alpha + b_{n-1} = \psi \sigma_0.$$

As we have seen in §1, $\epsilon \in A(d)^*$.

Theorem 2.6. $A(d)^* = \{\pm\epsilon^k : k \in \mathbb{Z}\}$.

Thus ϵ is the smallest unit larger than 1 in the ring $A(d)$. This also shows that if $n+1$ is odd, the smallest positive solution to the diophantine equation $t^2 - du^2 = -4$ is obtained by solving $\epsilon = \frac{t+u\sqrt{d}}{2}$, and that the smallest positive solution to the equation $t^2 - du^2 = 4$ is obtained by solving $\epsilon^2 = \frac{t+u\sqrt{d}}{2}$. If $n+1$ is even, then the smallest positive solution to $t^2 - du^2 = 4$ is obtained by solving $\epsilon = \frac{t+u\sqrt{d}}{2}$, and the equation $t^2 - du^2 = -4$ has no solutions at all. For example, with $d = 1969$ my computer informs me that $n+1$ is even and that

$$\epsilon = \frac{9377001831617185213368865694750 2 + 2113202631220407492138882654600\sqrt{1969}}{2}.$$

Thus ϵ, the smallest unit bigger than 1 in $A(d)$, is approximately 4.6650×10^{31}—and its reciprocal is correspondingly infinitesimal. In other words, after $(\pm 2, 0)$, the integral points on the curve $t^2 - 1969u^2 = 4$ nearest to the origin are the points

$$(\pm 93770018316171852133688656947502, \pm 2113202631220407492138882654600).$$

Moreover, the next nearest points have roughly twice as many digits, and so on! We also learn that $t^2 - 1969u^2 = -4$ has no integral solutions at all (since the length of the period is even, so the norm of the fundamental unit is $+1$).

Incidentally, the computer also tells me that the class-number $h(1969)$ is 1; and that the unique sign-equivalence class of quadratic forms of discriminant 1969 contains $11x^2 - 33xy - 20y^2$ (and 69 other reduced forms). (The period is even, so there are two strict equivalence classes of quadratic forms of discriminant 1969; the one not containing $11x^2 - 33xy - 20y^2$ contains $11x^2 + 33xy - 20y^2$.)

3. Invertibility and norms of ideals.

Ideals are supposed to be generalized numbers. Let $A = A(d)$, $K = \mathbb{Q}(\sqrt{d})$ (although for the moment A could be any integral domain and K its field of fractions). An element $\zeta \in K$ determines a "principal" fractional ideal ζA for A. Note that ζ and ξ determine the same principal ideal if and only if $\xi = \eta\zeta$ for some $\eta \in A^*$: i.e., if and only if ξ and ζ are *associates*.

In this section we will set up two tools we already have at hand for numbers: inverses and norms. Recall that we can multiply two ideals, and get another ideal:

$$\mathfrak{a}\mathfrak{b} = \{\sum a_i b_i : a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}.$$

The ring A itself is an ideal, and is the unit for this product.

Definition 3.1. A fractional ideal $\mathfrak{a}$ is *invertible* if and only if there is an ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = A$.

For example, any nonzero principal ideal is invertible:

$$(\zeta A)(\zeta^{-1}A) = \zeta\zeta^{-1}A = A.$$

Lemma 3.2. The set of invertible fractional ideals for A forms a group under this product, with unit element A. The set of principal ideals forms a subgroup.

One need only check that the product of two invertible ideals is again invertible.

Thus the ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = A$ is *unique*; it's the *inverse* of $\mathfrak{a}$, and we write $\mathfrak{a}^{-1}$ for it.

Now specialize to the case of a quadratic number ring.

Theorem 3.3. A fractional ideal of $A(d)$ is invertible if and only if it is proper.

Proof. Suppose $\mathfrak{a}$ is invertible, and let $\zeta \in K$ be such that $\zeta\mathfrak{a} \subseteq \mathfrak{a}$. Then $\zeta \in \zeta A = \zeta\mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{a}a^{-1} = A$; so $\mathfrak{a}$ is proper.

Now suppose $\mathfrak{a}$ is proper. We will construct an inverse ideal, mimicing the fact that if $\alpha \in K^*$ then $\alpha^{-1} = \frac{\alpha'}{N(\alpha)}$.

There are $\zeta, \alpha \in K^*$, with $D(\alpha) = d$, such that $\mathfrak{a} = \zeta\langle 1, \alpha\rangle$. Let's define the *conjugate* of $\mathfrak{a}$ to be

$$\mathfrak{a}' = \zeta'\langle 1, \alpha'\rangle.$$

Then

$$\mathfrak{a}a' = \zeta\zeta' \text{Span}\,\{1, \alpha, \alpha', \alpha\alpha'\}.$$

α satisfies an equation $ax^2 + bx + c = 0$ with $\gcd\{a, b, c\} = 1$, and in these terms $\alpha + \alpha' = -\frac{b}{a}, \alpha\alpha' = \frac{c}{a}$. Thus

$$a\mathfrak{a}a' = a\zeta\zeta'\langle 1, \alpha, -\frac{b}{a}, \frac{c}{a}\rangle = N(\zeta)\langle a, b, c, a\alpha\rangle = N(\zeta)\langle 1, a\alpha\rangle = N(\zeta)A.$$

Since $\zeta \neq 0, N(\zeta) \neq 0$; so we may define

$$\mathfrak{a}^{-1} = \frac{a}{N(\zeta)}\mathfrak{a}'. \qquad \blacksquare$$

Thus the set $I(d)$ of proper fractional ideals forms a group and the set $P(d)$ of nonzero principal ideals forms a subgroup. This subgroup determines an equivalence relation on $I(d)$, which is exactly the relation of equivalence of proper ideals; so

$$I(d)/\sim = I(d)/P(d)$$

is a group (which we have proved earlier is finite): the *class group* $Cl(d)$. From our construction of the inverse of a proper ideal, we also have that the inverse of the class of $\mathfrak{a}$ in $Cl(d)$ is given by $\mathfrak{a}'$.

We turn to the norm, for which we need a lemma.

Lemma 3.4. Let $\mathfrak{a}$ be a nonzero ideal in the ring $A = A(d)$. Then $A/\mathfrak{a}$ is a finite commutative ring.

Proof. See Theorem 1.13 in Stewart and Tall. $\blacksquare$

Definition 3.5. Let $\mathfrak{a}$ be a nonzero ideal in $A = A(d)$. Its *norm* is

$$N(\mathfrak{a}) = \#A/\mathfrak{a}.$$

Proposition 3.6. (a) If $\zeta \in A, \zeta \neq 0$, then $N(\zeta A) = |N(\zeta)|$.
(b) If $\mathfrak{a}$ is proper, then $\mathfrak{a}a' = (N(\mathfrak{a}))$.
(c) If $\mathfrak{a}$ and $\mathfrak{b}$ are proper, then $N(\mathfrak{a}b) = N(\mathfrak{a})N(\mathfrak{b})$.

Proof. (a) follows by combining Lemma 2.3 above with Stewart and Tall's Theorem 1.13.

Next we prove (c) in case $\mathfrak{a}$ is principal; say $\mathfrak{a} = (\alpha)$. Then we have a surjection $A/\alpha\mathfrak{b} \to A/(\alpha)$, with kernel $(\alpha)/\alpha\mathfrak{b}$. Basic algebra shows that the order of $A/\alpha\mathfrak{b}$ is then the product of the orders of $A/(\alpha)$ and $(\alpha)/\alpha\mathfrak{b}$. But multiplication by α induces an isomorphism from $A/\mathfrak{b}$ to $(\alpha)/\alpha\mathfrak{b}$, so (c) holds in this case.

Next we prove (b). Write $\mathfrak{a}$ as $\zeta\langle 1, \alpha\rangle$, with $D(\alpha) = d$. Let $ax^2 + bx + c = 0$ be the primitive equation for α. Then $a\alpha$ is a quadratic integer of discriminant d, so $A(d) = \langle 1, a\alpha\rangle$. Now compute:

$$\begin{aligned} a^2 N(\mathfrak{a}) &= N(a\mathfrak{a}) \quad \text{(by (c) in the case we've proved)} \\ &= N(a\zeta\langle 1, \alpha\rangle) \\ &= N(\zeta\langle a, a\alpha\rangle) \\ &= |N(\zeta)|N(\langle a, a\alpha\rangle) \quad \text{(by (c) again, and (a))} \\ &= |N(\zeta)||a|, \end{aligned}$$

where the last equality follows from the definition of the norm of an ideal and the fact that $A = \langle 1, a\alpha\rangle$. Thus

$$N(\mathfrak{a}) = \left|\frac{N\zeta}{a}\right|. \qquad (*)$$

This shows that $\frac{N\zeta}{a} \in \mathbb{Z}$, and that

$$\mathfrak{a}a' = (N(\mathfrak{a})),$$

from our description of $\mathfrak{a}^{-1}$. This proves (b).

We can now deal with the general case of (c): we calculate with the principal ideals:

$$(N(\mathfrak{a}b)) = (\mathfrak{a}b)(\mathfrak{a}b)' = \mathfrak{a}a'bb' = (N(\mathfrak{a}))(N(\mathfrak{b})) = (N(\mathfrak{a})N(\mathfrak{b})).$$

But all these norm elements are positive integers, so the product formula follows. ∎

4. Unique factorization of ideals.

As we know, unique factorization can fail in a quadratic number ring. The situation for fundamental discriminants is summarized by:

Theorem 4.1. Let A be the quadratic number ring $A(d)$, with d a fundamental discriminant. The following four conditions are equivalent.
(a) Any irreducible element in A is prime.
(b) Any nonzero element factors into a product of irreducibles, in a way which is unique up to order and replacing the factors by associates (i.e., by unit multiples): A is a "unique factorization domain."
(c) Every ideal is principal: A is a "principal ideal domain."
(d) $Cl(d)$ is the trivial group.

This will be proved below.

Ideals provide a context for a more general unique factorization theorem.

Definition 4.2. Let A be any commutative ring.
(a) Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in A. $\mathfrak{a}$ *divides* $\mathfrak{b}$, written $\mathfrak{a}|\mathfrak{b}$, iff $\mathfrak{a} \supseteq \mathfrak{b}$.
(b) An ideal $\mathfrak{p}$ in A is *prime* iff it is not the unit ideal A and for any pair $\mathfrak{a}, b$ of ideals in A such that $\mathfrak{p}|ab$, either $\mathfrak{p}|a$ or $\mathfrak{p}|b$.
(c) An ideal $\mathfrak{m}$ in A is *maximal* iff the only ideals $\mathfrak{a}$ in A such that $\mathfrak{a}|m$ are $\mathfrak{a} = m$ and $\mathfrak{a} = A$. (One might also call such an ideal *irreducible.*)

Lemma 4.3. Let $\mathfrak{a}$ be an ideal in the ring A.
(a) $\mathfrak{a}$ is prime iff $A/\mathfrak{a}$ is a nonzero integral domain.
(b) $\mathfrak{a}$ is maximal iff $A/\mathfrak{a}$ is a field.
(c) The principal ideal $(\alpha) = \alpha A$ is prime if and only if α is a (nonzero) prime element of A.

Corollary 4.4. Any prime ideal in a quadratic number ring is maximal.

Proof. Any finite integral domain is a field. ∎

Proposition 4.5. Any nonzero ideal in a fundamental quadratic number ring A (i.e., the ring of all quadratic integers in $\mathbb{Q}(\sqrt{d})$) factors uniquely (up to order) as a product of prime ideals.

Proof of existence: Assume there is a nonzero ideal $\mathfrak{a}$ which doesn't factor as a product of prime ideals. The quotient $A/\mathfrak{a}$ is finite, so has only finitely many ideals. Thus there are only finitely many ideals of A containing $\mathfrak{a}$. Let $\mathfrak{b}$ be maximal among them with the property that it does not factor as a

product of primes either. A itself factors as the empty product, so $\mathfrak{b} \neq A$. $\mathfrak{b}$ may not be maximal among all non-unit ideals in A, but it is contained in a maximal ideal (by the same argument, applied to the quotient $A/\mathfrak{b}$), say $\mathfrak{m}$. Since $\mathfrak{m}$ is maximal, it is prime. Since the discriminant is fundamental, every ideal is proper, and so $\mathfrak{m}$ is invertible. Now $\mathfrak{m} \subset A$ implies that $A \subset \mathfrak{m}^{-1}$, so

$$\mathfrak{b} \subset \mathfrak{m}^{-1}\mathfrak{b} \subseteq \mathfrak{m}^{-1}\mathfrak{m} = A.$$

By maximality of $\mathfrak{b}$, $\mathfrak{m}^{-1}\mathfrak{b}$ factors as a product of primes. Thus, multiplying by the prime ideal $\mathfrak{m}$, you see that $\mathfrak{b}$ does also, contrary to assumption.

Proof of uniqueness: If $\mathfrak{p}_1 \cdots \mathfrak{p}_m = \mathfrak{q}_1 \cdots \mathfrak{q}_n$, then as $\mathfrak{p}_1$ is prime it must divide one of the $\mathfrak{q}$'s: renumber if necessary so it divides $\mathfrak{q}_1$: $\mathfrak{q}_1 \subseteq \mathfrak{p}_1$. But $\mathfrak{q}_1$ is maximal, so $\mathfrak{q}_1 = \mathfrak{p}_1$. Now multiply both sides by the inverse of this ideal and continue. ∎

Remark 4.6. The proof shows that if $\mathfrak{a}$ is a nonzero ideal and $\mathfrak{p}$ and $\mathfrak{q}$ are distinct prime ideals dividing $\mathfrak{a}$, then the product $\mathfrak{p}q$ divides $\mathfrak{a}$. We also notice that if the norm of $\mathfrak{a}$ is a rational prime, then $\mathfrak{a}$ is a prime ideal: it's not the unit ideal (which has norm 1), and if $\mathfrak{a}$ is not prime then it has a nontrivial prime factorization, which application of the norm translates into a nontrivial factorization of its norm. The converse if false; the principal ideal (p) may be prime in A, but it always has norm p^2.

Proof of 4.1: (b) ⇒ (a): Let $p \in A$ be irreducible, and suppose $p|ab$. Write $pc = ab$. By assumption a, b, and c factor as products of irreducibles. By uniqueness, p must be one of the irreducible factors of a or b, up to a unit, and hence must divide either a or b.

(a) & (b) ⇒ (c): Since any ideal factors as a product of prime ideals, and products of principal ideals are principal, it will be enough to show that any *prime* ideal $\mathfrak{p}$ is principal. $\mathfrak{p}$ is at least related to a principal ideal, by the equation $\mathfrak{p}p' = (N(\mathfrak{p}))$. By assumption $N(\mathfrak{p})$ factors as a product of irreducibles: $N(\mathfrak{p}) = \pi_1 \cdots \pi_n$. Then

$$\mathfrak{p}p' = (N(\mathfrak{p})) = (\pi_1) \cdots (\pi_n).$$

By the definition of prime ideal, $\mathfrak{p}|(\pi_i)$ for some i. Since every prime ideal is maximal, it follows that in fact $\mathfrak{p} = (\pi_i)$.

(c) ⇒ (a): Let π be irreducible, and suppose $\mathfrak{a}|(\pi)$. $\mathfrak{a}$ is principal; say $\mathfrak{a} = (a)$, so $a|\pi$. Thus a is a unit or an associate of π, by definition of

irreducible. Thus $\mathfrak{a} = A$ or $\mathfrak{a} = (\pi)$; that is, (π) is maximal. But every maximal ideal is prime, so (π) is a prime ideal, and this is equivalent to π being a prime element.

(c) & (a) $\Rightarrow$ (b): Let $a \in A$, and factor (a) as a product of (principal!) prime ideals: $(a) = (\pi_1) \cdots (\pi_n)$. Then $a = \epsilon \pi_1 \cdots \pi_n$ for some $\epsilon \in A^*$. π_i is a prime element since (π_i) is a prime ideal. We claim any prime element π is irreducible, so we have a factorization of the desired type. If $\pi = bc$ in A, then $(\pi) = (b)(c)$. Since (π) is maximal, either $(b) = (\pi)$ so b is an associate of π or $(b) = A$ so b is a unit. This is the definition of irreducible. Finally, uniqueness of the factorization follows in the usual way from the fact that the irreducible elements are prime. ∎

5. Splitting of rational primes.

As we have seen, a rational prime may split as a nontrivial product of primes in a quadratic number ring; for example,

$$(2) = (1+i)(1-i) \quad \text{in} \quad A(-4);$$

$$(3) = \langle 3, 1+\sqrt{-5} \rangle \langle 3, 1-\sqrt{-5} \rangle \quad \text{in} \quad A(-12).$$

In the first example it is interesting to notice that $1-i = (-i)(1+i)$ (and here I mean as *elements* of $\mathbb{Z}[i]$, not ideals, as the left-hand side of the equation shows); so that $(1-i) = (1+i)$ (now as ideals!) because $-i$ is a unit; and so we find that (2) splits as the *square* of an ideal in $\mathbb{Z}[i]$: $(2) = (1+i)^2$ (even though the number 2 is of course not a square in $\mathbb{Z}[i]$).

The following theorem describes exactly how odd primes split in a fundamental quadratic number ring. Recall that a polynomial algebra over a field is a Euclidean domain, and so enjoys unique factorization into irreducibles.

Theorem 5.1 Let d be a fundamental discriminant, let $A = A(d)$, and let α be a quadratic integer of discriminant d, with primitive equation $f(x) = x^2 + bx + c = 0$. Let p be an odd rational prime. Then:
(a) If $f(x)$ is irreducible mod p, then pA is prime.
(b) If $f(x) \equiv (x-m)(x-n) \pmod{p}$, then

$$pA = \langle p, \alpha - m \rangle \langle p, \alpha - n \rangle$$

is the factorization of pA into prime ideals. These prime ideals are equal if and only if $m \equiv n \pmod{p}$.

We know how to decide whether a quadratic polynomial has a root mod p; this is equivalent to $4f(x) = (2x+b)^2 - d$ having a root, i.e., to d being a square mod p. This happens if $p|d$ (when we say that the Legendre symbol $\left(\frac{d}{p}\right)$ is 0)—in which case $f(x)$ splits as a square in $\mathbb{Z}_p[x]$— or if d is a quadratic residue mod p (i.e., $\left(\frac{d}{p}\right) = +1$). Conversely, if $f(x)$ is a square in $\mathbb{Z}_p[x]$—say $f(x) = (x-m)^2$—then $b \equiv -2m$, $c \equiv m^2$, and $d \equiv 4m^2 - 4m^2 = 0 \pmod{p}$.

The following language is important.

Definition 5.2. Let p be a rational prime, and A a quadratic number ring.
(a) p *ramifies* in A iff pA is the square of a prime ideal in A.
(b) p *splits* in A iff pA is the product of two distinct prime ideals in A.
(c) p *stays prime* or is *inert* in A iff pA is a prime ideal in A.

Taking the paragraph after the statement of the theorem into account, Theorem 5.1 can be restated:

Theorem 5.3. Let A and p be as above. Then:
(a) p ramifies in A iff $\left(\frac{d}{p}\right) = 0$.
(b) p splits in A iff $\left(\frac{d}{p}\right) = +1$.
(c) p is inert in A iff $\left(\frac{d}{p}\right) = -1$.

The same statement holds with $p = 2$ if we interpret $\left(\frac{d}{2}\right)$ as the *Kronecker symbol*

$$\left(\frac{d}{2}\right) = \begin{cases} 0 & \text{if } d \equiv 0 \pmod{4} \\ +1 & \text{if } d \equiv 1 \pmod{8} \\ -1 & \text{if } d \equiv 5 \pmod{8} \end{cases}$$

Note that an odd discriminant is a square mod 2^n, for $n \geq 3$, iff $\left(\frac{d}{2}\right) = +1$. We won't prove this case here, though the proof is entirely analogous to what we do.

Proof of Theorem 5.1. The proof is based on the following trivial but important observation:

$$\mathbb{Z}[x]/(f(x)) \xrightarrow{\cong} A.$$

The map sends x to α.

(a) Suppose $f(x)$ is irreducible mod p. Since $\mathbb{Z}_p[x]$ is a Euclidean domain, $f(x)$ is then a prime element, so $(f(x))$ is a prime ideal (by Lemma 4.3(c)). The quotient $\mathbb{Z}_p[x]/(f(x))$ is generated additively by $\{1, x\}$, so is a finite integral domain—hence a field. But of course $\mathbb{Z}_p[x]/(f(x)) = (\mathbb{Z}[x]/(f(x)))/(p)$, so we conclude that (p) is a maximal ideal in the ring $\mathbb{Z}[x]/(f(x)) \cong A$, and in particular is prime.

Remark 5.4. This is quite interesting, since in this case $\mathbb{Z}_p[x]/(f(x))$ is a 2-dimensional vector space over $\mathbb{Z}_p$, which is in its own right a field. We know that its group of units must be cyclic. So one way to think of it is as $\mathbb{Z}_p(\zeta)$, where ζ is a primitive (p^2-1)th root of unity. This shows that there is only one such field (for each p). Similarly, there is a unique field of order p^n, for any $n \geq 1$. These show up in number theory precisely as quotients of number rings by prime ideals. You should be careful to distinguish these fields from the cyclic rings $\mathbb{Z}_{p^n}$; they coincide only when $n = 1$.

Proof, continued. (b) We begin by verifying that $\mathfrak{p} = \langle p, \alpha - m\rangle$ is an ideal. Since $A = \langle 1, \alpha\rangle$, this comes to checking that $p\alpha \in \mathfrak{p}$ and that $\alpha(\alpha - m) \in \mathfrak{p}$. The first is easy: $p\alpha = p(\alpha - m) + mp$. For the second, compute

$$\alpha^2 - m\alpha = -b\alpha - c - m\alpha = -(m+b)(\alpha - m) - (m^2 + bm + c).$$

The last term is divisible by p, since m is a root mod p.

Next we compute the norm of $\mathfrak{a}$. $\frac{\alpha - m}{p}$ satisfies an equation $px^2 + ?x + ? = 0$, so, by equation $(*)$ above,

$$N(\langle p, \alpha - m\rangle) = N(p\langle 1, \frac{\alpha - m}{p}\rangle) = \left|\frac{N(p)}{p}\right| = \frac{p^2}{p} = p.$$

It follows that $\mathfrak{a}$ is a prime, by Remark 4.6.

These considerations apply equally well of course to $\mathfrak{q} = \langle p, \alpha - n\rangle$.

Since $(\alpha - m)(\alpha - n) = pk$,

$$\langle p, \alpha - m\rangle\langle p, \alpha - n\rangle = \text{Span}\,\{p^2, p\alpha - pm, p\alpha - pn, pk\} \subseteq (p).$$

The norm computation shows that equality must hold here. All that is left is to show that $\mathfrak{p} \neq \mathfrak{q}$ when $m \not\equiv n \,(\text{mod}\, p)$. Suppose $m \not\equiv n \,(\text{mod}\, p)$, and assume that $\mathfrak{p} = \mathfrak{q}$. Then $\alpha - n \in \langle p, \alpha - m\rangle$, so

$$n - m = (\alpha - m) - (\alpha - n) \in \langle p, \alpha - m\rangle,$$

so, since $\gcd\{p, n-m\} = 1$, $\langle p, \alpha - m\rangle = (1)$. But it's not. ∎

Remark 5.5. We can express this factorization using the operation of *conjugation* of ideals. Since $(p)' = (p)$ (obviously), the fact that $\mathfrak{p}|(p)$ implies that $\mathfrak{p}'|(p)$ as well. It is not hard to see that $\mathfrak{p}' = \mathfrak{q}$.

Application 5.6. Take $A = A(-4) = \mathbb{Z}[i]$. Then

$$\left(\frac{-4}{p}\right) = \begin{cases} 0 & \text{if } p = 2 \\ +1 & \text{if } p \equiv 1 \,(\mathrm{mod}\, 4) \\ -1 & \text{if } p \equiv 3 \,(\mathrm{mod}\, 4). \end{cases}$$

Our theorem does not cover the case $p = 2$, but we saw above that in this case 2 ramifies. 2 is the only ramified prime; primes congruent to 1 mod 4 split, primes congruent to 3 mod 4 are inert.

We can compute the norms of the prime ideals in $\mathbb{Z}[i]$ which divide (p). The norm of (p) is p^2, so the norms of its prime divisors must be p if p splits, p^2 if p is inert: that is, p if $p \equiv 1 \,(\mathrm{mod}\, 4)$, p^2 if $p \equiv 3 \,(\mathrm{mod}\, 4)$.

We know that the class-number of $\mathbb{Z}[i] = A(-4)$ is 1, so the above splitting is into products of principal ideals. Thus there are Gaussian integers $x + iy$ with the given norms. But of course

$$N(x + iy) = x^2 + y^2,$$

so we have proven anew that any prime congruent to 1 mod 4 is a sum of two squares.

The fact that $\mathbb{Z}[i]$ is a unique factorization domain lets us count the ways a general positive integer n can be written as a sum of two squares. Factor n as a product of primes, $n = 2^a p_1^{b_1} \cdots p_m^{b_m} q_1^{c_1} \cdots q_n^{c_n}$, where the p_j are distinct primes congruent to 1 mod 4 and the q_j are distinct primes congruent to 3 mod 4. Then in A there is a prime factorization

$$n = u(1+i)^{2a}(\pi_1\pi_1')^{b_1} \cdots (\pi_m\pi_m')^{b_m} q_1^{c_1} \cdots q_n^{c_n},$$

where $u \in A^* = \{\pm 1, \pm i\}$ (in fact, $u = (-i)^a$) and $p_j = \pi_j\pi_j'$ is a prime factorization in A.

Expressions of n as a sum of two squares come from Gaussian integers of norm n. Such Gaussian integers come in groups of four associates. There are none unless all the c_k's are even. If the c_k's are all even, we get a Gaussian

integer with norm n by taking $(1+i)^a$, $q_k^{c_k/2}$, and either π_j or π_j' each time one occurs in the expression for n. There are thus

$$(b_1+1)\cdots(b_m+1)$$

such choices; this is the number of ways of writing n as a sum of two squares of nonnegative numbers.

For example, if $n = 5850 = 2\cdot 3^2\cdot 5^2\cdot 13$, let $5 = \pi_1\pi_1'$ and $13 = \pi_2\pi_2'$. There is some choice here; let's take $\pi_1 = 2+i$ and $\pi_2 = 3+2i$. Then there are $(2+1)(1+1) = 6$ ways to choose up sides:

$$\begin{aligned}
(1+i)\cdot 3\cdot \pi_1^2\pi_2 &= 3(-17+19i)\\
(1+i)\cdot 3\cdot \pi_1\pi_1'\pi_2 &= 3(5+25i)\\
(1+i)\cdot 3\cdot \pi_1'^2\pi_2 &= 3(23+11i)\\
(1+i)\cdot 3\cdot \pi_1^2\pi_2' &= 3(11+23i)\\
(1+i)\cdot 3\cdot \pi_1\pi_1'\pi_2' &= 3(25+5i)\\
(1+i)\cdot 3\cdot \pi_1'^2\pi_2' &= 3(19-17i).
\end{aligned}$$

This gives us six expressions for 5850 as a sum of two squares of positive numbers:

$$(3\cdot 17)^2+(3\cdot 19)^2,\quad (3\cdot 5)^2+(3\cdot 25)^2,\quad (3\cdot 23)^2+(3\cdot 11)^2,$$

and the same three sums with the summands reversed.