3. Rings of integers.

In this section we introduce for an arbitrary number field an analogue of the subring $\mathbf{Z}$ of $\mathbf{Q}$. Combining this with the results of section 1, we obtain an analogue of the inclusion maps

$$\mathbf{Z} \quad \subset \quad \mathbf{Q} \quad \subset \quad \mathbf{R} \quad \subset \quad \mathbf{C}.$$

For a number field F it is the following sequence of subrings

$$O_F \quad \subset \quad F \quad \subset \quad F_{\mathbf{R}} \quad \subset \quad F_{\mathbf{C}}.$$

where $F_{\mathbf{R}}$ and $F_{\mathbf{C}}$ are the rings introduced in section 1. The ring O_F is the *ring of integers* of F.

Definition. *Let F be a number field. An element $x \in F$ is called integral if there exists a monic polynomial $f(T) \in \mathbf{Z}[T]$ with $f(x) = 0$. The subset of integral elements of F is denoted by O_F.*

It is clear that the integrality of an element does not depend on the field F it contains. An example of an integral element is $i = \sqrt{-1}$, since it is a zero of the monic polynomial $T^2 + 1 \in \mathbf{Z}[T]$. Every n-th root of unity is integral, since it is a zero of $T^n - 1$. All ordinary integers $n \in \mathbf{Z}$ are integral in this new sense because they are zeroes of the polynomials $T - n$.

Lemma 3.1. *Let F be a number field and let $x \in F$. the following are equivalent*
(a) x is integral.
(b) The minimum polynomial $f^x_{\min}(T)$ of x over $\mathbf{Q}$ is in $\mathbf{Z}[T]$.
(c) The characteristic polynomial $f^x_{\mathrm{char}}(T)$ of x over $\mathbf{Q}$ is in $\mathbf{Z}[T]$.
(d) There exists a finitely generated subgroup $M \neq 0$ of F such that $xM \subset M$.

Proof. *(a)⇒(b)* Let x be integral and let $f(T) \in \mathbf{Z}[T]$ be a monic polynomial such that $f(x) = 0$. The minimum polynomial $f^x_{\min}(T)$ divides $f(T)$ in $\mathbf{Q}[T]$. Since the minimum polynomial of x is monic, we have $f(T) = g(T)f^x_{\min}(T)$ with $g(T) \in \mathbf{Q}[T]$ monic. By Gauss' Lemma (Exer.3.1) both $f^x_{\min}(T)$ and $g(T)$ are in $\mathbf{Z}[T]$ as required.
(b)⇒(c) This is immediate from Prop.2.7*(c)*.
(c)⇒(d) Let n be the degree of $f^x_{\mathrm{char}}(T) = \sum_i a_i T^i$. Let M be the additive group generated by $1, x, x^2, \ldots, x^{n-1}$. The finitely generated group M satisfies $xM \subset M$ because $x \cdot x^{n-1} = x^n = -a_{n-1}x^{n-1} - \ldots - a_1 x - a_0 \in M$.
d)⇒(a) Let $M \neq 0$ be generated by $e_1, e_2, \ldots, e_m \in F$. Since $xM \subset M$ there exist $a_{ij} \in \mathbf{Z}$ such that

$$xe_i = \sum_{j=1}^{m} a_{ij} e_j \qquad \text{for all } 1 \leq i \leq m,$$

in other words

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1m} \\ a_{21} & a_{22} & \ldots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mm} \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{pmatrix} = x \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{pmatrix}.$$

This implies that the determinant $\det(a_{ij} - x \cdot \mathrm{Id}) = 0$. Since $M \neq 0$, at least one of the e_i is not zero. Therefore x is an eigenvalue and the monic polynomial

$$f(T) = \det(a_{ij} - T \cdot \mathrm{Id}) \in \mathbf{Z}[T]$$

vanishes in x. This proves the lemma.

Proposition 3.2. *The set O_F of integral elements of a number field F is a subring of F.*

Proof. It suffices to show that $x \pm y$ and xy are integral whenever x and y are integral. Let therefore $x, y \in F$ be integral. By Lemma 3.1 there exist non-zero finitely generated subgroups M_1 and M_2 of F, such that $xM_1 \subset M_1$ and $yM_2 \subset M_2$. Let $e_1, e_2, \ldots, e_l$ be generators of M_1 and let $f_1, f_2, \ldots, f_m$ be generators of M_2. Let M_3 be the additive subgroup of F generated by the products $e_i f_j$ for $1 \leq i \leq l$ and $1 \leq j \leq m$. Then we have $(x \pm y)M_3 \subset M_3$ and that $xyM_3 \subset M_3$. This proves the proposition.

Proposition 3.3. *Let F be a number field. Then there exists for every $x \in F$ an non-zero integer in $\mathbf{Z}$ so that mx is contained in the ring of integers of O_F. In particular, F is the field of fractions of O_F.*

Proof. Let $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \in \mathbf{Q}[X]$ be the minimum polynomial of x. Let m be a common denominator of the coefficients a_k. In other words, $m \neq 0$ and $ma_k \in \mathbf{Z}$ for $0 \leq k \leq n-1$. Then we have

$$m^n f(X) = (mX)^n + a_{n-1}m(mX)^{n-1} + \ldots + a_1 m^{n-1}(mX) + a_0 m^n.$$

Substituting $Y = mX$ we obtain a monic polynomial in Y with coeffients in $\mathbf{Z}$. So its zero $y = mx$ is integral and hence in O_F. This proves the first statement. The second is an immediate consequence.

It is, in general, a difficult problem to determine the ring of integers of a given number field. According to Theorem 2.4, every number field F can be written as $F = \mathbf{Q}(\alpha)$ for some algebraic number α. A similar statement for rings of integers is, in general false: there exist number fields F such that $O_F \neq \mathbf{Z}[\alpha]$ for any $\alpha \in O_F$. For example, the ring of integers of the field $\mathbf{Q}(\sqrt[3]{20})$ is $\mathbf{Z}[\sqrt[3]{20}, \sqrt[3]{50}]$. See exercises 3.7 and 3.8 for a proof that this ring is not of the form $\mathbf{Z}[\alpha]$ for any $\alpha \in \mathbf{Q}(\sqrt[3]{20})$.

For quadratic fields however, the rings of integers are generated by one element and the calculations are rather easy:

Proposition 3.4. *Let F be a quadratic number field. Then*
(a) There exists a unique squarefree integer $d \in \mathbf{Z}$ such that $F = \mathbf{Q}(\sqrt{d})$.
(b) Let $d \neq 1$ be a squarefree integer. The ring of integers O_F of $F = \mathbf{Q}(\sqrt{d})$ is given by

$$\begin{aligned} O_F &= \mathbf{Z}[\sqrt{d}] && \text{if } d \equiv 2 \text{ or } 3 \pmod 4, \\ &= \mathbf{Z}[\frac{1+\sqrt{d}}{2}] && \text{if } d \equiv 1 \pmod 4. \end{aligned}$$

Proof. *(a)* For any $\alpha \in F - \mathbf{Q}$ one has that $F = \mathbf{Q}(\alpha)$. The number α is a zero of an irreducible polynomial $f(T) \in \mathbf{Q}[T]$ of degree 2. This means that the discriminant d of $f(T)$ is not a square and we have $F = \mathbf{Q}(\sqrt{d})$. The field $\mathbf{Q}(\sqrt{d})$ does not change if we divide or multiply d by squares of non-zero integers. We conclude that $F = \mathbf{Q}(\sqrt{d})$ for some squarefree integer d.

Suppose $\mathbf{Q}(\sqrt{d}) = \mathbf{Q}(\sqrt{d'})$ for squarefree integers d, d'. Then $\sqrt{d'} = a + b\sqrt{d}$ for certain $a, b \in \mathbf{Q}$. This implies that $d' + b^2 d - 2b\sqrt{dd'} = a^2$. Since d' is not a square, we have $b \neq 0$ and hence $\sqrt{dd'}$ is in $\mathbf{Q}^*$. Since d and d' are squarefree and have the same sign, it follows that $d = d'$

(b) Let $\alpha \in F = \mathbf{Q}(\sqrt{d})$. Then α can be written as $\alpha = a + b\sqrt{d}$ with $a, b \in \mathbf{Q}$. It is easily verified that the characteristic polynomial is given by $f^x_{\mathrm{char}}(T) = T^2 - 2aT + (a^2 - b^2 d)$ By Prop. 3.1(c) a necessary and sufficient condition for $\alpha = a + b\sqrt{d}$ to be in O_F, is that $2a \in \mathbf{Z}$ and $a^2 - b^2 d \in \mathbf{Z}$.

Since $2a$ and $a^2 - b^2 d$ are in $\mathbf{Z}$, so is $4db^2 = d(2b)^2$. Since d is squarefree, this implies that $2b \in \mathbf{Z}$ as well. The second condition implies that $(2a)^2 - (2b)^2 d$ is in $4\mathbf{Z}$. Since d is squarefree, this implies that $2a$ is an even integer if and only if $2b$ is. If both are even, the coefficients a, b are in $\mathbf{Z}$ confirming that O_F contains $\mathbf{Z}[\sqrt{d}]$. If $2a$ and $2b$ both are odd, then both a and b are in $\frac{1}{2} + \mathbf{Z}$. The fact that $(2a)^2 - (2b)^2 d$ is in $4\mathbf{Z}$ implies that in this case we must have $d \equiv 1 \pmod 4$. Conversely, when $d \equiv 1 \pmod 4$, every element in $\mathbf{Z}[\frac{1+\sqrt{d}}{2}]$ is integral.

This completes the proof.

Next we discuss *discriminants* of integral elements $\omega_1, \ldots, \omega_n \in F$.

Proposition 3.5. *Let F be a number field of degree n. Let $\omega_1, \ldots, \omega_n \in F$.*

(a) If $\omega_1, \ldots, \omega_n \in O_F$ then $\Delta(\omega_1, \ldots, \omega_n)$ is in $\mathbf{Z}$.

(b) The ring O_F admits a $\mathbf{Z}$-basis. In other words, there exist $\omega_1, \ldots, \omega_n \in O_F$ for which O_F is equal to the direct sum $\oplus_{i=1}^n \omega_i \mathbf{Z}$.

(c) All $\mathbf{Z}$-bases have the same discriminant. This discriminant is a non-zero integer. Its absolute value is minimal among $|\Delta(\omega_1, \ldots, \omega_n)|$ where $\omega_1, \ldots, \omega_n$ are elements of O_F that form a $\mathbf{Q}$-basis of F.

Proof. *(a)* If the ω_i are in O_F, so are the products $\omega_i \omega_j$. It follows that the traces of $\omega_i \omega_j$ are in $\mathbf{Z}$, so that the discriminant $\Delta(\omega_1, \ldots, \omega_n)$ is in $\mathbf{Z}$ as well. This proves (a).

By Proposition 3.4 there exists an integral basis $\omega_1, \ldots, \omega_n$ for F over $\mathbf{Q}$. Indeed, it suffices to multiply a $\mathbf{Q}$-basis by a suitable non-zero integer. This basis has a non-zero discriminant which by an *(a)* is an integer.

Now let $\omega_1, \ldots, \omega_n \in O_F$ be a $\mathbf{Q}$-basis of F for which $|\Delta(\omega_1, \ldots, \omega_n)|$ is minimal. Then we have $O_F \cong \oplus_{i=1}^n \omega_i \mathbf{Z}$. Indeed, if this were not the case, there would exist an element $x = \sum_i \lambda_i \omega_i \in O_F$ for certain $\lambda_i \in \mathbf{Q}$, that is not contained in the additive group generated by the ω_i. This implies that $\lambda_i \notin \mathbf{Z}$ for some i. After adding a suitable integral multiple of ω_i to x, we may assume that $0 \leq \lambda_i < 1$. Now we replace ω_i by x in our basis. One checks easily that $|\Delta(\omega_1, \ldots, x, \ldots, \omega_n)| = \lambda_i^2 |\Delta(\omega_1, \ldots, \omega_n)|$ which is integral by *(a)*, non-zero, but smaller than $|\Delta(\omega_1, \ldots, \omega_n)|$. This contradicts the minimality and proves *(b)*.

To see that the discriminant does not depend on the $\mathbf{Z}$-basis $\{\omega_1, \ldots, \omega_n\}$, consider two $\mathbf{Z}$-bases $\omega_1, \ldots, \omega_n$ and $\omega_1', \ldots, \omega_n'$ of O_F. Then there exist integers $\lambda_{ij} \in \mathbf{Z}$ such that $\omega_i' = \sum_{j=1}^n \lambda_{ij}\omega_j$ for $1 \leq j \leq n$. Since the same is true when we reverse the roles of the two bases, the matrix (λ_{ij}) is invertible. Therefore its determinant is equal to ± 1. By Prop.2.8 we have

$$\Delta(\omega_1', \ldots, \omega_n') = \det(\lambda_{ij})^2 \Delta(\omega_1, \ldots, \omega_n) = \Delta(\omega_1, \ldots, \omega_n),$$

as required.

Since F is the field of fractions of O_F, any $\mathbf{Z}$-basis $\omega_1, \ldots, \omega_n$ of O_F is automatically also a $\mathbf{Q}$-basis for F and hence an $\mathbf{R}$-basis for $F_{\mathbf{R}}$ and a $\mathbf{C}$-basis for $F_{\mathbf{C}}$. For a number field of degree n we have the following situation

$$\begin{array}{ccccccc} O_F & \subset & F & \hookrightarrow & F_{\mathbf{R}} & \hookrightarrow & F_{\mathbf{C}} \\ \| & & \| & & \| & & \| \\ \bigoplus_{i=1}^n \mathbf{Z}\omega_i & \subset & \bigoplus_{i=1}^n \mathbf{Q}\omega_i & \subset & \bigoplus_{i=1}^n \mathbf{R}\omega_i & \subset & \bigoplus_{i=1}^n \mathbf{C}\omega_i \end{array}$$

The following proposition says that O_F is *integrally closed.*

Proposition 3.6. *Let F be a number field. Suppose $x \in F$ is a zero of a monic polynomial in $O_F[X]$. Then x is in O_F.*

Proof. Suppose x is a zero of $X^k + a_{k-1}X^{k-1} + \ldots a_1 X + a_0$. Consider the additive subgroup $M = O_F + xO_F + \ldots + x^{k-1}O_F$. Since O_F is finitely generated by Prop. 3.5(b), so is M. Since $xM \subset M$, Proposition 3.1 implies that x is in O_F, as required.

Definition 3.7. The *discriminant* Δ_F of a number field F is the discriminant of a $\mathbf{Z}$-basis $\omega_1, \ldots, \omega_n$ of the ring of integers of O_F.

The discriminant of a number field is a non-zero integer. Since 1 is a $\mathbf{Z}$-basis for $\mathbf{Z}$, the discriminant of $\mathbf{Q}$ is 1. The discriminants of quadratic fields are calculated in Exercise 3.6. In general, it is rather difficult to calculate the discriminant and the ring of integers of a number field. We will come back to this problem in section 6. The following proposition is often useful.

Proposition 3.8. *Let F be a number field of degree n. Suppose $\omega_1, \omega_2, \ldots, \omega_n \in O_F$ have the property that $\Delta(\omega_1, \omega_2, \ldots, \omega_n)$ is a squarefree integer. Then the $\omega_1, \ldots, \omega_n$ form a $\mathbf{Z}$-basis of O_F. In particular, if there exists $\alpha \in O_F$ for which the discriminant $\Delta(1, \alpha, \ldots, \alpha^{n-1})$ is squarefree, then O_F is equal to $\mathbf{Z}[\alpha]$.*

Proof. It follows from Prop.2.8*(c)* that $\Delta(\omega_1, \omega_2, \ldots, \omega_n) = \det(M)^2 \Delta_F$, where $M \in \mathrm{GL}_2(\mathbf{Z})$ is the matrix expressing the ω_i in terms of a $\mathbf{Z}$-base of O_F. Since $\det(M)^2$ is the square of an integer the first statement follows. The second statement is a special case.

Example. Let α be a zero of the polynomial $f(T) = T^3 - T - 1 \in \mathbf{Z}[T]$. Since $f(T)$ is irreducible modulo 2, it is irreducible over $\mathbf{Q}$. Put $F = \mathbf{Q}(\alpha)$. We compute

$$\Delta(1, \alpha, \alpha^2) = \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) \\ \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha^3) \\ \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha^3) & \mathrm{Tr}(\alpha^4) \end{pmatrix}.$$

The trace of 1 is 3. We have

$$f(T) = T^3 - T - 1 = (T - \phi_1(\alpha))(T - \phi_2(\alpha))(T - \phi_3(\alpha)).$$

Let s_1 and s_2 denote the elementary symmetric functions of degree 1 and 2 in the zeroes of $f(T)$. Then $s_1 = 0$ and $s_2 = 1$. It follows that $\mathrm{Tr}(\alpha) = -s_1 = 0$ while $\mathrm{Tr}(\alpha^2) = s_1^2 - 2s_2 = 0 - 2 \cdot -1 = 2$. Since $\alpha^3 = \alpha + 1$, the traces of α^k can be computed using the formula

$$\mathrm{Tr}(\alpha^k) = \mathrm{Tr}(\alpha^{k-2}) + \mathrm{Tr}(\alpha^{k-3}), \qquad \text{for } k \geq 3.$$

We find $\mathrm{Tr}(\alpha^3) = 3$ and $\mathrm{Tr}(\alpha^4) = 3$ and hence

$$\Delta(1, \alpha, \alpha^2) = \det \begin{pmatrix} 3 & 0 & 2 \\ 0 & 2 & 3 \\ 2 & 3 & 2 \end{pmatrix} = -23.$$

Since 23 is prime and hence squarefree, we may apply Prop.3.8 and conclude that the ring of integers of $\mathbf{Q}(\alpha)$ is $\mathbf{Z}[\alpha]$. The discriminant Δ_F is therefore equal to -23.

The fact that the additive group of the ring of integers of a number field F is free of rank $n = [F : \mathbf{Q}]$ has consequences for the structure of the addtive groups of O_F-ideals.

Proposition 3.9. *Let F be a number field with ring of integers O_F. Then*
(a) Every non-zero ideal I of O_F contains a non-zero integer.
(b) Every ideal $I \neq 0$ of O_F has finite index $[O_F : I]$.
(c) There are only finitely many ideals $I \subset O_F$ of a given norm.
(d) Every ideal I of O_F is a finitely generated abelian group.
(e) Every prime ideal $I \neq 0$ of O_F is maximal.

Proof. (a) Let $I \neq 0$ be an ideal of O_F and let $0 \neq x \in I$. Let $f(X) = X^n + \ldots + a_1 X + a_0 \in \mathbf{Z}[X]$ be the minimum polynomial of x. Then a_0 is not zero and since we have $x^n + \ldots + a_1 x = -a_0$, it is contained in I. This proves (a).
By Prop.5 *(b)*, the additive group of O_F is isomorphic to $\mathbf{Z}^n$, where n is the degree of F. Let $I \subset O_F$ be a non-zero ideal. By (a) it contains a non-zero integer m. It follows that O_F/I is a quotient of $O_F/(m) \cong \mathbf{Z}^n/m\mathbf{Z}^n$, which is a finite group. This proves (b). By Lagrange's theorem ideals of norm m contain the integer m. Therefore they are in one to one correspondence with the ideals of the finite ring $O_F/(m)$. This proves (c).

To prove (d), let I be an ideal of O_F. We may assume that $I \neq 0$ and choose an integer $m \in \mathbf{Z}_{>0}$ in I. By *(b)*, the ring $O_F/(m)$ is finite and therefore the ideal $I \pmod{mO_F}$ can be generated, as an abelian group, by a finite number of elements $x_1, \ldots, x_k \in I$. It follows that the additive group I is generated by $x_1, \ldots, x_k$ and $m\omega_1, \ldots, m\omega_n$, where the ω_i are a $\mathbf{Z}$-basis for the ring of integers O_F. We do not need it here, but it follows from the structure of finitely generated abelian groups that the additive group I is actually isomorphic to $\mathbf{Z}^n$. See section 5.
(e) Let $I \neq 0$ be a prime ideal of O_F. By *(b)*, the ring O_F/I is a finite domain. Since finite domains are fields, I is a maximal ideal.

As a consequence of Proposition 3.9 the following definition is justified:

Definition. *Let F be a number field and let $I \neq 0$ be an ideal of the ring of integers of O_F of F. We define the norm $\mathrm{N}(I)$ of the ideal I by*

$$\mathrm{N}(I) = [O_F : I] = \#(O_F/I).$$

The norm $N(I)$ of an ideal $I \subset O_F$ is a positive integer.

3.1. Prove Gauss' Lemma: let R be a unique factorization domain with field of fractions K and let $f \in R[T]$ be a monic polynomial. If $f = g \cdot h$ in $K[T]$, with g and h monic polynomials, then $g, h \in R[T]$. mm

3.2 Show that for every number field F there exists an *integral* element $\alpha \in O_F$ such that $F = \mathbf{Q}(\alpha)$.

3.3 Let $F \subset K$ be an extension of number fields. Show that $O_K \cap F = O_F$.

3.4 Show that the polynomial $X^3 + X - 1 \in \mathbf{Q}[X]$ is irreducible. Let α denote a zero. Determine the ring of integers and the discriminant of the number field $\mathbf{Q}(\alpha)$.

3.5 Let F and K be two quadratic number fields. Show that $F \cong K$ if and only if $\Delta_F = \Delta_K$.

3.6 Let $d \neq 1$ be a squarefree integer. Let F be the quadratic field $\mathbf{Q}(\sqrt{d})$. Show that the discriminant of F is given by

$$\Delta_F = \begin{cases} d & \text{if } d \equiv 1 \pmod 4; \\ 4d & \text{if } d \equiv 2 \text{ or } 3 \pmod 4. \end{cases}$$

3.7 Let $F = \mathbf{Q}(\sqrt[3]{20})$.

(a) Show $\mathbf{Z}[\sqrt[3]{20}, \sqrt[3]{50}] \subset O_F$.

(b) Let $c \in \mathbf{Q}$ with $c\sqrt[3]{20}$ or $c\sqrt[3]{50}$ in O_F. Show that $c \in \mathbf{Z}$.
Let $a, b \in \mathbf{Q}$ and $x = a\sqrt[3]{20} + b\sqrt[3]{50} \in O_F$.

(c) Show that $2a$, $5b$ are in $\mathbf{Z}$ (Hint: $\sqrt[3]{20}x$ and $\sqrt[3]{50}x$ are in O_F.)

(d) Show that $a, b \in \mathbf{Z}$ (hint: x^2 is in O_F) and conclude that $O_F = \mathbf{Z}[\sqrt[3]{20}, \sqrt[3]{50}]$.

3.8 Let $F = \mathbf{Q}(\sqrt[3]{20})$.

(a) Show that the discriminant of F is equal to -2700.

(b) Let $x = a\sqrt[3]{20} + b\sqrt[3]{50}$ for certain integers a, b. Show that $\Delta(1, x, x^2)$ is equal to $-2700(2a^3 - 5b^3)^2$.

(c) Show that the equation $2a^3 - 5b^3 = \pm 1$ has no solutions $a, b \in \mathbf{Z}$. Conclude that O_F is not of the form $\mathbf{Z}[\alpha]$ (Hint: reduce modulo 7 or 9)

3.9*(Stickelberger 1923) Let F be a number field of degree n and discriminant Δ. Let $\phi_i : F \hookrightarrow \mathbf{C}$ be the embeddings of F into $\mathbf{C}$ and let $\{\omega_1, \omega_2, \ldots, \omega_n\}$ be a $\mathbf{Z}$-basis for the ring of integers of F.

By S_n we denote the symmetric group on n symbols and by A_n the normal subgroup of *even* permutations. We define $\Delta^+ = \sum_{\tau \in A_n} \prod_{i=1}^n \phi_i(\omega_{\tau(i)})$ and $\Delta^- = \sum_{\tau \in S_n - A_n} \prod_{i=1}^n \phi_i(\omega_{\tau(i)})$.

(a) Prove that $\Delta = (\Delta^+ - \Delta^-)^2$.

(b) Prove, using Galois theory, that $\Delta^+ + \Delta^-$ e $\Delta^+\Delta^-$ are in $\mathbf{Z}$. Conclude that $\Delta = (\Delta^+ + \Delta^-)^2 - 4\Delta^+\Delta^-$ is congruent to 0 or 1 (mod 4).