8. Minkowski's theorem.

In this section we prove the an important finiteness result in algebraic number theory. We prove that the class group of the ring of integers of a number field is finite.

Theorem 8.1. *(Blichfeldt 1873–1945, Danish-US mathematician) Let L be a lattice in a Euclidean vector space V. Then any measurable set $A \subset V$ with $\mathrm{vol}(A) > \mathrm{covol}(L)$ contains two vectors $\mathbf{a} \neq \mathbf{b}$ for which $\mathbf{a} - \mathbf{b}$ is in L.*

Proof. Let $F \subset V$ be a fundamental domain for L. Then A is a disjoint union of the sets $A_{\mathbf{x}} = A \cap (F + \mathbf{x})$ where $\mathbf{x} \in L$. Next consider the translated sets $A_{\mathbf{x}} - \mathbf{x}$. They are all contained in F. Therefore the volume of their union is at most $\mathrm{vol}(F)$. On the other hand we have

$$\mathrm{vol}(A) = \sum_{\mathbf{x} \in L} \mathrm{vol}(A_{\mathbf{x}}) = \sum_{\mathbf{x} \in L} \mathrm{vol}(A_{\mathbf{x}} - \mathbf{x}).$$

Since $\mathrm{vol}(A) > \mathrm{vol}(F)$, the sum of the volumes of the sets $A_{\mathbf{x}} - \mathbf{x}$ is strictly larger than the volume of their union. This means that some of the sets $A_{\mathbf{x}} - \mathbf{x}$ must have non-empty intersection. In other words, there exist two distinct $\mathbf{x}, \mathbf{y} \in L$ for which $(A_{\mathbf{x}} - \mathbf{x}) \cap (A_{\mathbf{y}} - \mathbf{y})$ is not empty. So there is a vector $\mathbf{v} \in F$ for which both $\mathbf{a} = \mathbf{v} + \mathbf{x}$ and $\mathbf{b} = \mathbf{v} + \mathbf{y}$ are in A. Since $\mathbf{a} - \mathbf{b}$ is equal to the non-zero vector $\mathbf{x} - \mathbf{y}$ in L, we are done.

Theorem 8.2. *(Minkowski's convex body theorem) Let L be a lattice in a Euclidean vector space V. Let B be a bounded, convex, symmetric subset of V. If*

$$\mathrm{vol}(B) > 2^n \mathrm{covol}(L)$$

then there exists a non-zero vector $\mathbf{x} \in L \cap B$.

Proof. Consider the lattice $2L = \{2\mathbf{x} : \mathbf{x} \in L\}$. An application of Blichfeldt's theorem shows that there exist two vectors $\mathbf{x} \neq \mathbf{y}$ in B for which $\mathbf{x} - \mathbf{y}$ is in $2L$. This means that $\frac{1}{2}(\mathbf{x} - \mathbf{y})$ is in L. On the other hand, since B is symmetric, the vector $-\mathbf{y}$ is in B and since B is convex, the vector $\frac{1}{2}(\mathbf{x} - \mathbf{y})$ is in B. This proves the theorem.

We need to compute the volumes of certain convex bodies. Let $k \in \mathbf{R}_{>0}$ and let $f : \mathbf{R}^n \longrightarrow \mathbf{R}_{\geq 0}$ be a continuous function with the property that

$$f(\lambda x) = \lambda^k f(x) \text{ for all } \lambda \in \mathbf{R}_{\geq 0} \text{ and } x \in \mathbf{R}^n,$$
$$B = \{x \in \mathbf{R}^n : f(x) \leq 1\} \text{ is bounded.}$$

This implies that f vanishes only in the origin. By continuity, f attains a minimum $c > 0$ on the unit sphere $S = \{x \in \mathbf{R}^n : f(x) = 1\}$. It follows that the integral $\int_{\mathbf{R}^n} e^{-f(x)} dx$ is at most $\int_0^\infty e^{-ct^k} dt$ times the area of S. Therefore it converges absolutely.

Lemma 8.3. *We have*

$$\mathrm{vol}(B) = \frac{1}{\Gamma(\frac{n}{k} + 1)} \int_{\mathbf{R}^n} e^{-f(x)} dx.$$

Proof. This follows by observing that $\mathbf{R}^n$ is a disjoint union of sets of the form $S_r = \{x \in \mathbf{R}^n : f(x) = r^k\}$ and that f is constant on each S_r. For $t > 0$ we have $S_{rt} = tS_r$. It follows that the volume of $B_r = \{x \in \mathbf{R}^n : f(x) \leq r^k\}$ is equal to $r^n \mathrm{vol}(B)$. On the other hand, we have $\mathrm{vol}(B_r) = \int_0^r \mathrm{area}(S_t)dt$. It follows that $\mathrm{area}(S_r) = \frac{d}{dr}\mathrm{vol}(B_r) = nr^{n-1}\mathrm{vol}(B)$. This gives

$$\int_{\mathbf{R}^n} e^{-f(x)}dx = \int_0^\infty e^{-t^k}\mathrm{area}(S_t)dt = \int_0^\infty e^{-t^k} nt^{n-1}\mathrm{vol}(B)dt = \Gamma(\frac{n}{k}+1)\mathrm{vol}(B),$$

as required.

As an application consider $f(x) = x_1^2 + \ldots + x_n^2$ with $k = 2$. The set B is the n-dimensional unit ball and the integral over $\mathbf{R}^n$ is a product of n integrals of the form $\int_{\mathbf{R}} e^{-x^2}dx = \sqrt{\pi}$. This gives the usual formula for the volume of the unit ball in $\mathbf{R}^n$:

$$\mathrm{vol}(B) = \frac{\pi^{n/2}}{\Gamma(\frac{n}{2}+1)}.$$

Our main application is the convex body given by the function

$$f(x) = |x_1| + \ldots + |x_{r_1}| + 2|z_1| + \ldots + 2|z_{r_2}|,$$

in the Euclidean space $F_{\mathbf{R}}$. In this case $k = 1$ and the integral of Lemma 8.3 is equal to the product $I^{r_1}J^{r_2}$, where $I = \int_{\mathbf{R}} e^{-|x|}dx = 2$ and J is the integral over $\mathbf{C}$ of the function $e^{-2|z|}$. Keeping in mind that identifying $\mathbf{C}$ with $\mathbf{R}^2$ in the usual way, doubles the scalar product on $\mathbf{R}^2$, we get $J = 2\int_{\mathbf{R}^2} e^{-2\sqrt{x^2+y^2}}dxdy = \pi$ and hence

$$\mathrm{vol}(B) = \frac{2^{r_1}\pi^{r_2}}{n!}.$$

Theorem 8.4. *(Minkowski) Let F be a number field of degree n. Let r_1 denote the number of real embeddings $\phi : F \hookrightarrow \mathbf{R}$ and r_2 the number of pairs of complex embeddings $F \hookrightarrow \mathbf{C}$. Then every non-zero ideal I of O_F contains an element x with*

$$|N(x)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}|\Delta_F|^{1/2}N(I).$$

Proof. We view the ideal I via the map $\Phi : O_F \longrightarrow F_{\mathbf{R}}$ as a lattice in $F_{\mathbf{R}} \cong \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$. By Prop.5.10*(ii)* the covolume of I in V_F is

$$\mathrm{covol}(I) = N(I)|\Delta_F|^{1/2}.$$

For any positive real number R we put

$$X(R) = \{(x_1, \ldots, x_{r_1}, y_1, \ldots, y_{r_2}) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2} : |x_1| + \ldots + |x_{r_1}| + 2|y_1| + \ldots + 2|y_{r_2}| \leq R\}.$$

Using the triangle inequality one easily verifies that $X(R)$ is a convex, symmetric and bounded set. By Lemma 7.2 its volume is given by

$$\mathrm{vol}(X(R)) = R^n\frac{2^{r_1}\pi^{r_2}}{n!}.$$

From Minkowski's convex body Theorem 7.1 we conclude that *if*

$$R^n \frac{2^{r_1}\pi^{r_2}}{n!} > 2^n \cdot N(I)|\Delta_F|^{1/2},$$

then there exists a non-zero element $x \in I \cap X(R)$. Since for every R the set $X(R)$ is bounded, and since the set $I \cap X(R)$ is finite, it follows that there is a vector $x \in I$ such that $x \in X(R)$ for *every* R satisfying this inequality. This vector x is also contained in $X(R_0)$ where R_0 satisfies the equality

$$\frac{R_0^n}{n!}\pi^{r_2}2^{r_1} = 2^n \cdot N(I)|\Delta_F|^{1/2}.$$

By Prop.2.7*(iii)* and the arithmetic-geometric-mean-inequality (Exer.7.D), we have that

$$\begin{aligned}
|N(x)| &= |x_1| \cdot \ldots |x_{r_1}||y_1|^2 \cdot \ldots \cdot |y_{r_2}|^2, \\
&\leq \left(\frac{|x_1| + \ldots + |x_{r_1}| + 2|y_1| + \ldots + 2|y_{r_2}|}{n}\right)^n, \\
&\leq \frac{R_0^n}{n^n} = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} |\Delta_F|^{1/2} N(I)
\end{aligned}$$

as required.

Corollary 8.5. *Let F be a number field of degree n. Then*
(a)

$$|\Delta_F| \geq \left(\frac{n^n}{n!}(\frac{\pi}{4})^{r_2}\right)^2.$$

(b) $|\Delta_F| \geq \frac{\pi^n}{4}$. *In particular,* $|\Delta_F| > 1$ *whenever* $F \neq \mathbf{Q}$.
(c) Every ideal class contains an ideal I with

$$|N(I)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} |\Delta_F|^{1/2}.$$

(d) The class group $Cl(O_F)$ is finite.

Proof. *(a)* It follows from the multiplicativity of the norm (Prop.4.6) that for every ideal I and $x \in I$, one has that $|N(x)| \geq N(I)$. Combining this with Theorem 7.3 gives *(a)*
(b) One verifies (by induction) that $n^n \geq 2^{n-1}n!$ for all $n \geq 1$. It follows from *(i)* that

$$|\Delta_F| \geq \left(\frac{n^n}{n!}\right)^2 \left(\frac{\pi}{4}\right)^{2r_2} \geq (2^{n-1})^2 \left(\frac{\pi}{4}\right)^n = \frac{\pi^n}{4}.$$

(c) Let c be an ideal class. Every ideal class contains integral ideals. Pick an integral ideal J in the inverse of the class of I. By Theorem 7.3 there exists an element $x \in J$ with

$$\left|N(xJ^{-1})\right| \leq \frac{n!}{n^n}\left(\frac{\pi}{4}\right)^{-r_2} |\Delta_F|^{1/2}.$$

Since the ideal xJ^{-1} is integral and in c, the result follows.
(d) By Prop.4.8*(iii)* there are only a finite number of prime ideals of a given norm. Therefore, for every number B, there are only a finite number of integral ideals of norm less than B. The result now follows from *(iii)*.

The cardinality of the class group $Cl(O_F)$ is called the *class number* of O_F, or of F. It is denoted by

$$h_F = \#Cl(O_F).$$

The expression

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\Delta_F|}$$

associated to a number field F, with the usual notations, is called the *Minkowski constant* associated to F. Using Stirling's formula is is easy to see that Cor.7.4*(i)* implies that for large values of n we have

$$\begin{aligned}|\Delta_F|^{1/n} &\geq \left(\frac{e^2\pi}{4}\right)\left(\frac{4}{\pi}\right)^{\frac{r_1}{n}},\\ &\geq (5.803)(1.273)^{\frac{r_1}{n}}.\end{aligned}$$

Minkowski's Theorem can be used to calculate class groups of rings of integers of number fields. In this section we present two small examples. In the next section we will give more elaborate examples.

Examples. *(i)* Take $F = \mathbf{Q}(\alpha)$ where α is a zero of the polynomial $f(T) = T^3 - T - 1$. In section 2 we have calculated the discriminant Δ_F of F. We have that $\Delta_F = \mathrm{Disc}(f) = -23$. It is easily verified that the polynomial $T^3 - T - 1$ has precisely one real zero. So $r_1 = 1$ and $r_2 = 1$. The bound in Minkowski's Theorem is now

$$\frac{3!}{3^3}\left(\frac{4}{\pi}\right)\sqrt{23} \approx 1.356942.$$

Therefore, by Cor.7.4*(iii)*, every ideal class contains an integral ideal of norm less than or equal to 1. This shows, at once, that the class group of F is trivial. (By Exer.7.R the ring of integers $\mathbf{Z}[\alpha]$ is even Euclidean!)
(ii) Take $F = \mathbf{Q}(\sqrt{-47})$. By the example in section 2, the ring of integers of F is $\mathbf{Z}[\frac{1+\sqrt{-47}}{2}]$ and the discriminant of F satisfies $\Delta_F = -47$. Since $r_1 = 0$ and $r_2 = 1$ we find that the Minkowski constant is equal to

$$\frac{2!}{2^2}\left(\frac{4}{\pi}\right)\sqrt{47} \approx 4.36444.$$

Therefore the class group is generated by the prime ideals of norm less than or equal to 4. To find these prime ideals explicitly, we decompose the primes 2 and 3 in O_F. Let $\alpha = \frac{1+\sqrt{-47}}{2}$. Then $\alpha^2 - \alpha + 12 = 0$. By the Factorization Lemma (Theorem 6.1) we see that $(2) = \mathfrak{p}_2\mathfrak{p}_2'$ where $\mathfrak{p}_2 = (2, \alpha)$ and $\mathfrak{p}_2' = (2, \alpha - 1)$. Similarly $(3) = \mathfrak{p}_3\mathfrak{p}_3'$ where

$\mathfrak{p}_3 = (3, \alpha)$ and $\mathfrak{p}'_3 = (3, \alpha - 1)$. We conclude that the only ideals of O_F of norm less than 4.36444 are O_F, $\mathfrak{p}_2$, $\mathfrak{p}'_2$, $\mathfrak{p}_3$, $\mathfrak{p}'_3$, $\mathfrak{p}_2^2$, $\mathfrak{p}_2'^2$, $\mathfrak{p}_2\mathfrak{p}'_2$. Therefore the class number is at most 8.

Since $(2) = \mathfrak{p}_2\mathfrak{p}'_2$, the ideal classes of $\mathfrak{p}_2$ and $\mathfrak{p}'_2$ are each others inverses: $\mathfrak{p}'_2 \sim \mathfrak{p}_2^{-1}$. Similarly $\mathfrak{p}'_3 \sim \mathfrak{p}_3^{-1}$. We conclude that the class group is generated by the classe of $\mathfrak{p}_2$ and $\mathfrak{p}_3$.

In order to determine the class group, we decompose some principal ideals into prime factors. Principal ideals (β) can be factored, by first factoring their norm $N(\beta) \in \mathbf{Z}$ and then determining the prime ideal divisors of (β). For the sake of convenience we take elements β of the form $\beta = \alpha - k$ where $k \in \mathbf{Z}$ is a small integer. By Exer.2.F we have that $N(\beta) = N(k - \alpha) = k^2 - k + 12$.

We find

Table.

	k	β	$N(\beta)$	(β)
(i)	1	$1-\alpha$	$12 = 2^2 \cdot 3$	${\mathfrak{p}'_2}^2\mathfrak{p}'_3$
(ii)	2	$2-\alpha$	$14 = 2 \cdot 7$	$\mathfrak{p}_2\mathfrak{p}_7$
(iii)	3	$3-\alpha$	$18 = 2 \cdot 3^2$	$\mathfrak{p}'_2{\mathfrak{p}_3}^2$
(iv)	4	$4-\alpha$	$24 = 2^3 \cdot 3$	${\mathfrak{p}_2}^3\mathfrak{p}_3$
(v)	5	$5-\alpha$	$32 = 2^5$	${\mathfrak{p}'_2}^5$

From entry (i), we see that the ideal class of ${\mathfrak{p}'_2}^2\mathfrak{p}'_3 \sim (1)$ is trivial. The relation implies that

$$\mathfrak{p}_3 \sim \mathfrak{p}_2^{-1}.$$

We conclude that the class group is *cyclic.* It is generated by the class of $\mathfrak{p}_2$. We will now determine the order of this class. The second entry tells us that $\mathfrak{p}_7 \sim \mathfrak{p}_2^{-1}$ and is not of much use to us. Relation (iii) implies that

$$\mathfrak{p}_2 \sim \mathfrak{p}_3^2.$$

Combining this with the relation obtained from the first entry of our table, gives at once that

$$\mathfrak{p}_2^5 \sim 1.$$

This relation can also be deduced directly from entry (v) of the table. It follows that the class group is cyclic of order 5 or 1. The latter case occurs if and only if the ideal $\mathfrak{p}_2$ is principal. Suppose that for $a, b \in \mathbf{Z}$ the element $\gamma = a + b(1+\sqrt{-47})/2 \in O_F$ is a generator of $\mathfrak{p}_2$. Since the norm of $\mathfrak{p}_2$ is 2, we must have that

$$2 = N(\mathfrak{p}_2) = |N(\gamma)| = a^2 + ab + 12b^2.$$

Writing this equation as $(2a+b)^2 + 47b^2 = 8$, it is immediate that there are no solutions $a, b \in \mathbf{Z}$. We conclude that $\mathfrak{p}_2$ is not principal and that $Cl_{\mathbf{Q}(\sqrt{-47})} \cong \mathbf{Z}/5\mathbf{Z}$.

Corollary 8.6. *(J. Hermite, French mathematician 1822–1901) Let $\Delta \in \mathbf{Z}$. Up to isomorphism there are only finitely many number fields F with $|\Delta_F| = \Delta$.*

Proof. Let $\Delta \in \mathbf{Z}$. By Cor.8.5 (b) there are only finitely many possible values for the degree n of F. Therefore we may assume that the degree n is fixed. Let F be a number field of degree n and discriminant Δ. In the usual notation we have $n = r_1 + 2r_2$.

We consider a certain bounded, convex and symmetric box B in $F_{\mathbf{R}}$. If F is totally complex, i.e. if $r_1 = 0$ the $\mathbf{R}$-algebra $F_{\mathbf{R}}$ is isomorphic to $\mathbf{C}^{r_2}$ and we put

$$B = \{(z_1, \ldots, z_{r_2}) \in F_{\mathbf{R}} : \ |\mathrm{Re}(z_1)| \leq 1, \ |\mathrm{Im}(z_1)| \leq \sqrt{|\Delta|} + 1 \text{ and } |z_i| < 1 \text{ for } i \geq 2\}.$$

If $r_1 = 1$ we put

$$B = \{(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \in F_{\mathbf{R}} : |z_i| < 1 \text{ for } i \geq 1 \text{ and } |x_i| < \begin{cases} \sqrt{|\Delta|} + 1, & \text{for } i = 1, \\ 1, & \text{for } i \geq 2. \end{cases} \}$$

It is easily checked that volume of B is $8(2\pi)^{r_2 - 1}(\sqrt{|\Delta|} + 1)$ in the first case, while it is $2^{r_1}(2\pi)^{r_2}(\sqrt{|\Delta|} + 1)$ in the second. In either case $\mathrm{vol}(B)$ exceeds $2^n \mathrm{covol}(O_F)$. By Minkowski's convex body theorem there exists a non-zero element $\alpha \in O_F$ for which the element $(\phi_1(\alpha), \ldots, \phi_n(\alpha))$ of $F_{\mathbf{R}}$ is in B.

Since α is not zero, its norm is at least 1. The fact that $\alpha \in B$ implies that $|\phi_i(\alpha)| < 1$ for all $i > 1$. We conclude that $|\phi_1(\alpha)| \geq 1$. It follows that $\phi_1(\alpha) \neq \phi_i(\alpha)$ for all $i \geq 2$. Indeed, this is clear when $r_1 > 0$. In this case we even have $|\phi_i(\alpha)| < |\phi_1(\alpha)|$ for all $i \geq 2$. In the case $r_1 = 0$, the same is true for all embeddings except the complex conjugate of ϕ_1. However, if it were the case that $\phi_1(\alpha) = \overline{\phi}_1(\alpha)$, then $\phi_1(\alpha)$ is in $\mathbf{R}$, which implies $|\phi_1(\alpha)| = |\mathrm{Re}(\phi_1(\alpha))| < 1$, which is a contradiction.

Let $f(T)$ denote the characteristic polynomial of α. Its zeroes are $\phi_1(\alpha), \ldots, \phi_n(\alpha)$. Since $\phi_1(\alpha) \neq \phi_i(\alpha)$ for all $i \geq 2$, the polynomial $f(T)$ has a simple zero. Prop. 2.7 (c) therefore implies that $f(T)$ is also the minimum polynomial of α. It follows that $F = \mathbf{Q}(\alpha)$.

Since the zeroes $\phi_i(\alpha)$ of $f(T)$ have absolute values bounded by $\sqrt{|\Delta|} + 1$, the coefficients of f are bounded as well. Since the coefficients are in $\mathbf{Z}$, there are only finitely many possibilities for f and therefore, up to isomorphism, for the field F. This proves the corollary.

8.0 (Jensen's inequality) Let $n \geq 1$, let $x_1, \ldots, x_n$ in the interval $[a, b] \subset \mathbf{R}$ and $\lambda_1, \ldots, \lambda_n$ be 'weights' in the interval $(0, 1)$ satisfying $\sum_{i=1}^n \lambda_i = 1$. Suppose f is a *convex* function on the interval $[a, b]$.

(a) Show that we have $f(\sum_{i=1}^n \lambda_i x_i) \leq \sum_{i=1}^n \lambda_i f(x_i)$.

(b) Apply (a) to the convex function "$-\log$" and prove the arithmetic-geometric mean inequaliy

$$\left(\prod_{i=1}^n x_i\right)^{1/n} \leq \frac{1}{n} \sum_{i=1}^n x_i,$$

with equality if and only if all x_i are equal. A function is called *convex* on $[a, b]$ if for each $x, x' \in [a, b]$ we have $f(\frac{x+x'}{2}) \leq \frac{f(x)+f(x')}{2}$.

8.1 Let $\Gamma(s) = \int_0^\infty e^x x^s \frac{dx}{x}$ denote Euler's gamma function.
  (a) Prove that the integral converges absolutely for $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$.
  (b) Show that $s\Gamma(s) = \Gamma(s+1)$ for $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$.
  (c) Show that $\Gamma(n+1) = n!$ for $n \in \mathbf{Z}_{>0}$.
  (d) Show that $\Gamma(\frac{1}{2}) = \sqrt{\pi}$.

8.2 Show that $\mathbf{Z}[\sqrt{-163}]$ has trivial class group and that $\mathbf{Z}[\sqrt{-71}]$ has class group isomorphic to $\mathbf{Z}/7\mathbf{Z}$.

8.3 Show that the class group of $\mathbf{Q}(\alpha)$ where α is a zero of the polynomial $T^3 + T - 1$ is trivial.

8.4 Show that the class group of $\mathbf{Q}(\zeta_{11})$ is trivial.

8.5 Let $f(T) \in \mathbf{Z}[T]$. Show: if $\mathrm{Disc}(f) = 1$, then $f(T) = (T-k)(T-k-1)$ for some $k \in \mathbf{Z}$.

8.6 Show that the ring $\mathbf{Z}[(1+\sqrt{19})/2]$ is *not* Euclidean, but admits unique factorization.

8.7 Show that the ring $\mathbf{Z}[\sqrt{-5}]$ has class number 2.

8.8 Suppose $x, y \in \mathbf{Z}$ satisfy $y^2 = x^3 - 5$.
  (a) Show that x is odd and y is even.
  (b) Show that $y + \sqrt{-5}$ and $y - \sqrt{5}$ are coprime in the ring $\mathbf{Z}[\sqrt{-5}]$.
  (c) Show that the ideal $(y + \sqrt{-5})$ is the cube of an ideal of $\mathbf{Z}[\sqrt{-5}]$.
  (d) Show that $y - \sqrt{-5}$ is the cube of an *element* of $\mathbf{Z}[\sqrt{-5}]$ (Hint: previous exercise)
  (e) Show that the Diophantine equation $Y^2 = X^3 - 5$ has no solutions $X, Y \in \mathbf{Z}$.

8.9 Let F be a number field. Show that if

$$\frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} |\Delta_F|^{1/2} < 2$$

then the ring of integers O_F is a Euclidean for the norm $|N(x)|$. (Hint: Let $x \in F_{\mathbf{R}}$. Show, using the notation of the proof of Theorem 7.3, that the set $X(R) \cup (X(R) + x)$ with $R = n$ has a volume that is larger than $2^n \mathrm{covol}(O_F)$. Show that it contains a lattice point.)