

University of Utah
Algebraic Number Theory

Dick Gross

Notes by Sean Sather-Wagstaff

Introduction

These notes are based on a semester-long course in algebraic number theory given at the University of Utah during the Spring of 1999. The author learned the subject from John Tate and has used many of Tate's unpublished ideas here.

Throughout these notes, we shall employ the following notations. For a ring A , we let A^\times denote the multiplicative group of units in A . If A is a subgroup (resp. subfield) of B , we let $(B : A)$ denote the index (resp. degree) of A in B . For a finite extension of fields $k \subseteq K$, we let Tr and \mathbb{N} denote the trace and norm maps, respectively.

Lecture 1

One of our first goals is to discuss the properties of the ring of integers in a number field. To accomplish this, we shall first consider general lattices in a rational vector space.

Definition. Let V be a finite dimensional vector space of dimension n over the rational numbers \mathbb{Q} . A *lattice* in V is a free abelian subgroup $L \subset V$ of rank n .

Assume that L is a lattice in V with $v_1, \dots, v_n \in V$ such that $L = \mathbb{Z}v_1 + \mathbb{Z}v_2 + \dots + \mathbb{Z}v_n$. Then the set $\{v_1, \dots, v_n\}$ forms a basis for V . It suffices to show that the v_i are linearly independent over \mathbb{Q} . Suppose that $\sum_i a_i v_i = 0$ for some $a_1, \dots, a_n \in \mathbb{Q}$. Choose a nonzero integer N so that Na_i is an integer for each i . Then $0 = N \sum_i a_i v_i = \sum_i Na_i v_i$ which is a sum of elements in L . Thus, each $Na_i = 0$ which implies that each $a_i = 0$.

We recall that the set of bases of V (over \mathbb{Q}) is in bijection with $GL(V)$ and the set of bases of L (over \mathbb{Z}) is in bijection with $\text{Aut}(L) = GL_n(\mathbb{Z})$. It follows from the previous comments that the set of lattices in V is in bijection with $GL(V)/\text{Aut}(L) \cong GL_n(\mathbb{Q})/GL_n(\mathbb{Z})$.

If M is a subgroup of L of finite index, then M is also a lattice in V . This follows from the fact that the quotient L/M is a finitely generated, *torsion* abelian group, and is therefore of the form $\mathbb{Z}/a_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/a_n\mathbb{Z}$ for some integers $a_i \geq 1$. It follows that there is a basis v_1, \dots, v_n of L such that $a_1 v_1, \dots, a_n v_n$ is a basis of M .

For any $\alpha \in GL(V)$, the image $\alpha(L)$ is another lattice in V . In particular, if $\alpha \in \mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ then αL is another lattice in V , with basis $\{\alpha v_1, \dots, \alpha v_n\}$.

If M and L are lattices in V , then there exists $\alpha, \beta \in \mathbb{Q}^\times$ such that $\alpha L \subseteq M \subseteq \beta L$ where each subgroup has finite index. It should be noted that this fact does not hold in a real vector space.

Definition. Assume that $\langle \cdot, \cdot \rangle : V \otimes V \rightarrow \mathbb{Q}$ is a nondegenerate bilinear form. Then there

is an isomorphism $V \rightarrow \text{Hom}(V, \mathbb{Q})$ which is given by $v \rightarrow \langle v, \cdot \rangle$. Assume that L is a lattice in V and define the *dual lattice* L^* of L to be $L^* = \{v \in V : \langle v, L \rangle \subseteq \mathbb{Z}\}$. The dual lattice is, in fact, a lattice: if $\{v_1, \dots, v_n\}$ is a basis of L , then L^* has the dual basis (over \mathbb{Z}) $\{v_1^*, \dots, v_n^*\}$ where v_i^* is given by $\langle v_i, v_j^* \rangle = \delta_{i,j}$ where $\delta_{i,j}$ is the Kronecker delta function.

Definition. Under these assumptions let E denote the “inner product matrix” $E = (\langle v_i, v_j \rangle)$. We define the *discriminant* of L as $\text{disc}(L) = \det(E) \in \mathbb{Q}^\times$. This is independent of the basis chosen. To see this, fix a change-of-basis matrix $A \in GL_n(\mathbb{Z})$. After changing basis, the new inner product matrix is $E' = AEA^t$ whose determinant is $\det(E') = \det(A)^2 \det(E) = \det(E)$.

Definition. By multiplying our bilinear form by a nonzero integer, we may assume that $\langle L, L \rangle \subseteq \mathbb{Z}$. We note that this condition is equivalent to the condition $L \subseteq L^*$. A lattice satisfying these equivalent conditions is called *integral*. By definition, if L is an integral lattice, then $\text{disc}(L) \in \mathbb{Z}$. Furthermore, we have the following proposition.

Proposition 1. *The index $(L^* : L) = \pm \text{disc}(L)$.*

Proof. Since L is a subgroup of L^* , and both groups are free abelian of rank n , the additivity of rank on short exact sequences shows that the rank of the quotient L^*/L is zero. Since the quotient is finitely generated, the classification of finitely generated abelian groups shows that the quotient is a finite group. Thus, the index $(L^* : L)$ is finite. From the observations above, it follows that there is a basis $\{v_1^*, \dots, v_n^*\}$ of L^* and nonzero integers a_1, \dots, a_n such that the set $\{a_1 v_1^*, \dots, a_n v_n^*\}$ forms a basis of L . Furthermore, $L^*/L \cong \bigoplus_{i=1}^n \mathbb{Z}/a_i \mathbb{Z}$, so that $(L^* : L) = |\prod_{i=1}^n a_i|$. Let $\{v_1, \dots, v_n\}$ denote the dual basis of L . Let E and E' denote the inner product matrices $E = (\langle v_i, v_j \rangle)$ and $E' = (\langle v_i, a_j v_j^* \rangle)$. By definition, E' is the diagonal matrix

$$E' = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}$$

There is a matrix $A \in GL_n(\mathbb{Z})$ such that $E' = EA$, and it follows that

$$\text{disc}(L) = \det(E) = \pm \det(E') = \pm a_1 \cdots a_n.$$

Thus, $(L^* : L) = |\prod_{i=1}^n a_i| = \pm \text{disc}(L)$. □

Definition. A lattice L is *unimodular* if $L = L^*$. By the proposition, we see that this is equivalent to the condition that $\text{disc}(L) = \pm 1$.

In the general (i.e., not necessarily unimodular) case, the inner product on V induces a pairing $\langle, \cdot \rangle : L^*/L \otimes L^*/L \rightarrow \mathbb{Q}/\mathbb{Z}$ which is a duality of finite abelian groups. It follows that the set of unimodular lattices M which lie between L and L^* is in bijection with the subgroups A of L^*/L such that $A = A^\perp$ under $\langle, \cdot \rangle$.

Example. Consider the lattice $\mathbb{Z}^n \subset \mathbb{Q}^n$ with $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_i x_i y_i$. Then \mathbb{Z}^n is a self-dual lattice and $e_i^* = e_i$.

Definition. An integral lattice L is *even* if, for all $v \in L$, $\langle v, v \rangle \in 2\mathbb{Z}$. Note that the previous example is not even.

Example. With \mathbb{Z}^n as in the previous example, let $L = \{\sum_i a_i e_i : \sum_i a_i \in 2\mathbb{Z}\}$. Then $L \subset \mathbb{Z}^n$ is a sublattice of index 2. Furthermore, L is even since $\sum_i a_i^2 \equiv \sum_i a_i \pmod{2}$.

Lemma 2. Assume that M and L are lattices in $(V, \langle \cdot, \cdot \rangle)$ such that M is a sublattice of L of index N . Then $\text{disc}(M) = N^2 \text{disc}(L)$.

Example. If $L \subseteq \mathbb{Z}^n$ is the even sublattice of the previous example, then the lemma implies that $\text{disc}(L) = 4$.

Proof. It is straight-forward to check that we have the following containments: $M \subseteq L \subseteq L^* \subseteq M^*$. We claim that the index $(M^*, L^*) = N$. Since $\langle \cdot, \cdot \rangle : M^*/L^* \otimes L/M \rightarrow \mathbb{Q}/\mathbb{Z}$ is a duality of finite abelian groups and L/M has order N , it follows that M^*/L^* also has order N by the theory of finite abelian groups. By Proposition 1, we see that

$$\text{disc}(M) = \pm(M^* : M) = \pm(L : M)(L^* : L)(M^* : L^*) = \pm N^2(L^* : L) = \pm N^2 \text{disc}(L).$$

Finally, $\text{disc}(L)$ and $\text{disc}(M)$ have the same sign. To see this, choose a basis v_1, \dots, v_n of L such that there are nonzero integers a_1, \dots, a_n such that $a_1 v_1, \dots, a_n v_n$ is a basis of M . Then

$$\text{disc}(M) = \det(\langle a_i v_i, a_j v_j \rangle) = \det(a_i a_j \langle v_i, v_j \rangle) = \left(\prod_i a_i^2 \right) \det(\langle v_i, v_j \rangle) = \left(\prod_i a_i^2 \right) \text{disc}(L)$$

as desired. \square

Example. Let $L \subset \mathbb{Z}^n$ be the even sublattice from the previous example. Then $L \subset \mathbb{Z}^n \subset L^*$. Since \mathbb{Z}^n is unimodular, the proof of Lemma 2 shows that $(\mathbb{Z}^n : L) = 2 = (L^* : \mathbb{Z}^n)$. One can verify directly that the element $\eta = \frac{1}{2}(e_1 + \dots + e_n)$ is contained in L^* , but not in \mathbb{Z}^n . If n is odd, then $2\eta \notin L$ and $4\eta \in L$, and it follows that $L^*/L \cong \mathbb{Z}/4\mathbb{Z}$. If n is even, then every element of L^*/L is annihilated by 2, so that $L^*/L \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

The inner product induces a pairing $\langle \cdot, \cdot \rangle : L^*/L \times L^*/L \rightarrow (\frac{1}{2}\mathbb{Z})/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$. We claim that for $v \in L^*/L$, $\langle v, v \rangle = 0$ in \mathbb{Q}/\mathbb{Z} if and only if $n \equiv 0 \pmod{4}$. If $n \not\equiv 0 \pmod{4}$ then $\langle \eta, \eta \rangle = \frac{1}{4}n \notin \mathbb{Z}$. Assume that $n \equiv 0 \pmod{4}$. It is always the case that for $v \in \mathbb{Z}^n$, $\langle v, v \rangle \in \mathbb{Z}$, so we need only check η : $\langle \eta, \eta \rangle = \frac{1}{4}n \in \mathbb{Z}$ since n is divisible by 4.

In the case when $L^*/L \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, there are exactly three distinct nontrivial subgroups of L^*/L . Thus, there are exactly three lattices in k which live between L and L^* . \mathbb{Z}^n is one of these lattices, and we call the others M and M' . We claim that $n \equiv 0 \pmod{4}$ if and only if M and M' are integral and unimodular. (Of course, by checking indexes, we see that M and M' are always unimodular, so the second condition is equivalent to M and M' being integral.) This follows from the fact that there are elements $v \in M$ and $v' \in M'$ such that $M = L + \mathbb{Z}v$ and $M' = L + \mathbb{Z}v'$. Then $\langle v, v \rangle$ and $\langle v', v' \rangle$ are integers if and only if for every $v'' \in L^*$, $\langle v'', v'' \rangle$ is an integer.

Finally, if $n \equiv 0 \pmod{8}$, then M and M' are both even. (This is the best of all worlds.) The point here is that $\langle \eta, \eta \rangle = \frac{1}{4}n \in 2\mathbb{Z}$ since n is divisible by 8. For more discussion and interesting applications, the interested reader is encouraged to consult *Sphere Packing, Lattices and Groups* by Conway and Sloane.

In order to define algebraic numbers and algebraic integers, we need the following propositions.

Proposition 3. For any complex number α the following conditions are equivalent:

1. α satisfies a monic polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with rational coefficients.
2. The smallest subfield $\mathbb{Q}(\alpha)$ of \mathbb{C} containing \mathbb{Q} and α is of finite degree over \mathbb{Q} .
3. There is a field k of finite degree over \mathbb{Q} which contains α .

Definition. We say that a complex number α is *algebraic* if one of these equivalent conditions holds.

Proof. “2. \Rightarrow 3.” clear

“1. \Rightarrow 2.” Since α satisfies a monic polynomial with rational coefficients, there exists unique such (monic) polynomial $g_\alpha(x) \in \mathbb{Q}[x]$ with minimal degree. Then $g_\alpha(x)$ is the generator of the nonzero ideal $I \subset \mathbb{Q}[x]$ of polynomials satisfied by α . I is a maximal ideal and the map $\mathbb{Q}[x]/I \rightarrow \mathbb{Q}(\alpha)$ given by $x + I \mapsto \alpha$ is an isomorphism. This implies that the degree of $\mathbb{Q}(\alpha)$ over \mathbb{Q} is finite.

“3. \Rightarrow 1.” The map $\alpha : k \rightarrow k$ given by multiplication by α is \mathbb{Q} -linear. The monic polynomial

$$f(x) = \det(xI - \alpha) = x^n - \text{Tr}(\alpha)x^{n-1} + \cdots \pm \det(\alpha)$$

is clearly satisfied by α . □

Corollary 4. The set $\overline{\mathbb{Q}}$ of algebraic numbers forms a subfield of \mathbb{C} .

Proof. Assume that $\alpha, \beta \neq 0$ are algebraic. It suffices to show that $\alpha \pm \beta$, $\alpha\beta$ and α/β are algebraic as well. Let $k = \mathbb{Q}(\alpha, \beta)$ denote the smallest subfield of \mathbb{C} containing $\mathbb{Q}, \alpha, \beta$. Then the degree $(k : \mathbb{Q}(\alpha)) = (\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)) \leq (\mathbb{Q}(\beta) : \mathbb{Q})$ is finite since β is algebraic. Thus, $(k : \mathbb{Q}) = (\mathbb{Q}(\alpha) : \mathbb{Q})(k : \mathbb{Q}(\alpha))$ is finite. Since the desired elements are all contained in k , they are all algebraic as desired. □

Proposition 5. For any complex number α the following conditions are equivalent:

1. α satisfies a monic polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with integer coefficients.
2. $\mathbb{Z}[\alpha]$ is a \mathbb{Z} -module of finite rank.
3. There is a subring $M \subset \mathbb{C}$ containing α which has finite rank as a \mathbb{Z} -module.

Definition. We say that a complex number α is an *algebraic integer* if one of these equivalent conditions holds.

Proof. “1. \Rightarrow 2.” $\mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{n-1}$.

“2. \Rightarrow 3.” clear

“3. \Rightarrow 1.” The argument from Proposition 3 applies. The map $\alpha : M \rightarrow M$ is an endomorphism of a free \mathbb{Z} -module. Therefore, the coefficients of the polynomial

$$f(x) = \det(xI - \alpha) = x^n - \text{Tr}(\alpha)x^{n-1} + \cdots \pm \det(\alpha)$$

are integers. □

Corollary 6. *The set $\overline{\mathbb{Z}}$ of algebraic integers forms a subring of $\overline{\mathbb{Q}}$.*

Proof. As before, given algebraic integers α, β , let $M = \mathbb{Z}[\alpha, \beta]$. This ring has finite rank as a \mathbb{Z} -module and contains $\alpha \pm \beta, \alpha\beta$. \square

Lemma 7. *With notation as above:*

1. $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.
2. $\overline{\mathbb{Q}}/\overline{\mathbb{Z}}$ is a torsion group (like \mathbb{Q}/\mathbb{Z}).

Proof. 1. For $a \in \mathbb{Z}$, a satisfies the monic polynomial $x - a \in \mathbb{Z}[x]$. This gives the containment “ \supseteq ”. For the other containment, fix $\alpha = a/b \in \overline{\mathbb{Z}} \cap \mathbb{Q}$ and suppose that $\alpha \notin \mathbb{Z}$. Without loss of generality, we assume that a and b are relatively prime. Since $\alpha \notin \mathbb{Z}$, it follows that $b \neq \pm 1$. If α satisfies the monic polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$, then

$$a^n/b^n + a_{n-1}a^{n-1}/b^{n-1} + \cdots + a_0 = 0.$$

Multiplication by b^n yields the equation

$$a^n + \underbrace{ba^{n-1}a_{n-1} + \cdots + b^na_0}_{\text{divisible by } b} = 0$$

which implies that a^n is divisible by b . However, since b is not a unit and $(a, b) = 1$, we see that this is a contradiction.

2. Assume that α satisfies the polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Q}[x]$. For a positive integer N , let $\beta = N\alpha$. Then

$$0 = N^n((\beta/N)^n + a_{n-1}(\beta/N)^{n-1} + \cdots + a_0) = \beta^n + Na_{n-1}\beta^{n-1} + \cdots + N^n a_0$$

which implies that if we choose N such that $N^i a_{n-i} \in \mathbb{Z}$, then $\beta = N\alpha \in \overline{\mathbb{Z}}$. Thus, $\overline{\mathbb{Q}}/\overline{\mathbb{Z}}$ is a torsion group. \square

Lecture 2

Let $k \supseteq \mathbb{Q}$ be a number field. It follows from the definition that every element of k is algebraic. Let A denote the subring of algebraic integers in k , that is, $A = k \cap \overline{\mathbb{Z}}$. It follows that $A \cap \mathbb{Q} = \mathbb{Z}$.

Theorem 8. *A is a lattice in the rational vector space k .*

Proof. First, we claim that A contains a lattice L in k . To see this, fix a basis v_1, \dots, v_n of k over \mathbb{Q} . Since $\overline{\mathbb{Q}}/\overline{\mathbb{Z}}$ is a torsion group, there exists nonzero integer N such that $Nv_1, \dots, Nv_n \in A$. Let $L = Nv_1\mathbb{Z} + \cdots + Nv_n\mathbb{Z}$, which is a lattice in k contained in A .

Now, consider the linear and bilinear forms on k defined by

$$\begin{array}{ll} k \rightarrow \mathbb{Q} & k \times k \rightarrow \mathbb{Q} \\ \alpha \mapsto \text{Tr}(\alpha) & (\alpha, \beta) \mapsto \langle \alpha, \beta \rangle = \text{Tr}(\alpha\beta) \end{array}$$

respectively. Recall that the trace is given by considering multiplication by α as a \mathbb{Q} -linear map $k \rightarrow K$ and using the formula

$$\det(xI - \alpha) = x^n - \text{Tr}(\alpha)x^{n-1} + \cdots + (-1)^n \text{N}(\alpha).$$

The fact that $\text{Tr}(\alpha + \beta) = \text{Tr}(\alpha) + \text{Tr}(\beta)$ implies that $\langle \cdot, \cdot \rangle$ is a symmetric, bilinear form on k . Furthermore, it is nondegenerate since $\langle \alpha, \alpha^{-1} \rangle = \text{Tr}(1) = \text{deg}(k) \neq 0$. We need the following.

Lemma 9. *The image of A under the trace map is contained in \mathbb{Z} .*

Before we prove the lemma, we use it to complete the proof of the theorem. Consider the dual lattice of L with respect to this bilinear form: $L^* = \{\alpha \in k : \text{Tr}(\alpha L) \subseteq \mathbb{Z}\}$. For every $\alpha \in A$, the fact that $L \subseteq A$ implies that $\alpha L \subseteq \alpha A \subseteq A$. Therefore, the lemma implies that $\alpha \in L^*$. Thus, $L \subseteq A \subseteq L^*$. Since the index $(L^* : L)$ is finite, we see that the index $(L^* : A)$ is also finite, which implies that A is a free abelian group of rank equal to the rank of L^* . That is, A is a lattice. \square

Proof of Lemma 9. It suffices to show that all the coefficients of the polynomial $f_\alpha(x) = \det(xI - \alpha)$ are integers when $\alpha \in A \subseteq \overline{\mathbb{Z}}$. To see this, let $m = (\mathbb{Q}(\alpha) : \mathbb{Q})$ and let $\ell = (k : \mathbb{Q}(\alpha))$, so that $n = m\ell$. Then a basis for $\mathbb{Q}(\alpha)$ over \mathbb{Q} is exactly $1, \alpha, \alpha^2, \dots, \alpha^{m-1}$. Let $g_\alpha(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$ denote the minimal polynomial of α over \mathbb{Q} .

Let $\beta_1, \dots, \beta_\ell$ be a basis for k over $\mathbb{Q}(\alpha)$. Then $\{\alpha^i \beta_j : 1 \leq j \leq \ell, 0 \leq i \leq m-1\}$ forms a basis for k over \mathbb{Q} . We wish to find the matrix representing left multiplication by α with respect to this basis. Let T be the following $m \times m$ matrix:

$$T = \begin{pmatrix} 0 & 0 & 0 & \cdots & -a_0 \\ 1 & 0 & 0 & \cdots & -a_1 \\ 0 & 1 & 0 & \cdots & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -a_{m-1} \end{pmatrix}$$

The matrix for $xI - \alpha$ is then given in block form:

$$\begin{pmatrix} xI - T & 0 & \cdots & 0 \\ 0 & xI - T & \cdots & 0 \\ \vdots & \vdots & \ddots & \cdots \\ 0 & 0 & \cdots & xI - T \end{pmatrix}$$

It follows that $f_\alpha(x) = (g_\alpha(x))^\ell$. Thus, it suffices to show that for $\alpha \in A$, the coefficients of the minimal polynomial of α are in \mathbb{Z} .

Over \mathbb{C} , we may factor $g_\alpha(x)$ as $g_\alpha(x) = \prod_{i=1}^m (x - \alpha_i)$. We then have a commuting diagram of \mathbb{Q} -isomorphisms of fields:

$$\begin{array}{ccc}
 \mathbb{Q}(\alpha) & \xleftarrow{\cong} & \mathbb{Q}[x]/(g_\alpha(x)) \\
 \cong \downarrow & \begin{array}{c} \alpha \longleftarrow x \\ \downarrow \quad \downarrow \\ \alpha_i \longleftarrow x \end{array} & \downarrow = \\
 \mathbb{Q}(\alpha_i) & \xleftarrow{\cong} & \mathbb{Q}[x]/(g_\alpha(x))
 \end{array}$$

Since $\mathbb{Q}(\alpha_i) \cong \mathbb{Q}(\alpha)$ and these are finite extensions of \mathbb{Q} , Proposition 5 implies that the α_i are algebraic integers. Corollary 6 implies that the symmetric functions in the α_i are algebraic integers. Since these are the coefficients of $g_\alpha(x)$, they are also in \mathbb{Q} , and it follows that they are in $\mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$. \square

Definition. We define the *discriminant* of k to be the discriminant of the lattice A in k with respect to the bilinear form $\langle \alpha, \beta \rangle = \text{Tr}(\alpha\beta)$. That is, if $\alpha_1, \dots, \alpha_n$ forms a basis of A over \mathbb{Z} , then $\text{disc}(k) = \text{disc}(A) = \det(\text{Tr}(\alpha_i\alpha_j))$. Since $\text{Tr}(A) \subseteq \mathbb{Z}$, this matrix has integer entries and $\text{disc}(k) \in \mathbb{Z}$.

Example. If $k = \mathbb{Q}$, then $A = \mathbb{Z} = A^*$ and $\text{disc}(\mathbb{Q}) = 1$. Next lecture, we shall prove the following theorem, due to Minkowski. The proof involves the “geometry of numbers”.

Theorem. If $\text{disc}(A) = \pm 1$, then $k = \mathbb{Q}$.

Proposition 10. Let $k \supseteq \mathbb{Q}$ be a number field with ring of algebraic integers A , and let $d = \text{disc}(A)$. Then $d \equiv 0, 1 \pmod{4}$. Equivalently, $d \equiv a^2 \pmod{4}$ for some integer a .

Proof. Since the extension $\mathbb{Q} \subseteq k$ is finite and separable, there are $n = (k : \mathbb{Q})$ distinct \mathbb{Q} -embeddings $\sigma_1, \dots, \sigma_n$ of k into \mathbb{C} . Then $\text{Tr}(\alpha) = \sum_{\ell=1}^n \sigma_\ell(\alpha)$ for all $\alpha \in k$. Let $\alpha_1, \dots, \alpha_n \in A$ form a basis of A over \mathbb{Z} . It follows that $\text{Tr}(\alpha_i\alpha_j) = \sum_{\ell=1}^n \sigma_\ell(\alpha_i\alpha_j) = \sum_{\ell=1}^n \sigma_\ell(\alpha_i)\sigma_\ell(\alpha_j)$. Let $B = (\sigma_\ell(\alpha_i))$, which is an $n \times n$ matrix with entries in $\overline{\mathbb{Z}}$. In particular, $\det(B) \in \overline{\mathbb{Z}}$. Then $d = \det(\text{Tr}(\alpha_i\alpha_j)) = \det(B^t B) = \det(B)^2$. Expanding $\det(B)$ using the formula for $\text{Tr}(\alpha_i)$ we have

$$\det(B) = \sum_{\pi \in S_n} \text{sign}(\pi) \prod_{\ell=1}^n \sigma_\ell(\alpha_{\pi(\ell)}) = \sum_{\pi \in A_n} \prod_{\ell=1}^n \sigma_\ell(\alpha_{\pi(\ell)}) - \sum_{\pi \notin A_n} \prod_{\ell=1}^n \sigma_\ell(\alpha_{\pi(\ell)}) = x - y$$

where $x = \sum_{\pi \in A_n} \prod_{\ell=1}^n \sigma_\ell(\alpha_{\pi(\ell)})$ and $y = \sum_{\pi \notin A_n} \prod_{\ell=1}^n \sigma_\ell(\alpha_{\pi(\ell)})$. Since each α_i is an algebraic integer, it follows that each $\sigma_\ell(\alpha_{\pi(\ell)})$ satisfies the same monic polynomial as $\alpha_{\pi(\ell)}$ and is therefore an algebraic integer. Thus, x and y are both algebraic integers, as are the elements $x + y$ and xy . For any \mathbb{Q} -automorphism τ of \mathbb{C} , τ permutes the zeroes of any given polynomial with integer coefficients. In particular, for any fixed $\pi \in S_n$, τ permutes the set $\{\sigma_\ell(\alpha_{\pi(\ell)})\}_{\ell=1}^n$. It follows that τ simply rearranges the terms and factors of $x + y$ and xy , so that $\tau(x + y) = x + y$ and $\tau(xy) = xy$. By taking a finite Galois extension K of \mathbb{Q} in \mathbb{C} which contains $x + y$ and xy , we see that these elements are in the fixed field of the Galois group of K over \mathbb{Q} . That is, $x + y, xy \in \mathbb{Q}$. Since these elements are also in $\overline{\mathbb{Z}}$, we see that they are integers. Finally, this shows that

$$d = (\det(B))^2 = (x - y)^2 = (x + y)^2 - 4xy$$

which is of the form $d = (\text{integer})^2 - 4(\text{integer})$. Thus, $d \equiv a^2 \pmod{4}$ for some integer a , as desired. \square

Example. We apply the proposition to the case of quadratic fields. Let k be an extension of \mathbb{Q} of degree 2. The Theorem of the Primitive Element implies that $k = \mathbb{Q}(\alpha)$ for some $\alpha \in k$. Let $x^2 - bx + c$ be the minimal polynomial of α , and let $\beta = \alpha - \frac{b}{2}$. Then $\beta \in k \setminus \mathbb{Q}$ implies that $k = \mathbb{Q}(\beta)$. Furthermore, $\beta^2 = (\alpha - \frac{b}{2})^2 = \alpha^2 - b\alpha + \frac{b^2}{4} = \frac{b^2}{4} - c$. That is, β satisfies a polynomial of the form $x^2 - D$. By replacing β by a rational multiple of β (after replacing α by β) we may assume that the minimal polynomial of α is $x^2 - D$ where D is a square-free integer. It follows that $k \cong \mathbb{Q}[x]/(x^2 - D)$. Let A denote the ring of algebraic integers in k and let L denote the lattice $L = \mathbb{Z} + \mathbb{Z}\alpha$. Since $\alpha \in A$, it follows that $L \subseteq A$, and since these are both lattices in k , the index $N = (A : L)$ is finite. By Lemma 2, $d = \text{disc}(A) = \text{disc}(L)/N^2$. To compute $\text{disc}(L)$, we let $\alpha_1 = 1$ and $\alpha_2 = \alpha$, and compute: $\text{Tr}(1) = (k : \mathbb{Q}) = 2$; $\text{Tr}(\alpha) = 0$ since the trace is the coefficient of x in the minimal polynomial $x^2 - D$ of α ; and $\text{Tr}(\alpha^2)$ is the sum of the two conjugates of $\alpha^2 = D$ which is $2D$ since $D \in \mathbb{Z}$. Thus,

$$\text{disc}(L) = \det(\text{Tr}(\alpha_i \alpha_j)) = \det \begin{pmatrix} 2 & 0 \\ 0 & 2D \end{pmatrix} = 4D$$

and $d = 4D/N^2$, which is an integer.

There are two possibilities since D is square-free and $4D$ is divisible by N^2 . (1) If $N = 1$ then $L = A$, which implies that $d = 4D \equiv 0 \pmod{4}$. (2) If $N = 2$ then L has index 2 in A and $d = 4D/N^2 = 4D/4 = D$ and the following argument shows that $D \equiv 1 \pmod{4}$. We write $\alpha = \sqrt{D}$ and note that since A/L has order 2, $2A \subseteq L$ which implies that $A \subseteq \frac{1}{2}L = \mathbb{Z}\frac{1}{2} + \mathbb{Z}\frac{1}{2}\sqrt{D}$. We wish to know exactly when an element of $\frac{1}{2}L$ is in $A \setminus L$. Let $\beta = \frac{1}{2}(a + b\sqrt{D})$ be such an element. Then a and b are not both even. Since $\beta \in A$, the proof of Lemma 9 shows that $\mathbb{N}(\beta) \in \mathbb{Z}$. Direct computation shows that $\mathbb{N}(\beta) = \frac{1}{4}(a^2 - b^2D) \in \mathbb{Z}$, which implies that $a^2 - b^2D \in 4\mathbb{Z}$. That is, $a^2 \equiv b^2D \pmod{4}$. If b were even, then this would imply that a is also even, a contradiction. Thus, b is odd, and $b^2 \equiv 1 \pmod{4}$. It follows that $a^2 \equiv D \pmod{4}$, so that if a were even, then D would be divisible by 4, contradicting the fact that D is square-free. Thus, $a^2 \equiv 1 \pmod{4}$, which implies that $D \equiv 1 \pmod{4}$. It also follows that $A = \mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{d}}{2}) = \mathbb{Z} + \mathbb{Z}(\frac{d+\sqrt{d}}{2})$.

Thus, we have proved the following.

Theorem 11. *The discriminants of quadratic fields are exactly the integers $d \equiv 0, 1 \pmod{4}$, $d \neq 1$ which are as square free as possible. That is, the only square factor of d permitted is 4, and this occurs if and only if $\frac{d}{4} \not\equiv 0, 1 \pmod{4}$.*

It follows that the possible values for d are

$$\begin{array}{ll} d > 0 & d = 5, 8, 12, 13, 17, 20, 21, \dots \\ d < 0 & d = -3, -4, -7, -8, -11, -15, -17, \dots \end{array}$$

The first list corresponds to real quadratic fields since $k = \mathbb{Q}(\sqrt{D})$ and $D = d > 0$ or $D = d/4 > 0$. The second list corresponds to imaginary quadratic fields.

Now we are in the position to completely describe the ring of integers for a quadratic field. If $d \equiv 0 \pmod{4}$, then $A = L = \mathbb{Z} + \mathbb{Z}\sqrt{D}$. In this case, $D = d/4$ so that $A = \mathbb{Z} + \mathbb{Z}\frac{\sqrt{d}}{2} =$

$\mathbb{Z} + \mathbb{Z}\left(\frac{d+\sqrt{d}}{2}\right)$. If $d \equiv 1 \pmod{4}$, then $A = \mathbb{Z} + \mathbb{Z}\left(\frac{d+\sqrt{d}}{2}\right)$, from the above work. Therefore, we have proved the following.

Theorem 12. *The ring of algebraic integers of a quadratic field k is always*

$$A = \mathbb{Z} + \mathbb{Z}\left(\frac{d + \sqrt{d}}{2}\right)$$

where $d = \text{disc}(k)$.

Lecture 3

Example. We continue with the example of quadratic fields. If $d = -4$, then with the previous notation, $D = -1$, and the ring of algebraic integers is the ring of Gaussian integers $A = \mathbb{Z} + \mathbb{Z}i \subset \mathbb{C} = \mathbb{R} + \mathbb{R}i$. Furthermore, $A^\times = \{i^n\}$ which is cyclic of order 4.

If $d = -3$, then $A = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{-3}}{2}\right)$ is the ring of Eisenstein integers. If we let $\zeta = \frac{1+\sqrt{-3}}{2}$, then

$$\text{Tr}(\zeta) = \frac{1 + \sqrt{-3}}{2} + \frac{1 - \sqrt{-3}}{2} = 1$$

and

$$\mathbb{N}(\zeta) = \left(\frac{1 + \sqrt{-3}}{2}\right)\left(\frac{1 - \sqrt{-3}}{2}\right) = \frac{1 + 3}{4} = 1.$$

It follows that $\zeta^2 - \zeta + 1 = 0$. Furthermore,

$$\zeta^3 = \frac{1 + 3\sqrt{-3} - 9 + (-3\sqrt{-3})}{8} = -1$$

so that ζ is a primitive sixth root of unity. Since $\zeta^2 = \frac{-1+\sqrt{-3}}{2}$, we see that $A = \mathbb{Z} + \mathbb{Z}\zeta = \mathbb{Z} + \mathbb{Z}\zeta^2$, and $A^\times = \{\zeta^n\}$ is cyclic of order 6. One point of interest here is that the point $(\zeta, \zeta^{-1}) \in \mathbb{C}^2$ is in the intersection of each Fermat curve $x^p + y^p = 1$ for primes $p > 3$.

If $d = 5$, then $A = \mathbb{Z} + \mathbb{Z}\epsilon$, where $\epsilon = \frac{1+\sqrt{5}}{2}$. Let $\epsilon' = \frac{1-\sqrt{5}}{2}$. Then $\epsilon\epsilon' = -1$ so that $\epsilon^{-1} = -\epsilon' \in A$. It follows that $A^\times = \{\pm 1\} \times \{\epsilon^{\mathbb{Z}}\}$.

Definition. If k is a number field, then an *order* in k is a subring $B \subseteq k$ of rank $n = (k : \mathbb{Q})$ as a free \mathbb{Z} -module.

An order B in k is always contained in the ring of algebraic integers with finite index. Since B is a lattice, it suffices to show that $B \subseteq A$. For $b \in B$, the fact that B is a ring implies that the \mathbb{Z} -linear map given by multiplication by b maps $B \rightarrow B$. Fixing a basis for B over \mathbb{Z} , this map is given by an $n \times n$ matrix with integer entries which we also denote b . Then b satisfies the polynomial $f_b(x) = \det(xI - b)$ which is monic with integer coefficients. Thus, $b \in A$. If $f = (A : B)$, then Lemma 2 implies that $\text{disc}(B) = f^2 \text{disc}(A)$.

Proposition 13. *Assume that k is a quadratic field and f is a positive integer. Then there is a unique order $B = \mathbb{Z} + fA$ of index f in A , the ring of integers.*

Proof. It is clear that $B = \mathbb{Z} + fA$ is a ring. Furthermore, if $d = \text{disc}(A)$, then $B = \mathbb{Z} + fA = \mathbb{Z} + f\mathbb{Z}\left(\frac{d+\sqrt{d}}{2}\right)$ is a lattice. Thus, B is an order, and this formulation shows that B has index f in A . Let B' be any order in k with index f in A . Then f annihilates A/B' so that $fA \subseteq B' \subseteq A$. Since B' is a ring, $\mathbb{Z} \subseteq B'$ so that $B \subseteq B' \subseteq A$. Since B and B' both have index f in A , they must be equal. \square

If $d = \text{disc}(A)$ and $d_B = \text{disc}(B)$, then $d_B = f^2d \equiv 0, 1 \pmod{4}$. It follows that

$$B = \mathbb{Z} + f\mathbb{Z}\left(\frac{d+\sqrt{d}}{2}\right) = \mathbb{Z} + \mathbb{Z}\left(\frac{f^2d+f\sqrt{d}}{2}\right) = \mathbb{Z} + \mathbb{Z}\left(\frac{d_B+\sqrt{d_B}}{2}\right).$$

Example. If $d = -3$, then $A = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{-3}}{2}\right)$. The unique order given by $f = 2$ is $B = \mathbb{Z} + 2A = \mathbb{Z} + \mathbb{Z}\sqrt{-3}$, and $B^\times = \{\pm 1\}$.

If $d = -4$, then $A = \mathbb{Z} + \mathbb{Z}i$. In this case, the order of index 2 is $B = \mathbb{Z} + \mathbb{Z}2i$. Again $B^\times = \{\pm 1\}$.

We note that there is a correspondence between orders B in a quadratic field k and binary quadratic forms. If $q(x, y) = ax^2 + bxy + cy^2$ for integers a, b, c then the discriminant of q is $\text{disc}(q) = b^2 - 4ac$. If M is a free \mathbb{Z} -module of rank 2, then choosing a basis e_1, e_2 of M induces a map $q : M \rightarrow \mathbb{Z}$ given by $q(xe_1 + ye_2) = q(x, y)$. We can use q to induce a symmetric bilinear form $[\cdot, \cdot] : M \times M \rightarrow \mathbb{Z}$ by defining $[m, n] = q(m+n) - q(m) - q(n)$. It is straightforward to verify that this operation is symmetric and bilinear. What we notice, however, is that this form is even since $[m, m] = q(2m) - 2q(m) = 4q(m) - 2q(m) = 2q(m)$. If we compare this to the bilinear form $\langle \alpha, \beta \rangle = \text{Tr}(\alpha\beta)$ on $B \subseteq k$, we see that it is not always even, even when $d \equiv 1 \pmod{4}$. For example, when $d = 5$, we have $\epsilon = \frac{1+\sqrt{5}}{2}$ and $\langle \epsilon, \epsilon \rangle = \text{Tr}(\epsilon^2) = \text{Tr}\left(\frac{3+\sqrt{5}}{2}\right) = 3$. From this we see that we should devise an alternate bilinear form on k .

From our notes before, we know that there is a square-free integer D such that $k \cong \mathbb{Q}(\sqrt{D})$. Quadratic extensions are always Galois, and the nontrivial \mathbb{Q} -automorphism of k is given by $\sigma(\sqrt{D}) = -\sqrt{D}$. We define a new bilinear form $\{ \cdot, \cdot \}$ on k by the formula $\{x, y\} = \text{Tr}(x\sigma(y))$. Since $\text{Tr}(x) = x + \sigma(x)$, it is straightforward to verify that this form is symmetric and bilinear. If we restrict to $B \times B$, the form takes its values in \mathbb{Z} since $B \subseteq A$ and $\sigma(A) = A$. Furthermore, for $x \in B$, $\{x, x\} = \text{Tr}(x\sigma(x)) = 2\mathbb{N}(x) \in 2\mathbb{Z}$. B is a free \mathbb{Z} -module of rank 2, and we define $q : B \rightarrow \mathbb{Z}$ by $x \mapsto \frac{1}{2}\{x, x\}$. With the correct basis, this is a binary quadratic form. Let $d_B = \text{disc}(B)$ and $\alpha = \frac{d_B+\sqrt{d_B}}{2}$, so that $1, \alpha$ forms a basis of B over \mathbb{Z} . Then

$$\begin{aligned} q(x, y) &= \frac{1}{2}\{x + y\alpha, x + y\alpha\} = \mathbb{N}(x + y\alpha) \\ &= \left(x + y\left(\frac{d_B + \sqrt{d_B}}{2}\right)\right)\left(x + y\left(\frac{d_B - \sqrt{d_B}}{2}\right)\right) \\ &= x^2 + d_Bxy + \frac{d_B^2 - d_B}{4}y^2 \end{aligned}$$

The coefficients 1 and d_B are clearly integers, and since $d_B \equiv 0, 1 \pmod{4}$ we see that $\frac{d_B^2 - d_B}{4}$ is also an integer. Furthermore, $\text{disc}(q) = d_B^2 - (d_B^2 - d_B) = d_B = \text{disc}(B)$. It is important to note that frequently there are many quadratic forms of discriminant d_B other than the ones coming from this construction.

Example. Let $d = -15$ and consider the quadratic forms $q_1(x, y) = x^2 - 15xy + 60y^2$ and $q_2(x, y) = 2x^2 + xy + 2y^2$, which both have discriminant -15 . These forms are not equivalent under any change of basis. To see this we notice that the first form comes from our construction. If these were equivalent, then A would have an element of norm 2 since $\mathbb{N}(e_1) = q_2(1, 0) = 2$. This is impossible, though, since if $2 = \mathbb{N}\left(\frac{a+b\sqrt{-15}}{2}\right) = \frac{a^2+15b^2}{4}$ then $a^2 + 15b^2 = 8$ which is impossible for integers a and b . It turns out that there is an ideal $I \subset A$ of index 2 which leads to q_2 .

Now, we discuss the “geometry of numbers” which will help us find estimates of d from the degree n of k . It will also give an elegant proof of the theorem of Minkowski from last lecture. We have a chain of containments $A \subset k \subset k \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^n$ so we may view A as a discrete, co-compact subspace of Euclidean space. Let $k = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/f_{\alpha}(x)$ where f_{α} is the minimal polynomial of α over \mathbb{Q} . By definition, f_{α} is irreducible over \mathbb{Q} , but over \mathbb{R} it splits into a product $f_{\alpha}(x) = \prod_i g_i(x)$ of distinct irreducible factors of degree 1 or 2. (The factors are distinct by separability.) If r_1 is the numbers of real zeroes of f_{α} and r_2 is the number of conjugate pairs of complex zeroes, then $r_1 + 2r_2 = n$ and the Chinese Remainder Theorem implies that

$$k \otimes \mathbb{R} = \mathbb{R}[x]/f_{\alpha}(x) = \mathbb{R}[x]/\prod_i g_i(x) = \prod_i \mathbb{R}[x]/g_i(x) = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

As a side note, another method for obtaining r_1 and r_2 is to consider the nondegenerate bilinear form $\langle x, y \rangle = \text{Tr}(xy)$ on $k \otimes \mathbb{R}$ and to observe that this form has signature $(r_1 + r_2, r_2)$.

Example. For the quadratic fields $k = \mathbb{Q}(\sqrt{D})$ where D is square-free, we see that

$$k \otimes \mathbb{R} = \begin{cases} \mathbb{R} \times \mathbb{R} & \text{if } D > 0 \\ \mathbb{C} & \text{if } D < 0 \end{cases}$$

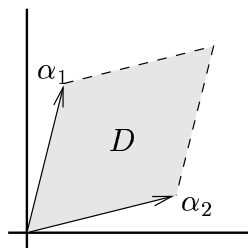
because if $D > 0$ then $f_{\alpha}(x) = x^2 - D$, and if $D < 0$ then $f_{\alpha}(x) = x^2 + D$. This is a specific case of the general fact that r_1 is the number of distinct real embeddings of a general number field k , and r_2 is the number of distinct conjugate pairs of complex embeddings.

We also observe that $k \otimes \mathbb{C} \cong \mathbb{C}^n$. Let $\sigma_1, \dots, \sigma_n$ be the distinct n embeddings of k into \mathbb{C} . Then the isomorphism $k \otimes \mathbb{C} \rightarrow \mathbb{C}^n$ is given by $\alpha \otimes 1 \mapsto (\sigma_1(\alpha), \dots, \sigma_n(\alpha))$.

Let $L \subset k$ be any lattice in k . The fundamental domain for L acting on \mathbb{R}^n is

$$D = \left\{ \sum_{i=1}^n x_i \alpha_i : 0 \leq x_i < 1 \right\}$$

as in the figure.



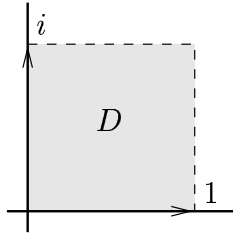
Proposition 14. $\text{disc}(L) = (-4)^{r_2} (\text{vol}(D))^2$.

Corollary 15. *The sign of $\text{disc}(L)$ is $(-1)^{r_2}$.*

Proof. If $r_2 = 0$, then all of the embeddings $\sigma_1, \dots, \sigma_n$ of k are real. Let $\alpha_1, \dots, \alpha_n$ be a basis of L . The coordinates of α_i in the standard orthonormal basis of \mathbb{R}^n are $(\sigma_1(\alpha_i), \dots, \sigma_n(\alpha_i))$ and $\text{vol}(D) = |\det(\sigma_i(\alpha_j))|$. If $B = (\sigma_i(\alpha_j))$ then we already observed that $\text{disc}(L) = \det(B^t B) = (\det(B))^2 = (\text{vol}(D))^2$, as desired.

If $r_2 \neq 0$, then each conjugate pair of complex embeddings contributes a factor of $dz \wedge d\bar{z} = -2idx \wedge dy$. Thus, each such pair contributes a factor of $(-2i)^2 = -4$, for a total contribution of $(-4)^{r_2}$. For more details, the interested reader should consult the book *Théorie algébrique des nombres* by Samuel. \square

Example. Consider the Gaussian integers $A = \mathbb{Z}[i] \subset k \otimes \mathbb{R} = \mathbb{C} = \mathbb{R} + \mathbb{R}i$. The fundamental domain of A



has volume 1, and $\text{disc}(A) = -4$.

Definition. A subset P of Euclidean space is *centrally symmetric* if for each point x of P , $-x$ is also a point of P .

Theorem 16. *Suppose that L is a lattice in \mathbb{R}^n with fundamental domain D , P is a closed, bounded, convex, centrally symmetric subset of \mathbb{R}^n and $\text{vol}(P) \geq 2^n \text{vol}(D)$. Then P contains a nonzero point of L .*

Proof. We will prove the theorem in the case $\text{vol}(P) > 2^n \text{vol}(D)$. A simple limiting argument gives the general case since P is closed and L is discrete.

If we let $\frac{1}{2}P = \{\frac{1}{2}x : x \in P\}$ then the condition $\text{vol}(P) > 2^n \text{vol}(D)$ is equivalent to the condition $\text{vol}(\frac{1}{2}P) > \text{vol}(D)$. We claim that there are distinct points $x, y \in \frac{1}{2}P$ such that $x - y \in L$. This will establish the theorem since it follows that $x = \frac{1}{2}p$ and $y = -\frac{1}{2}q$ for some points $p, q \in P$ (by central symmetry). Then $0 \neq x - y = \frac{1}{2}p + \frac{1}{2}q \in P$ by convexity, and $x - y$ is the desired point.

We give an intuitive argument to see that such x and y exist. The interested reader can find the details in Samuel. We can translate pieces of $\frac{1}{2}P \bmod L$ to fill up D , like cutting up a round carpet to cover the floor of a square room. Since $\text{vol}(P) > 2^n \text{vol}(D)$, it follows that some point of D is double-covered in this process. That is, there are distinct points x, y of $\frac{1}{2}P$ whose images via some translation by a vector of L are the same., So, $x \equiv y \pmod{L}$, as desired. \square

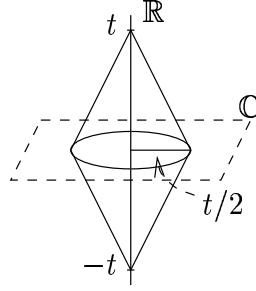
Theorem 17. *If L is any lattice in k , then there exists a nonzero element α of L such that*

$$|\mathbb{N}(\alpha)| \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} |\text{disc}(L)|^{1/2}.$$

Proof. For $t > 0$, let P_t be the following region in $\mathbb{R}^n \cong k \otimes \mathbb{R}$:

$$P_t = \left\{ \alpha \in k \otimes \mathbb{R} : \sum_{i=1}^n |\sigma_i(\alpha)| \leq t \right\}$$

As the sketch suggests



the volume of P_t is

$$\text{vol}(P_t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!} \quad (1)$$

which can be verified directly by integration. Choose t so that $\text{vol}(P_t) = 2^n \text{vol}(D)$. By Proposition 14,

$$\text{vol}(P_t) = 2^n \text{vol}(D) = \frac{2^{(r_1+2r_2)} |\text{disc}(L)|^{1/2}}{2^{r_2}} = 2^{(r_1+r_2)} |\text{disc}(L)|^{1/2} \quad (2)$$

Then P_t satisfies the hypotheses of Theorem 16, and we may fix $\alpha \in (L \setminus \{0\}) \cap P_t$. Then

$$|\mathbb{N}(\alpha)|^{1/n} = \underbrace{\left(\prod_{i=1}^n |\sigma_i(\alpha)|\right)^{1/n}}_{\text{geometric mean}} \leq \underbrace{\frac{1}{n} \sum_{i=1}^n |\sigma_i(\alpha)|}_{\text{arithmetic mean}} \leq \frac{t}{n} \quad (3)$$

which implies that $|\mathbb{N}(\alpha)| \leq \frac{t^n}{n^n}$. From equations (1), (2) and (3) it follows that

$$|\mathbb{N}(\alpha)| \leq \frac{t^n}{n^n} = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} |\text{disc}(L)|^{1/2}$$

as desired. □

Corollary 18. *If A is the ring of algebraic integers in a number field k , then*

$$|\text{disc}(A)|^{1/2} \geq \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^{r_2}.$$

Proof. Every $\alpha \in A \setminus \{0\}$ has $|\mathbb{N}(\alpha)| \geq 1$, so the theorem implies that for some such α ,

$$1 \leq |\mathbb{N}(\alpha)| \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} |\text{disc}(A)|^{1/2}$$

from which the result is immediate. \square

Corollary 19. (Minkowski) *If $\text{disc}(A) = \pm 1$, then $A = \mathbb{Z}$ and $k = \mathbb{Q}$.*

Proof. The function of n :

$$\frac{n^{2n}}{(n!)^2} \left(\frac{\pi}{4}\right)^{2n} \leq \frac{n^{2n}}{(n!)^2} \left(\frac{\pi}{4}\right)^{2r_2} \leq |\text{disc}(A)| = 1$$

is monotone increasing, and for $n = 2$

$$\frac{n^{2n}}{(n!)^2} \left(\frac{\pi}{4}\right)^{2n} > 1.$$

It follows that $n = 1$. \square

Lecture 4

Let k be a number field with ring of algebraic integers A , and let $d = \text{disc}(A)$. We now use the geometry of numbers to give a bound on d in terms of $n = (\mathbb{Q} : k)$. By Corollary 18

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

By Stirling's formula, $n! = \Gamma(n+1)$, so there exists θ in the interval $(0, 1)$ such that

$$n! = \sqrt{2\pi n} n^n e^{-(n+\frac{\theta}{12n})}$$

and it follows that

$$|d|^{1/2} \geq \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^{r_2} = \frac{e^{(n-\frac{\theta}{12n})}}{\sqrt{2\pi n}} \left(\frac{\pi}{4}\right)^{r_2}.$$

Raising both sides to the $2/n$ power, we find that

$$|d|^{1/n} \geq e^2 \left(\frac{\pi}{4}\right)^{2r_2/n} \left(\frac{e^{(-\frac{\theta}{6n^2})}}{\sqrt[n]{2\pi n}}\right).$$

We can write $e^2 = (e^2)^{n/n} = (e^2)^{(\frac{r_1}{n} + \frac{2r_2}{n})}$ so that

$$|d|^{1/n} \geq (e^2)^{r_1/n} \left(e^2 \frac{\pi}{4}\right)^{2r_2/n} \left(\frac{e^{(-\frac{\theta}{6n^2})}}{\sqrt[n]{2\pi n}}\right).$$

The factor $\left(\frac{e^{(-\frac{\theta}{6n^2})}}{\sqrt[n]{2\pi n}}\right) \rightarrow 1$ as $n \rightarrow \infty$ so that

$$|d|^{1/n} \gtrsim_{n \rightarrow \infty} (7.3)^{r_1/n} (5.8)^{2r_2/n}$$

Example. If $n = 2r_2$ (the case when k is totally complex) then asymptotically $|d|^{1/n} \geq 5.8$ so that $|d| \geq (5.8)^n$. This inequality actually holds for $n \geq 10^8$.

Stark-Odlyzko have given the following improvement on the bound. Assuming the Riemann Hypothesis for the zeta function of k :

$$|d|^{1/n} \geq (215)^{r_1/n} (44)^{2r_2/n}.$$

In the totally complex case $n = 2r_2$, this gives the bound $|d| \geq (44)^n$.

Now we consider the arithmetic properties of the ring of integers A of a number field k . It is a fact that A is a Dedekind domain, i.e., a smooth ring of dimension 1. In particular, every ideal I in A is a product of prime ideals. However, if we take an arbitrary order B in k , then B will generally not be a Dedekind domain. Among other things, we want to know what keeps B from being a Dedekind domain.

We note that there are standard methods of constructing new Dedekind domains from old ones. If A_0 is a Dedekind domain, with field of quotients $k_0 \supset A_0$ and k is a finite separable extension of k_0 , then we let A be the integral closure of A_0 in k . It follows that A is a Dedekind domain, as well.

Given two lattices L and M in k , we have ways of combining L and M to get other lattices in k . (We will apply these constructions mostly to ideals of an order B , but they are valid in this more general context.) The intersection $L \cap M$ is a lattice in k since there is a nonzero rational number α such that $\alpha L \subseteq M$. This implies that there are nonzero integers a, b such that $aL \subseteq bM$, and it follows that for all $x \in L$, $ax \in aL \cap bM \subseteq L \cap M$. That is, $L/(L \cap M)$ is torsion and finitely generated, so that $L \cap M$ has finite index in L . The sum $L + M$ is also a lattice because the same argument as above shows that $a(L + M) \subseteq M$ so that $(L + M)/M$ is also finitely generated and torsion. The product

$$L \cdot M = \left\{ \sum_i \ell_i m_i : \ell_i \in L, m_i \in M \right\}$$

is a lattice because if m_1, \dots, m_n is a basis for M then $L \cdot M = Lm_1 + \dots + Lm_n$ is a finite sum of lattices. The quotient

$$L/M = \{ \alpha \in k : \alpha M \subseteq L \} = \bigcap_{i=1}^n Lm_i^{-1}$$

is a finite intersection of lattices and therefore a lattice. The quotient lattice should not be confused with the quotient of a group by a subgroup since M is not necessarily contained in L . We call this lattice the quotient and use the fraction notation because the definition implies that $(L/M) \cdot M \subseteq L$, so that in some sense L/M (almost) behaves like an object which we might call $L \cdot M^{-1}$. It is important to note that strict containment may occur here, so this justification is, at best, imprecise. We also note that $L \cdot M = L \otimes_{\mathbb{Z}} M$ and $L/M = \text{hom}_{\mathbb{Z}}(M, L)$. Finally, $L/L = \{ \alpha \in k : \alpha L \subseteq L \} = \text{End}(L)$ is a ring, and therefore an order in k . If we let $B = L/L$, then L is a left B -module in k .

Fix an order B in k and let I be a nonzero ideal of B . Then I is a lattice in k since for a nonzero element $\alpha \in I$, $\alpha B \subseteq I \subseteq B$. αB is a lattice, so it follows that I has finite index in B . Furthermore, by definition, $B \subseteq I/I$.

Lemma 20. *The index $(B : \alpha B) = |\mathbb{N}(\alpha)|$.*

Proof. $(B : \alpha B) = |\det(\alpha : B \rightarrow B)| = |\mathbb{N}(\alpha)|$ by definition. \square

Definition. If I is a nonzero ideal in an order B , then we define the *norm* of I to be the index $\mathbb{N}(I) = (B : I)$.

Definition. If L is any lattice in k (not necessarily contained in B) with $\text{End}(L) \supseteq B$, then we say that L is a *fractional ideal* of B . The condition $\text{End}(L) \supseteq B$ is equivalent to the condition $BL \subseteq L$.

Proposition 21. *An order B in k is a domain of dimension 1, i.e., every nonzero prime ideal $P \subset B$ is maximal.*

Proof. B is a domain since it is a subring of a field. Since P has finite index in B , the ring $k_P = B/P$ is a finite integral domain. For a nonzero element α of k_P the multiplication map $\alpha : k_P \rightarrow k_P$ is therefore injective, and since k_P is finite, the map is also surjective. This implies that k_P is a field since this homomorphism maps onto the identity. Thus, P is maximal. \square

Definition. An ideal I of B is called *principal* if $I = \alpha B$ for some $\alpha \in B$. We notice that a principal ideal $I = \alpha B$ satisfies the condition $\text{End}(I) = B$:

$$\text{End}(I) = \{\beta \in k : \beta \alpha B \subseteq \alpha B\} = \{\beta \in k : \beta B \subseteq B\} = B$$

The last equality follows from two facts: (1) every element of B maps $B \rightarrow B$ since B is a ring, so “ \supseteq ”; and (2) if $\beta \in k$ maps $B \rightarrow B$, then $\beta = \beta(1) \in \beta B \subseteq B$, so “ \subseteq ”.

We claim that non-maximal orders are not principal ideal domains (even though they are all domains of dimension 1). To see this, let $B \subset A$ be an order with index $f = (A : B) > 1$. Then the ideal fA is principal in A and is contained in B (and is an ideal in B since $fA \subset B \subset A$). However, fA is not a principal ideal of B since, if it were, then the above notes would show that $\text{End}(fA) = B$. But $\text{End}(fA) = A \neq B$ so this is not possible.

Example. Here is a case where the ring of integers $A \subset k$ is not a principal ideal domain. Let p be a positive prime in \mathbb{Z} such that $p \equiv 1 \pmod{4}$ and let $k = \mathbb{Q}(\sqrt{-p})$. Then by our work in Lecture 2, $A = \mathbb{Z} + \mathbb{Z}(\sqrt{-p})$ since the discriminant is $d = -4p$ and

$$A = \mathbb{Z} + \mathbb{Z}\left(\frac{-4p + \sqrt{-4p}}{2}\right) = \mathbb{Z} + \mathbb{Z}(-2p + \sqrt{-p}) = \mathbb{Z} + \mathbb{Z}\sqrt{-p}$$

Let $I = \{a + b\sqrt{-p} : a \equiv b \pmod{2}\} \subset A$. I is an ideal of A , as follows. Clearly, I is closed under addition. Take $a + b\sqrt{-p} \in I$ and $\alpha + \beta\sqrt{-p} \in A$. Then

$$(a + b\sqrt{-p})(\alpha + \beta\sqrt{-p}) = (a\alpha - b\beta p) + \sqrt{-p}(a\beta + b\alpha)$$

The relation between a and b says that a and b are either both odd or both even. If a and b are both even, then the product is in $2A \subseteq I$. If they are both odd, then since p is odd, $a\alpha - b\beta p \equiv \alpha + \beta \pmod{2}$ and $a\beta + b\alpha \equiv \alpha + \beta \pmod{2}$, so mod 2 the coefficients of the product are the same and the product is in I . It is straightforward to check (by the definition of I) that the containments $A \subset I$ and $I \subset 2A$ each have index 2. Now, suppose that I were principal, say $I = \alpha A$. Then $\mathbb{N}(\alpha) = (A : \alpha A) = (A : I) = 2$. However, if $\alpha = a + b\sqrt{-p}$, then $2 = \mathbb{N}(\alpha) = a^2 + pb^2$, which can never occur since $p \geq 5$. Thus, I is

not principal. Note that this example encompasses the classical example which states that $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ is not a principal ideal domain.

Next, we want to show that if $P \subset A$ is a nonzero prime ideal, then $P \cdot (A/P) = A$. That is, A/P is a fractional ideal which “inverts P ”.

Proposition 22. *Let B be an order in k and P a nonzero prime in B . Then exactly one of the following holds.*

1. $P \cdot (B/P) = B$, or
2. $P/P = \text{End}(P) \supsetneq B$.

This proposition follows from the following theorem.

Theorem 23. *Let B be an order in k and P a nonzero prime in B . Then $B/P \supsetneq B$.*

Example. If p is a prime in \mathbb{Z} , then $\mathbb{Z}/p\mathbb{Z} = \frac{1}{p}\mathbb{Z} \supsetneq \mathbb{Z}$.

Proof of Proposition 22. We have the following containments in general:

$$P = B \cdot P \subseteq (B/P) \cdot P \subseteq B.$$

If $(B/P) \cdot P = B$, then 1. holds. Otherwise, $(B/P) \cdot P = \subsetneq B$. It is straightforward to show that $(B/P) \cdot P$ is an ideal in B . The maximality of P implies that $P = (B/P) \cdot P$, and the theorem implies that there exists $\gamma \in (B/P) \setminus B$. Then $\gamma P \subseteq (B/P) \cdot P = P$ which implies that $\gamma \in (P/P) \setminus B$, which implies 2. \square

We need a bit more machinery before we can prove the theorem. Let M be a nonzero, simple, finite B -module. Then M is cyclic, say $M = Be$. Let P be the annihilator of M , $P = \text{Ann}(e) \subset B$. Then the map $B/P \rightarrow M$ given by $b \mapsto be$ is an isomorphism of one-dimensional vector spaces over the residue field B/P .

Proposition 24. *Any nonzero ideal I in an order B of k contains a product of prime ideals P_1, \dots, P_t . The primes which occur in this product are exactly the primes which contain I .*

Proof. Since I has finite index in B , we can find a chain of ideals $I = I_0 \subset I_1 \subset I_2 \subset \dots \subset I_t = B$ such that each quotient I_m/I_{m-1} is a simple B -module. By the previous remark, there are prime ideals P_1, \dots, P_t such that $I_m/I_{m-1} \cong B/P_m$. It follows that $P_m I_m \subseteq I_{m-1}$, and therefore, $P_1 \cdots P_t \subseteq I_0 = I$.

To prove the second claim, let $P \supseteq I \subseteq P_1 \cdots P_t$. By maximality, it suffices to show that some $P_i \subseteq P$. Suppose that no P_i is contained in P . Then there are elements $\alpha_i \in P_i \setminus P$, and the product of these elements is in $P_1 \cdots P_t \subseteq I \subseteq P$. However, the product is not in P since P is prime and no factor is in P , yielding a contradiction. \square

We note, in addition, that the norm $\mathbb{N}(I) = \prod_{i=1}^t \mathbb{N}(P_i)$. The chain of ideals $I = I_0 \subset I_1 \subset I_2 \subset \dots \subset I_t = B$ shows us that

$$\mathbb{N}(I) = (B : I) = (I_t : I_{t-1}) \cdots (I_1 : I_0) = (B : P_t) \cdots (B : P_1) = \mathbb{N}(P_t) \cdots \mathbb{N}(P_1)$$

as claimed.

Example. In the notation of the proposition, I may not equal $P_1 \cdots P_t$. Let k be a quadratic field with ring of integers A . By Proposition 13, for a fixed prime p there is a unique order $B = \mathbb{Z} + pA \subset A$ with index $(A : B) = p$. By our notes above, the ideal of A $P = pA \subset B$ is also an ideal in B which is prime and not principal in B . Furthermore, $I = pB \subset pA$. P is the unique prime of B containing I and $P \supsetneq I \supset P^2 = p^2A$, but $I \neq P^2$ since $p \in I \setminus P^2$.

Proof of Theorem 23. It is clear from the definition that $B \subseteq B/P$. To see that equality does not hold, fix a nonzero element α of P and let $I = \alpha B \subseteq P \subset B$. By Proposition 24, there are primes P_1, \dots, P_t such that $I \supseteq PP_1 \cdots P_t$. If $I \supseteq P_1 \cdots P_t$, then $P = P_i$ for some i . Cancel off as many “factors” of P as possible so that we may assume that $P_1 \cdots P_u \not\subseteq I$ and $PP_1 \cdots P_u \subseteq I$. Fix $\beta \in (P_1 \cdots P_u) \setminus I$. Then in k , $\gamma = \beta/\alpha \notin B$ and $\gamma P \subseteq B$ so that $\gamma \in B/P$. \square

Corollary 25. *If P is a prime ideal in the ring of integers A , then $P \cdot (A/P) = A$.*

Proof. By Proposition 22, if $P \cdot (A/P) \neq A$, then $\text{End}(P)$ is a ring in k which properly contains A . But every order in k is contained in A , so this is a contradiction. \square

Theorem 26. (Dedekind) *Let A be the ring of integers in a number field k .*

1. *Every nonzero prime ideal is invertible, in the sense that there is a fractional ideal $P^{-1} \subset k$ such that $PP^{-1} = A$.*
2. *Every ideal is uniquely the product of prime ideals $I = P_1 \cdots P_t$.*
3. *The set Ideal of fractional ideals forms an abelian group, freely generated by the prime ideals of A . The identity element is A , and for any fractional ideal I , $I^{-1} = A/I$. If $I = \prod_P P^{\text{ord}_P(I)}$, then the isomorphism $\text{Ideal} \rightarrow \bigoplus_P \mathbb{Z}$ is given by $I \mapsto (\dots, \text{ord}_P(I), \dots)$.*

Proof. 1. follows from Corollary 25 since A/P is a fractional ideal. We shall prove 3. in the following lecture.

2. As in the proof of Proposition 24, we have ideals I_j and prime ideals P_j such that

$$P_1 \cdots P_t \subseteq I = I_0 \subset I_1 \subset \cdots \subset I_t = B$$

If $t = 1$, then the only prime containing I is P_1 and $P_1 \subseteq I \subseteq P_1$ which implies that $I = P_1$. So, we proceed by induction. The chain $I_1 \subset I_2 \subset \cdots \subset I_t = B$ satisfies the induction hypothesis, so

$$P_2 \cdots P_t = I_1 \supseteq I \supseteq P_1 \cdots P_t = P_1 I_1$$

Multiplying by $P_2^{-1} \cdots P_t^{-1}$ yields

$$A \supseteq IP_2^{-1} \cdots P_t^{-1} \supseteq P_1$$

If $A = IP_2^{-1} \cdots P_t^{-1}$, then multiplying by $P_2 \cdots P_t$ implies that $I = P_2 \cdots P_t$. This implies that A/I has a Jordan-Holder series with $t - 1$ links, a contradiction. Thus,

$A \neq IP_2^{-1} \cdots P_t^{-1}$, and the maximality of P_1 implies that $IP_2^{-1} \cdots P_t^{-1} = P_1$ so that multiplying by $P_1 \cdots P_t$ implies that $I = P_1 \cdots P_t$.

For uniqueness, we write $I = P_1 \cdots P_t = P'_1 \cdots P'_u$. Then $P_1 \supseteq P'_1 \cdots P'_u$ which implies that $P_1 = P'_i$ for some i as in the proof of Proposition 24. Multiply by P_1^{-1} and apply induction. \square