

## 14 The geometry of numbers

### 14.1 Lattices in real vector spaces

Recall that for an integral domain  $A$  with fraction field  $K$ , an  $A$ -lattice in a finite dimensional  $K$ -vector space  $V$  is a finitely generated  $A$ -submodule of  $V$  that contains a  $K$ -basis for  $V$  (see Definition 5.9). We now want to specialize to the case  $A = \mathbb{Z}$ , but rather than working with the fraction field  $K = \mathbb{Q}$  we will instead work with its completion  $\mathbb{R}$  at the unique infinite place of  $\mathbb{Q}$ .

**Remark 14.1.** In this lecture we focus on number fields, but we will make remarks along the way about how to similarly treat global function fields (where one would take  $A = \mathbb{F}_q[t]$  and work with its completion  $\mathbb{F}_q(t)_\infty \simeq \mathbb{F}_q((\frac{1}{t}))$  at the unique infinite place of  $\mathbb{F}_q(t)$ ). You will be able to explore the function field case in more detail on Problem Set 7.

Let  $V$  be an  $\mathbb{R}$ -vector space of dimension  $n$ . Then  $V \simeq \mathbb{R}^n$  is a locally compact group with a Haar measure that is unique up to scaling, by Theorem 13.14.

**Definition 14.2.** A subgroup  $H$  of a topological group  $G$  is *discrete* if the subspace topology on  $H$  is the discrete topology (every point is open), and *cocompact* if  $H$  is a normal subgroup of  $G$  and the quotient  $G/H$  is compact (here  $G/H$  denotes the group  $G/H$  with the quotient topology given by identifying elements of  $G$  that lie in the same coset of  $H$ ).

**Lemma 14.3.** A subgroup  $G \subseteq V \simeq \mathbb{R}^n$  is finitely generated if and only if it is discrete, in which case  $G \simeq \mathbb{Z}^m$  for some  $m \leq n$  and  $G$  is then cocompact if and only if  $m = n$ .

*Proof.* It follows from the structure theorem for finitely generated abelian group that if  $G$  is finitely generated it is a free  $\mathbb{Z}$ -module, since it lies in the torsion free abelian group  $V$ , and the rank of  $G$  must be equal to the dimension  $m \leq n$  of the subspace it spans. A subgroup  $G \simeq \mathbb{Z}^m$  of  $V \simeq \mathbb{R}^n$  is discrete (0 is an isolated point), and cocompact if and only if  $m = n$ .

Let  $v_1, \dots, v_m$  be a basis for the subspace  $W$  of  $V$  spanned by  $G$ , and let  $\Lambda \simeq \mathbb{Z}^m$  be the subgroup of  $G$  generated by this basis. The quotient  $W/\Lambda \simeq \mathbb{R}^m/\mathbb{Z}^m$  is compact (it is isomorphic to the closed unit cube in  $\mathbb{R}^m$ ), so the image of the discrete group  $G$  under the quotient map  $\pi: W \rightarrow W/\Lambda$  must be finite. We can thus choose a finite  $S \subseteq G$  such that  $\pi(S) = \pi(G)$ , and then  $G$  is generated by  $v_1, \dots, v_m$  and  $S$ .  $\square$

**Definition 14.4.** A (full) *lattice* in  $V \simeq \mathbb{R}^n$  is a  $\mathbb{Z}$ -submodule generated by an  $\mathbb{R}$ -basis, equivalently, a discrete cocompact subgroup.

**Remark 14.5.** A discrete subgroup of a Hausdorff topological group is always closed; see [1, III.2.1.5] for a proof. This implies that the quotient of a Hausdorff topological group by a normal discrete subgroup is Hausdorff (which is false for topological spaces in general); see [1, III.2.1.18]. It follows that the quotient of a Hausdorff topological group (including all locally compact groups) by a discrete cocompact subgroup is a compact group. These facts are easy to see in the case of lattices:  $\mathbb{Z}$  is closed in  $\mathbb{R}$  (as the complement of a union of open intervals), so  $\mathbb{Z}^n$  is closed in  $\mathbb{R}^n$ . Given a lattice  $\Lambda$  in  $V$ , each  $\mathbb{Z}$ -basis for  $\Lambda$  determines an isomorphism of topological groups  $\Lambda \simeq \mathbb{Z}^n$  and  $V \simeq \mathbb{R}^n$ , and the quotient  $V/\Lambda \simeq \mathbb{R}^n/\mathbb{Z}^n \simeq (\mathbb{R}/\mathbb{Z})^n$  (an  $n$ -torus), is compact Hausdorff and thus a compact group.

**Remark 14.6.** You might ask why we are using the archimedean completion  $\mathbb{R} = \mathbb{Q}_\infty$  rather than some other completion  $\mathbb{Q}_p$ . The reason is  $\mathbb{Z}$  is not a discrete subgroup of  $\mathbb{Q}_p$  for any finite place  $p$  (elements of  $\mathbb{Z}$  can be arbitrarily close to 0 under the  $p$ -adic metric). Similarly,  $\mathbb{F}_q[t]$  is a discrete subgroup of  $\mathbb{F}_q(t)_\infty$ , but not of any other completion of  $\mathbb{F}_q(t)$ .

Any basis  $v_1, \dots, v_n$  for  $V$  determines a parallelepiped

$$F(v_1, \dots, v_n) := \{t_1 v_1 + \dots + t_n v_n : t_1, \dots, t_n \in [0, 1]\}$$

that we may view as the unit cube by fixing an isomorphism  $\varphi: V \xrightarrow{\sim} \mathbb{R}^n$  that maps  $(v_1, \dots, v_n)$  to the standard basis of unit vectors for  $\mathbb{R}^n$ . It then makes sense to normalize the Haar measure  $\mu$  so that  $\mu(F(v_1, \dots, v_n)) = 1$ , and we then have  $\mu(S) = \mu_{\mathbb{R}^n}(\varphi(S))$  for every measurable set  $S \subseteq V$ , where  $\mu_{\mathbb{R}^n}$  denotes the standard Lebesgue measure on  $\mathbb{R}^n$ .

For any other basis  $e_1, \dots, e_n$  of  $V$ , if we let  $E = [e_{ij}]_{ij}$  be the matrix whose  $j$ th column expresses  $e_j = \sum_i e_{ij} v_i$ , in terms of our normalized basis  $v_1, \dots, v_n$ , then

$$\mu(F(e_1, \dots, e_n)) = |\det E| = \sqrt{\det E^t \det E} = \sqrt{\det(E^t E)} = \sqrt{\det[\langle e_i, e_j \rangle]_{ij}}, \quad (1)$$

where  $\langle e_i, e_j \rangle$  is the canonical inner product (the dot product) on  $\mathbb{R}^n$ . Here we have used the fact that the determinant of a matrix in  $\mathbb{R}^{n \times n}$  is the signed volume of the parallelepiped spanned by its columns (or rows). This is a consequence of the following more general result, which is independent of the choice of basis or the normalization of  $\mu$ .

**Proposition 14.7.** *Let  $T: V \rightarrow V$  be a linear transformation of  $V \simeq \mathbb{R}^n$ . For any Haar measure  $\mu$  on  $V$  and every measurable set  $S \subseteq V$  we have*

$$\mu(T(S)) = |\det T| \mu(S). \quad (2)$$

*Proof.* See [11, Ex. 1.2.21]. □

If  $\Lambda$  is a lattice  $e_1 \mathbb{Z} + \dots + e_n \mathbb{Z}$  in  $V$ , the quotient  $V/\Lambda$  is a compact group that we may identify with the parallelepiped  $F(e_1, \dots, e_n) \subseteq V$ , which forms a set of unique coset representatives. More generally, we make the following definition.

**Definition 14.8.** Let  $\Lambda$  be a lattice in  $V \simeq \mathbb{R}^n$ . A *fundamental domain* for  $\Lambda$  is a measurable set  $F \subseteq V$  such that

$$V = \bigsqcup_{\lambda \in \Lambda} (F + \lambda).$$

In other words,  $F$  is a measurable set of coset representatives for  $V/\Lambda$ . Fundamental domains exist: if  $\Lambda = e_1 \mathbb{Z} + \dots + e_n \mathbb{Z}$  we may take the parallelepiped  $F(e_1, \dots, e_n)$ .

**Proposition 14.9.** *Let  $\Lambda$  be a lattice in  $V \simeq \mathbb{R}^n$  and let  $\mu$  be a Haar measure on  $V$ . Every fundamental domain for  $\Lambda$  has the same measure, and this measure is finite and nonzero.*

*Proof.* Let  $F$  and  $G$  be two fundamental domains for  $\Lambda$ . Using the translation invariance and countable additivity of  $\mu$  (note that  $\Lambda \simeq \mathbb{Z}^n$  is a countable set) along with the fact that  $\Lambda$  is closed under negation, we obtain

$$\begin{aligned} \mu(F) &= \mu(F \cap V) = \mu\left(F \cap \bigsqcup_{\lambda \in \Lambda} (G + \lambda)\right) = \mu\left(\bigsqcup_{\lambda \in \Lambda} (F \cap (G + \lambda))\right) \\ &= \sum_{\lambda \in \Lambda} \mu(F \cap (G + \lambda)) = \sum_{\lambda \in \Lambda} \mu((F - \lambda) \cap G) = \sum_{\lambda \in \Lambda} \mu(G \cap (F + \lambda)) = \mu(G), \end{aligned}$$

where the last equality follows from the first four (swap  $F$  and  $G$ ). If we fix a  $\mathbb{Z}$ -basis  $e_1, \dots, e_n$  for  $\Lambda$ , the parallelepiped  $F(e_1, \dots, e_n)$  is a fundamental domain for  $\Lambda$ , and its

closure is compact, so  $\mu(F(e_1, \dots, e_n))$  is finite, and it is nonzero because there is an isomorphism  $V \simeq \mathbb{R}^n$  that maps the closure of  $F(e_1, \dots, e_n)$  to the unit cube in  $\mathbb{R}^n$  whose Lebesgue measure is nonzero (whether a set has zero measure or not does not depend on the normalization of the Haar measure and is therefore preserved by isomorphisms of locally compact groups).  $\square$

**Definition 14.10.** Let  $\Lambda$  be a lattice in  $V \simeq \mathbb{R}^n$  and fix a Haar measure  $\mu$  on  $V$ . The *covolume*  $\text{covol}(\Lambda) \in \mathbb{R}_{>0}$  of  $\Lambda$  is the measure  $\mu(F)$  of any fundamental domain  $F$  for  $\Lambda$ .

Note that covolumes depend on the normalization of  $\mu$ , but ratios of covolumes do not.

**Proposition 14.11.** If  $\Lambda' \subseteq \Lambda$  are lattices in  $V \simeq \mathbb{R}^n$ , then  $\text{covol}(\Lambda') = [\Lambda : \Lambda'] \text{covol}(\Lambda)$ .

*Proof.* Fix a fundamental domain  $F$  for  $\Lambda$  and a set of coset representatives  $S$  for  $\Lambda/\Lambda'$ . Then

$$F' := \bigsqcup_{\lambda \in S} (F + \lambda)$$

is a fundamental domain for  $\Lambda'$ , and  $\#S = [\Lambda : \Lambda'] = \mu(F')/\mu(F)$  is finite. We then have

$$\text{covol}(\Lambda') = \mu(F') = \sum_{\lambda \in S} \mu(F + \lambda) = (\#S)\mu(F) = [\Lambda : \Lambda'] \text{covol}(\Lambda),$$

since every translation  $F + \lambda$  of  $F$  is a fundamental domain for  $\Lambda$ .  $\square$

**Definition 14.12.** Let  $S$  be a subset of a real vector space. The set  $S$  is *symmetric* if it is closed under negation, and *convex* if for all  $x, y \in S$  we have  $\{tx + (1-t)y : t \in [0, 1]\} \subseteq S$ .

**Theorem 14.13** (MINKOWSKI'S LATTICE POINT THEOREM). Let  $\Lambda$  be a lattice in  $V \simeq \mathbb{R}^n$  and  $\mu$  a Haar measure on  $V$ . If  $S \subseteq V$  is a symmetric convex measurable set that satisfies

$$\mu(S) > 2^n \text{covol}(\Lambda),$$

then  $S$  contains a nonzero element of  $\Lambda$ .

*Proof.* See Problem Set 6.  $\square$

Note that the inequality in Theorem 14.13 bounds the ratio of the measures of two sets ( $S$  and a fundamental domain for  $\Lambda$ ), and is thus independent of the choice of  $\mu$ .

**Remark 14.14.** In the function field analog of Theorem 14.13 the convexity assumption is not needed and the factor of  $2^n$  can be removed.

## 14.2 The canonical inner product

Let  $K/\mathbb{Q}$  be a number field of degree  $n$  with  $r$  real places and  $s$  complex places; then  $n = r + 2s$ , by Corollary 13.9. We now want to consider the base change of  $K$  to  $\mathbb{R}$  and  $\mathbb{C}$ :

$$\begin{aligned} K_{\mathbb{R}} &:= K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^r \times \mathbb{C}^s, \\ K_{\mathbb{C}} &:= K \otimes_{\mathbb{Q}} \mathbb{C} \simeq \mathbb{C}^n. \end{aligned}$$

The isomorphism  $K_{\mathbb{R}} \simeq \mathbb{R}^r \times \mathbb{C}^s$  follows from Theorem 13.5 and the isomorphism  $K_{\mathbb{C}} \simeq \mathbb{C}^n$  follows from the fact that  $\mathbb{C}$  is separably closed; see Example 4.31. We note that  $K_{\mathbb{R}}$  is an

$\mathbb{R}$ -vector space of dimension  $n$ , thus  $K_{\mathbb{R}} \simeq \mathbb{R}^n$ , but this is an isomorphism of  $\mathbb{R}$ -vector spaces and is not an  $\mathbb{R}$ -algebra isomorphism unless  $s = 0$ .

We have a sequence of injective homomorphisms of topological rings

$$\mathcal{O}_K \hookrightarrow K \hookrightarrow K_{\mathbb{R}} \hookrightarrow K_{\mathbb{C}}, \quad (3)$$

which are defined as follows:

- the map  $\mathcal{O}_K \hookrightarrow K$  is inclusion;
- the map  $K \hookrightarrow K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$  is the canonical embedding  $\alpha \mapsto \alpha \otimes 1$ ;
- the map  $K_{\mathbb{R}} \simeq \mathbb{R}^r \times \mathbb{C}^s \hookrightarrow \mathbb{C}^r \times \mathbb{C}^{2s} \simeq K_{\mathbb{C}}$  embeds each factor of  $\mathbb{R}^r$  in a corresponding factor of  $\mathbb{C}^r$  via inclusion and each  $\mathbb{C}$  in  $\mathbb{C}^s$  is mapped to  $\mathbb{C} \times \mathbb{C}$  in  $\mathbb{C}^{2s}$  via  $z \mapsto (z, \bar{z})$ .

To better understand the last map, note that each  $\mathbb{C}$  in  $\mathbb{C}^s$  arises as  $\mathbb{R}[\alpha] = \mathbb{R}[x]/(f) \simeq \mathbb{C}$  for some monic irreducible  $f \in \mathbb{R}[x]$  of degree 2, but when we base-change to  $\mathbb{C}$  the field  $\mathbb{R}[\alpha]$  splits into the étale algebra  $\mathbb{C}[x]/(x - \alpha) \times \mathbb{C}[x]/(x - \bar{\alpha}) \simeq \mathbb{C} \times \mathbb{C}$ . The composition  $K \hookrightarrow K_{\mathbb{R}} \hookrightarrow K_{\mathbb{C}}$  is given by the map

$$x \mapsto (\sigma_1(x), \dots, \sigma_n(x)),$$

where  $\text{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \{\sigma_1, \dots, \sigma_n\}$ . If we put  $K = \mathbb{Q}(\alpha) := K[x]/(f)$  and let  $\alpha_1, \dots, \alpha_n \in \mathbb{C}$  be the roots of  $f$  in  $\mathbb{C}$ , each  $\sigma_i$  is the  $\mathbb{Q}$ -algebra homomorphism  $K \rightarrow \mathbb{C}$  defined by  $\alpha \mapsto \alpha_i$ .

If we fix a  $\mathbb{Z}$ -basis for  $\mathcal{O}_K$ , its image under the maps in (3) is a  $\mathbb{Q}$ -basis for  $K$ , an  $\mathbb{R}$ -basis for  $K_{\mathbb{R}}$ , and a  $\mathbb{C}$ -basis for  $K_{\mathbb{C}}$ , all of which are vector spaces of dimension  $n = [K : \mathbb{Q}]$ . We may thus view the injections in (3) as inclusions of topological groups (but not rings!)

$$\mathbb{Z}^n \hookrightarrow \mathbb{Q}^n \hookrightarrow \mathbb{R}^n \hookrightarrow \mathbb{C}^n.$$

The ring of integers  $\mathcal{O}_K$  is a lattice in the real vector space  $K_{\mathbb{R}} \simeq \mathbb{R}^n$ , which inherits an inner product from the canonical Hermitian inner product on  $K_{\mathbb{C}} \simeq \mathbb{C}^n$  defined by

$$\langle z, z' \rangle := \sum_{i=1}^n z_i \bar{z}'_i \in \mathbb{C}.$$

For elements  $x, y \in K \hookrightarrow K_{\mathbb{R}} \hookrightarrow K_{\mathbb{C}}$  the Hermitian inner product can be computed as

$$\langle x, y \rangle := \sum_{\sigma \in \text{Hom}_{\mathbb{Q}}(K, \mathbb{C})} \sigma(x) \overline{\sigma(y)} \in \mathbb{R}, \quad (4)$$

which is a real number because the non-real embeddings in  $\text{Hom}_{\mathbb{Q}}(K, \mathbb{C})$  come in complex conjugate pairs. The inner product defined in (4) agrees with the restriction of the Hermitian inner product on  $K_{\mathbb{R}} \hookrightarrow K_{\mathbb{C}}$ . The metric space topology it induces on  $K_{\mathbb{R}}$  is the same as the Euclidean topology on  $K_{\mathbb{R}} \simeq \mathbb{R}^n$  induced by the usual dot product on  $\mathbb{R}^n$ , but the corresponding norm  $\|x\| := \langle x, x \rangle$  has a different normalization, as we now explain.

If we write elements  $z \in K_{\mathbb{C}} \simeq \mathbb{C}^n$  as vectors  $(z_{\sigma})$  indexed by the set  $\sigma \in \text{Hom}_{\mathbb{Q}}(K, \mathbb{C})$  in some fixed order, we may identify  $K_{\mathbb{R}}$  with its image in  $K_{\mathbb{C}}$  as the set

$$K_{\mathbb{R}} = \{z \in K_{\mathbb{C}} : \bar{z}_{\sigma} = z_{\bar{\sigma}} \text{ for all } \sigma \in \text{Hom}_{\mathbb{Q}}(K, \mathbb{C})\}.$$

For real embeddings  $\sigma = \bar{\sigma}$  we have  $z_\sigma \in \mathbb{R} \subseteq \mathbb{C}$ , and for pairs of conjugate complex embeddings  $(\sigma, \bar{\sigma})$  we get the embedding  $z \mapsto (z_\sigma, z_{\bar{\sigma}}) = (z_\sigma, \bar{z}_\sigma)$  of  $\mathbb{C}$  into  $\mathbb{C} \times \mathbb{C}$  used to define the map  $K_{\mathbb{R}} \hookrightarrow K_{\mathbb{C}}$  above. Each  $z \in K_{\mathbb{R}}$  can be uniquely written in the form

$$(w_1, \dots, w_r, x_1 + iy_1, x_1 - iy_1, \dots, x_s + iy_s, x_s - iy_s), \quad (5)$$

with  $w_i, x_j, y_j \in \mathbb{R}$ . Each  $w_i$  corresponds to a  $z_\sigma$  with  $\sigma = \bar{\sigma}$ , and each  $(x_j + iy_j, x_j - iy_j)$  corresponds to a complex conjugate pair  $(z_\sigma, z_{\bar{\sigma}})$  with  $\sigma \neq \bar{\sigma}$ . The canonical inner product on  $K_{\mathbb{R}}$  can then be written as

$$\langle z, z' \rangle = \sum_{i=1}^r w_i w'_i + 2 \sum_{j=1}^s (x_j x'_j + y_j y'_j).$$

Thus if we take  $w_1, \dots, w_r, x_1, y_1, \dots, x_s, y_s$  as coordinates for  $K_{\mathbb{R}} \simeq \mathbb{R}^n$  (as  $\mathbb{R}$ -vector spaces), in order to normalize the Haar measure  $\mu$  on  $K_{\mathbb{R}}$  so that it is consistent with the Lebesgue measure  $\mu_{\mathbb{R}^n}$  on  $\mathbb{R}^n$  we define

$$\mu(S) := 2^s \mu_{\mathbb{R}^n}(S) \quad (6)$$

for any measurable set  $S \subseteq K_{\mathbb{R}}$  that we may view as a subset of  $\mathbb{R}^n$  by expressing it in  $w_i, x_j, y_j$  coordinates as above. With this normalization, the identity (1) still holds when we replace  $\mu_{\mathbb{R}^n}$  with  $\mu$  and the dot product on  $\mathbb{R}^n$  with the Hermitian inner product on  $K_{\mathbb{R}}$ , that is, for any  $\mathbb{R}$ -basis  $e_1, \dots, e_n$  of  $K_{\mathbb{R}}$  we still have

$$\mu(F(e_1, \dots, e_n)) = \sqrt{|\det[\langle e_i, e_j \rangle]_{ij}|} \quad (7)$$

Using the Hermitian inner product on  $K_{\mathbb{R}} \subseteq K_{\mathbb{C}}$  rather than the dot product on  $K_{\mathbb{R}} \simeq \mathbb{R}^n$  multiplies  $2s$  of the columns in the matrix  $[\langle e_i, e_j \rangle]_{ij}$  by 2, and thus multiplies the RHS by  $\sqrt{2^{2s}} = 2^s$ ; our normalization of  $\mu = 2^s \mu_{\mathbb{R}^n}$  multiplies the LHS by  $2^s$  so that (7) still holds.

**Remark 14.15.** In the function field case one replaces the separable closure  $\mathbb{C}$  of  $\mathbb{R}$  with a separable closure  $\mathbb{F}_q(t)_{\infty}^{\text{sep}}$  of  $\mathbb{F}_q(t)_{\infty}$ . The situation is slightly more complicated, since unlike  $\mathbb{C}/\mathbb{R}$ , the extension  $\mathbb{F}_q(t)_{\infty}^{\text{sep}}/\mathbb{F}_q(t)_{\infty}$  is not finite, but for any finite separable extension  $K/\mathbb{F}_q(t)$  (a finite étale  $\mathbb{F}_q(t)$ -algebra) one can base change  $K$  to  $\mathbb{F}_q(t)_{\infty}$  and  $\mathbb{F}_q(t)_{\infty}^{\text{sep}}$ ; these play the role of  $K_{\mathbb{R}}$  and  $K_{\mathbb{C}}$ .

### 14.3 Covolumes of fractional ideals

Having fixed a normalized Haar measure  $\mu$  for  $K_{\mathbb{R}}$ , we can now compute covolumes of lattices in  $K_{\mathbb{R}} \simeq \mathbb{R}^n$ . This includes not only (the image of) the ring of integers  $\mathcal{O}_K$ , but also any nonzero fractional ideal  $I$  of  $\mathcal{O}_K$ : every such  $I$  contains a nonzero principal fraction ideal  $a\mathcal{O}_K$ , and if  $e_1, \dots, e_n$  is a  $\mathbb{Z}$ -basis for  $\mathcal{O}_K$  then  $ae_1, \dots, ae_n$  is a  $\mathbb{Z}$ -basis for  $a\mathcal{O}_K$  that is an  $\mathbb{R}$ -basis for  $K_{\mathbb{R}}$  that lies in  $I$ .

Recall from Remark 12.14 that the discriminant of a number field  $K$  is the integer

$$D_K := \text{disc } \mathcal{O}_K := \text{disc}(e_1, \dots, e_n) \in \mathbb{Z}.$$

**Proposition 14.16.** *Let  $K$  be a number field. Using the normalized Haar measure on  $K_{\mathbb{R}}$  defined in (6),*

$$\text{covol}(\mathcal{O}_K) = \sqrt{|D_K|}.$$

*Proof.* Let  $e_1, \dots, e_n \in \mathcal{O}_K$  be a  $\mathbb{Z}$ -basis for  $\mathcal{O}_K$ , let  $\text{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \{\sigma_1, \dots, \sigma_n\}$ , and define  $A := [\sigma_i(e_j)]_{ij} \in \mathbb{C}^{n \times n}$ . Then  $D_K = \text{disc}(e_1, \dots, e_n) = (\det A)^2$ , by Proposition 12.6

Viewing  $\mathcal{O}_K \hookrightarrow K_{\mathbb{R}}$  as a lattice in  $K_{\mathbb{R}}$  with basis  $e_1, \dots, e_n$ , we may use (7) to compute  $\text{covol}(\mathcal{O}_K) = \mu(F(e_1, \dots, e_n)) = \sqrt{|\det[\langle e_i, e_j \rangle]_{ij}|}$ . Applying (4) yields

$$\det[\langle e_i, e_j \rangle]_{ij} = \det \left[ \sum_k \sigma_k(e_i) \overline{\sigma_k(e_j)} \right]_{ij} = \det(A^t \bar{A}) = (\det A)(\det \bar{A}).$$

Noting that  $\det A$  is the square root of an integer (hence either real or purely imaginary), we have  $\text{covol}(\mathcal{O}_K)^2 = |(\det A)^2| = |D_K|$ , and the proposition follows.  $\square$

Recall from Remark 6.13 that for number fields  $K$  we view the absolute norm

$$\begin{aligned} \mathbb{N}: \mathcal{I}_{\mathcal{O}_K} &\rightarrow \mathcal{I}_{\mathbb{Z}} \\ I &\mapsto [\mathcal{O}_K : I]_{\mathbb{Z}} \end{aligned}$$

as having image in  $\mathbb{Q}_{>0}$  by identifying  $\mathbb{N}(I) \in \mathcal{I}_{\mathbb{Z}}$  with a positive generator for  $\mathbb{N}(I)$  (note that  $\mathbb{Z}$  is a PID). Recall that  $[\mathcal{O}_K : I]_{\mathbb{Z}}$  is a module index of  $\mathbb{Z}$ -lattices in the  $\mathbb{Q}$ -vector space  $K$  (see Definitions 6.1 and 6.5), and for ideals  $I \subseteq \mathcal{O}_K$  this is just the positive integer  $[\mathcal{O}_K : I]_{\mathbb{Z}} = [\mathcal{O}_K : I]$ . When  $I = (a)$  is a principal fractional ideal with  $a \in K$ , we may simply write  $\mathbb{N}(a) := \mathbb{N}((a)) = |\mathbb{N}_{K/\mathbb{Q}}(a)|$ .

**Corollary 14.17.** *Let  $K$  be a number field and let  $I$  be a nonzero fractional ideal of  $\mathcal{O}_K$ . Then*

$$\text{covol}(I) = \mathbb{N}(I) \sqrt{|D_K|}$$

*Proof.* Let  $n = [K:\mathbb{Q}]$ . Since  $\text{covol}(bI) = b^n \text{covol}(I)$  and  $\mathbb{N}(bI) = b^n \mathbb{N}(I)$  for any  $b \in \mathbb{Z}_{>0}$ , without loss of generality we may assume  $I \subseteq \mathcal{O}_K$  (replace  $I$  with a suitable  $bI$  if not). Applying Propositions 14.11 and 14.16, we have

$$\text{covol}(I) = [\mathcal{O}_K : I] \text{covol}(\mathcal{O}_K) = \mathbb{N}(I) \text{covol}(\mathcal{O}_K) = \mathbb{N}(I) \sqrt{|D_K|}$$

as claimed.  $\square$

## 14.4 The Minkowski bound

**Theorem 14.18 (MINKOWSKI BOUND).** *Let  $K$  be a number field of degree  $n$  with  $s$  complex places. Define the Minkowski constant  $m_K$  for  $K$  as the positive real number*

$$m_K := \frac{n!}{n^n} \left( \frac{4}{\pi} \right)^s \sqrt{|D_K|}.$$

*For every nonzero fractional ideal  $I$  of  $\mathcal{O}_K$  there is a nonzero  $a \in I$  for which*

$$\mathbb{N}(a) \leq m_K \mathbb{N}(I).$$

To prove this theorem we need the following lemma.

**Lemma 14.19.** *Let  $K$  be a number field of degree  $n$  with  $r$  real and  $s$  complex places. For each  $t \in \mathbb{R}_{>0}$ , the measure of the convex symmetric set*

$$S_t := \left\{ (z_{\sigma}) \in K_{\mathbb{R}} : \sum |z_{\sigma}| \leq t \right\} \subseteq K_{\mathbb{R}}$$

*with respect to the normalized Haar measure  $\mu$  on  $K_{\mathbb{R}}$  is*

$$\mu(S_t) = 2^r \pi^s \frac{t^n}{n!}.$$

*Proof.* As in (5), we may uniquely write each  $z = (z_\sigma) \in K_{\mathbb{R}}$  in the form

$$(w_1, \dots, w_r, x_1 + iy_1, x_1 - iy_1, \dots, x_s + iy_s, x_s - iy_s)$$

with  $w_i, x_j, y_j \in \mathbb{R}$ . We will have  $\sum_{\sigma} |z_{\sigma}| \leq t$  if and only if

$$\sum_{i=1}^r |w_i| + \sum_{j=1}^s 2\sqrt{|x_j|^2 + |y_j|^2} \leq t. \quad (8)$$

We now compute the volume of this region in  $\mathbb{R}^n$  by relating it to the volume of the simplex

$$U_t := \left\{ (u_1, \dots, u_n) \in \mathbb{R}_{\geq 0}^n : u_1 + \dots + u_n \leq t \right\} \subseteq \mathbb{R}^n,$$

which is  $\mu_{\mathbb{R}^n}(U_t) = t^n/n!$  (volume of the standard simplex in  $\mathbb{R}^n$  scaled by a factor of  $t$ ).

If we view all the  $w_i, x_j, y_j$  as fixed except the last pair  $(x_s, y_s)$ , then  $(x_s, y_s)$  ranges over a disk of some radius  $d \in [0, t/2]$  determined by (8). If we replace  $(x_s, y_s)$  with  $(u_{n-1}, u_n)$  ranging over the triangular region bounded by  $u_{n-1} + u_n \leq 2d$  and  $u_{n-1}, u_n \geq 0$ , we need to incorporate a factor of  $\pi/2$  to account for the difference between  $(2d)^2/2 = 2d^2$  and  $\pi d^2$ ; repeat this  $s$  times. Similarly, if we hold everything but  $w_r$  fixed and replace  $w_r$  ranging over  $[-d, d]$  for some  $d \in [0, t]$  with  $u_r$  ranging over  $[0, d]$ , we need to incorporate a factor of 2 to account for this change of variable; repeat  $r$  times. We then have

$$\mu(S_t) = 2^s \mu_{\mathbb{R}^n}(S_t) = 2^s \left(\frac{\pi}{2}\right)^s 2^r \mu_{\mathbb{R}^n}(U) = 2^r \pi^s \frac{t^n}{n!}. \quad \square$$

*Proof of Theorem 14.18.* Let  $I$  be a nonzero fractional ideal of  $\mathcal{O}_K$ . By Theorem 14.13, if we choose  $t$  so that  $\mu(S_t) > 2^n \text{covol}(I)$ , then  $S_t$  will contain a nonzero  $a \in I$ . By Lemma 14.19 and Corollary 14.17, it suffices to choose  $t$  so that

$$\left(\frac{t}{n}\right)^n = \frac{n! \mu(S_t)}{n^n 2^r \pi^s} > \frac{n! 2^n}{n^n 2^r \pi^s} \text{covol}(I) = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|D_K|} \mathbf{N}(I) = m_K \mathbf{N}(I).$$

Let us now pick  $t$  so that  $\left(\frac{t}{n}\right)^n > m_K \mathbf{N}(I)$ . Then  $S_t$  contains  $a \in I$  with  $\sum_{\sigma} |\sigma(a)| \leq t$ . Recalling that the geometric mean is bounded above by the arithmetic mean, we then have

$$\mathbf{N}(a) = \left(\mathbf{N}(a)^{1/n}\right)^n = \left(\prod_{\sigma} |\sigma(a)|^{1/n}\right)^n \leq \left(\frac{1}{n} \sum_{\sigma} |\sigma(a)|\right)^n \leq \left(\frac{t}{n}\right)^n,$$

Taking the limit as  $\left(\frac{t}{n}\right)^n \rightarrow m_K \mathbf{N}(I)$  from above yields  $\mathbf{N}(a) \leq m_K \mathbf{N}(I)$ . □

## 14.5 Finiteness of the class group

Recall that the ideal class group  $\text{cl } \mathcal{O}_K$  is the quotient of the ideal group  $\mathcal{I}_K$  of  $\mathcal{O}_K$  by its subgroup of principal fractional ideals. We now use the Minkowski bound to prove that every ideal class  $[I] \in \text{cl } \mathcal{O}_K$  can be represented by an ideal  $I \subseteq \mathcal{O}_K$  of small norm. It will then follow that the ideal class group is finite.

**Theorem 14.20.** *Let  $K$  be a number field. Every ideal class in  $\text{cl } \mathcal{O}_K$  contains an ideal  $I \subseteq \mathcal{O}_K$  of absolute norm  $\mathbf{N}(I) \leq m_K$ , where  $m_K$  is the Minkowski constant for  $K$ .*

*Proof.* Let  $[J]$  be an ideal class of  $\mathcal{O}_K$  represented by the nonzero fractional ideal  $J$ . By Theorem 14.18, the fractional ideal  $J^{-1}$  contains a nonzero element  $a$  for which

$$N(a) \leq m_K N(J^{-1}) = m_K N(J)^{-1},$$

and therefore  $N(aJ) = N(a)N(J) \leq m_K$ . We have  $a \in J^{-1}$ , thus  $aJ \subseteq J^{-1}J = \mathcal{O}_K$ , so  $I = aJ$  is an  $\mathcal{O}_K$ -ideal in the ideal class  $[J]$  with  $N(I) \leq m_K$  as desired.  $\square$

**Lemma 14.21.** *Let  $K$  be a number field of degree  $n$  and let  $M \in \mathbb{R}_{>0}$ . The number of  $\mathcal{O}_K$ -ideals of norm  $N(I) \leq M$  is bounded by  $(nM)^{\log_2 M}$  (and in particular, finite).*

*Proof.* Let  $I$  be an ideal of absolute norm  $N(I) \leq M$  and let  $I = \mathfrak{p}_1 \cdots \mathfrak{p}_k$  be its factorization into (not necessarily distinct) prime ideals. We have  $N(\mathfrak{p}_i) \geq 2$  for each  $\mathfrak{p}_i$  so  $k \leq \log_2 M$ . There are less than  $M$  primes  $p \leq M$  and at most  $n$  primes  $\mathfrak{p}$  of  $\mathcal{O}_K$  above each  $p \leq M$ . It follows that there are less than  $(nM)^{\log_2 M}$   $\mathcal{O}_K$ -ideals with norm  $N(I) \leq M$ .  $\square$

**Corollary 14.22.** *Let  $K$  be a number field. The ideal class group of  $\mathcal{O}_K$  is finite.*

*Proof.* By Theorem 14.20, each ideal class is represented by an ideal of norm at most  $m_K$ , and by Lemma 14.21, the number of such ideals is finite.  $\square$

More generally, we have the following result, which can be applied to the analog of the ring of integers in any global field.

**Theorem 14.23.** *Let  $A$  be the ring  $\mathbb{Z}$  or  $\mathbb{F}_q[t]$  and let  $B$  be the integral closure of  $A$  in a finite separable extension of its fraction field. The ideal class group of  $B$  is finite.*

*Proof.* See Problem Set 7.  $\square$

**Remark 14.24.** The geometry of numbers is not a necessary ingredient to Corollary 14.22, there are purely algebraic proofs that apply to any global field; see [9] for an example.

**Remark 14.25.** For imaginary quadratic fields  $K = \mathbb{Q}(\sqrt{-d})$  it is known that the *class number*  $h_K := \#\text{cl } \mathcal{O}_K$  tends to infinity as  $d \rightarrow \infty$  ranges over square-free integers. This was conjectured by Gauss in his *Disquisitiones Arithmeticae* [3] and proved by Heilbronn [5] in 1934; the first fully explicit lower bound was obtained by Oesterlé in 1988 [7]. This implies that there are only a finite number of imaginary quadratic fields with any particular class number. It was conjectured by Gauss that there are exactly 9 imaginary quadratic fields with class number one, but this was not proved until the 20th century by Stark [10] and Heegner [4].<sup>1</sup> Complete lists of imaginary quadratic fields for each class number  $h_K \leq 100$  are now available [12]. By contrast, Gauss predicted that infinitely many real quadratic fields should have class number 1, however this question remains completely open.<sup>2</sup>

**Corollary 14.26.** *Let  $K$  be a number field of degree  $n$  with  $s$  complex places. Then*

$$|D_K| \geq \left(\frac{n^n}{n!}\right)^2 \left(\frac{\pi}{4}\right)^{2s} > \frac{1}{e^2 n} \left(\frac{\pi e^2}{4}\right)^n.$$

<sup>1</sup>Heegner's 1952 result [4] was essentially correct but contained some gaps that prevented it from being generally accepted until 1967 when Stark gave a complete proof in [10].

<sup>2</sup>In fact it is conjectured that  $h_K = 1$  for approximately 75.446% of real quadratic fields with prime discriminant; this follows from the Cohen-Lenstra heuristics [2].

*Proof.* If  $I$  is an ideal and  $a \in I$  is nonzero, then  $N(a) \geq N(I)$ , so Theorem 14.20 implies

$$m_K = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|D_K|} \geq 1,$$

the first inequality follows. The second uses an explicit form of Stirling's approximation,

$$n! \leq e\sqrt{n} \left(\frac{n}{e}\right)^n,$$

and the fact that  $2s \leq n$ . □

We note that  $\pi e^2/4 \approx 5.8 > 1$ , so the minimum value of  $|D_K|$  increases exponentially with  $n = [K : \mathbb{Q}]$ . The lower bounds for  $n \in [2, 7]$  given by the corollary are listed below, along with the least value of  $|D_K|$  that actually occurs. As can be seen in the table,  $|D_K|$  appears to grow much faster than the corollary suggests. Better lower bounds can be proved using more advanced techniques, but a significant gap still remains.

	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$
lower bound from Corollary 14.26	3	13	44	259	986	6267
minimum value of $ D_K $	3	23	275	4511	92799	2306599

**Corollary 14.27.** *If  $K$  is a number field other than  $\mathbb{Q}$  then  $|D_K| > 1$ ; equivalently, there are no nontrivial unramified extensions of  $\mathbb{Q}$ .*

**Theorem 14.28.** *For every real  $M$  the set of number fields  $K$  with  $|D_K| < M$  is finite.*

*Proof.* It follows from Corollary 14.26 that it suffices to prove this for fixed  $n := [K : \mathbb{Q}]$ , since for all sufficiently large  $n$  we will have  $|D_K| > M$  for all number fields  $K$  of degree  $n$ .

**Case 1:** Let  $K$  be a totally real field (so every place  $v|\infty$  is real) with  $|D_K| < M$ . Then  $r = n$  and  $s = 0$ , so  $K_{\mathbb{R}} \simeq \mathbb{R}^r \times \mathbb{C}^s = \mathbb{R}^n$ . Consider the convex symmetric set

$$S := \{(x_1, \dots, x_n) \in K_{\mathbb{R}} \simeq \mathbb{R}^n : |x_1| \leq \sqrt{M} \text{ and } |x_i| < 1 \text{ for } i > 1\}$$

with measure

$$\mu(S) = 2\sqrt{M}2^{n-1} = 2^n\sqrt{M} > 2^n\sqrt{|D_K|} = 2^n \text{covol}(\mathcal{O}_K).$$

By Theorem 14.13, the set  $S$  contains a nonzero  $a \in \mathcal{O}_K \subseteq K \hookrightarrow K_{\mathbb{R}}$  that we may write as  $a = (a_1, \dots, a_n) = (\sigma_1(a), \dots, \sigma_n(a))$ , where the  $\sigma_i$  are the  $n$  embeddings of  $K$  into  $\mathbb{C}$ , all of which are real embeddings. We have

$$N(a) = \left| \prod_i \sigma_i(a) \right| \geq 1,$$

since  $N(a)$  must be a positive integer, and  $|a_2|, \dots, |a_n| < 1$ , so  $|a_1| > 1 > |a_i|$  for all  $i \neq 1$ .

We claim that  $K = \mathbb{Q}(a)$ . If not, each  $a_i = \sigma_i(a)$  would be repeated  $[K : \mathbb{Q}(a)] > 1$  times in the vector  $(a_1, \dots, a_n)$ , since there must be  $[K : \mathbb{Q}(a)]$  elements of  $\text{Hom}_{\mathbb{Q}}(K, \mathbb{C})$  that fix  $\mathbb{Q}(a)$ , namely, those lying in the kernel of the map  $\text{Hom}_{\mathbb{Q}}(K, \mathbb{C}) \rightarrow \text{Hom}_{\mathbb{Q}}(\mathbb{Q}(a), \mathbb{C})$  induced by restriction. But this is impossible since  $a_i \neq a_1$  for  $i \neq 1$ .

The minimal polynomial  $f \in \mathbb{Z}[x]$  of  $a$  is a monic irreducible polynomial of degree  $n$ . The roots of  $f(x)$  in  $\mathbb{C}$  are precisely the  $a_i = \sigma_i(a) \in \mathbb{R}$ , all of which are bounded by  $|a_i| \leq \sqrt{M}$ .

Each coefficient  $f_i$  of  $f(x)$  is an elementary symmetric functions of its roots, hence also bounded in absolute value (certainly  $|f_i| \leq 2^n M^{n/2}$  for all  $i$ ). The  $f_i$  are integers, so there are only finitely many possibilities for  $f(x)$ , hence only finitely many totally real number fields  $K$  of degree  $n$ .

**Case 2:**  $K$  has  $r$  real and  $s > 0$  complex places, and  $K_{\mathbb{R}} \simeq \mathbb{R}^r \times \mathbb{C}^s$ . Now let

$$S := \{(w_1, \dots, w_r, z_1, \dots, z_s) \in K_{\mathbb{R}} : |z_1|^2 < c\sqrt{M} \text{ and } |w_i|, |z_j| < 1 \ (j > 1)\}$$

with  $c$  chosen so that  $\mu(S) > 2^n \text{covol}(\mathcal{O}_K)$  (the exact value of  $c$  depends on  $s$  and  $n$ ). The argument now proceeds as in case 1: we get a nonzero  $a \in \mathcal{O}_K \cap S$  for which  $K = \mathbb{Q}(a)$ , and only a finite number of possible minimal polynomials  $f \in \mathbb{Z}[x]$  for  $a$ .  $\square$

**Lemma 14.29.** *Let  $K$  be a number field of degree  $n$ . For each prime number  $p$  we have*

$$v_p(D_K) \leq n \lfloor \log_p n \rfloor + n - 1.$$

*In particular,  $v_p(D_K) \leq n \lfloor \log_2 n \rfloor + n - 1$  for all  $p$ .*

*Proof.* We have

$$v_p(D_K) = v_p(N_{K/\mathbb{Q}}(\mathcal{D}_{K/\mathbb{Q}})) = \sum_{\mathfrak{q}|p} f_{\mathfrak{q}} v_{\mathfrak{q}}(\mathcal{D}_{K/\mathbb{Q}})$$

where  $\mathcal{D}_{K/\mathbb{Q}}$  is the different ideal and  $f_{\mathfrak{q}}$  is the residue degree of  $\mathfrak{q}|p$ . Using Theorem 12.27 to bound  $v_{\mathfrak{q}}(\mathcal{D}_{K/\mathbb{Q}})$  yields

$$v_p(D_K) \leq \sum_{\mathfrak{q}|p} f_{\mathfrak{q}} (e_{\mathfrak{q}} - 1 + v_{\mathfrak{q}}(e_{\mathfrak{q}})) = n - \sum_{\mathfrak{q}|p} f_{\mathfrak{q}} + \sum_{\mathfrak{q}|p} f_{\mathfrak{q}} e_{\mathfrak{q}} v_p(e_{\mathfrak{q}}) \leq n - 1 + n \lfloor \log_p n \rfloor,$$

where we have used  $-1$  as an upper bound on  $-\sum_{\mathfrak{q}|p} f_{\mathfrak{q}}$  and  $\lfloor \log_p n \rfloor$  as an upper bound on each  $v_p(e_{\mathfrak{q}})$  (since  $e_{\mathfrak{q}} \leq n$ ), and the fact that  $\sum_{\mathfrak{q}|p} e_{\mathfrak{q}} f_{\mathfrak{q}} = n$  (by Theorem 5.35).  $\square$

**Remark 14.30.** The bound in Lemma 14.29 is tight; it is achieved by  $K = \mathbb{Q}[x]/(x^{p^e} - p)$ , for example.

**Theorem 14.31** (Hermite). *Let  $S$  be a finite set of places of  $\mathbb{Q}$ , and let  $n$  be an integer. The number of extensions  $K/\mathbb{Q}$  of degree  $n$  unramified outside of  $S$  is finite.*

*Proof.* By Lemma 14.29, since  $n$  is fixed, the valuation  $v_p(D_K)$  is bounded for each  $p \in S$  and must be zero for  $p \notin S$ . Thus  $|D_K|$  is bounded, and the theorem then follows from Proposition 14.28.  $\square$

**Remark 14.32.** In the function field analogs of Theorem 14.28 and Theorem 14.31 one requires  $K$  to be a separable extension of  $\mathbb{F}_q(t)$  with constant field  $\mathbb{F}_q$  (so  $K \cap \overline{\mathbb{F}_q} = \mathbb{F}_q$ ). This is not really a restriction in the sense that every global function field  $K$  contains a subfield  $\mathbb{F}_q(t)$  for which this is true, but one needs to take  $q = \#(K \cap \overline{\mathbb{F}_q})$  and to choose  $t$  to be a separating element (such a  $t$  exists by [6, Thm. 7.20]). Unlike the number field setting where the embedding of the rational numbers  $\mathbb{Q}$  in a number field  $K$  is unique, there are many ways to embed the rational function field  $\mathbb{F}_q(t)$  in a global function field  $K$ . The notion of an absolute discriminant  $D_K$  doesn't really make sense in this setting, one can speak of the discriminant  $D_{K/\mathbb{F}_q(t)}$  only after fixing a suitable choice of  $\mathbb{F}_q(t)$ . As you showed on Problem Set 6, the valuation of the discriminant of an extension of global function fields is not bounded as a function of the degree, in general, and this means that the function field analog of Lemma 14.29 only holds when we use the discriminant of a separable extension.

## References

- [1] Nicolas Bourbaki, [\*General Topology: Chapters 1-4\*](#), Springer, 1995.
- [2] Henri Cohen and Hendrik W. Lenstra Jr., [\*Heuristics on class groups of number fields\*](#), in *Number Theory (Noordwijkerhout 1983)*, Lecture Notes in Mathematics **1068**, Springer, 1984, 33–62.
- [3] Carl F. Gauss, [\*Disquisitiones Arithmeticae\*](#), Göttingen (1801), English translation by Arthur A. Clark, revised by William C. Waterhouse, Spring-Verlag 1986 reprint of Yale University Press 1966 edition.
- [4] Kurt Heegner, [\*Diophantische Analysis und Modulfunktionen\*](#), Math. Z. **56** (1952), 227–253.
- [5] Hans Heilbronn, [\*On the class number in imaginary quadratic fields\*](#), Quart. J. of Math. Oxford **5** (1934), 150–160.
- [6] Anthony W. Knapp, [\*Advanced Algebra\*](#), Digital Second Edition, 2016.
- [7] Joseph Oesterlé, [\*La probléme de Gauss sur le nombre de classes\*](#), Enseign. Math. **34** (1988), 43–67.
- [8] Michael Rosen, [\*A geometric proof of Hermite’s theorem in function fields\*](#), J. Théor. Nombres Bordeaux **29** (2017), 799–813.
- [9] Alexander Stasinski, [\*A uniform proof of the finiteness of the class group of a global field\*](#), American Mathematical Monthly **1228** (2021), 239–249.
- [10] Harold Stark, [\*A complete determination of the complex quadratic fields of class-number one\*](#), Mich. Math. J. **14** (1967), 1–27.
- [11] Terence Tao, [\*An introduction to measure theory\*](#), Graduate Studies in Mathematics **126**, AMS, 2010.
- [12] Mark Watkins, [\*Class numbers of imaginary quadratic fields\*](#), Math. Comp. **73** (2004), 907–938.

MIT OpenCourseWare  
<https://ocw.mit.edu>

18.785 Number Theory I  
Fall 2021

For information about citing these materials or our Terms of Use, visit: <https://ocw.mit.edu/terms>.