Algebraic Number Theory

Rahul Dintyala

May 9, 2024

Theorem

Let H be a discrete subgroup of $\mathbb{R}^n$. Then H is generated (as a $\mathbb{Z}$-module) by r vectors which are linearly independent over $\mathbb{R}$ (so $r \leq n$).

Theorem

Let G be a group and $\mathbb{K}$ a field. Then, distinct characters are linearly independent over $\mathbb{K}$.

Proof. Suppose

$$a_1\chi_1 + \ldots + a_n\chi_n = 0 \qquad (\star)$$

with $a_i \in \mathbb{K}$ not all zero and n minimal with this property. Then ofcourse $n \geq 2$ and $a_i \neq 0$ for all i. Since χ_1 and χ_2 are distinct, there exists $h \in G$ such that $\chi_1(h) \neq \chi_2(h)$. Then, for any $g \in G$,

$$0 = a_1\chi_1(hg) + \cdots + a_n\chi_n(hg) = a_1\chi_1(h)\chi_1(g) + \cdots + a_n\chi_n(h)\chi_n(g)$$

which means that $a_1\chi_1(h)\chi_1 + \cdots + a_n\chi_n(h)\chi_n = 0$. Dividing this last expression by $\chi_1(h)$ and subtracting it from $(\star)$ we get :

$$\left(a_2 - a_2\frac{\chi_2(h)}{\chi_1(h)}\right)\chi_2 + \cdots + \left(a_n - a_n\frac{\chi_n(h)}{\chi_1(h)}\right)\chi_n = 0$$

contradicting the minimality of n. Thus, any collection of distinct characters must be linearly independent. ∎

Corollary

Suppose that $L/\mathbb{K}$ is a finite normal extension of fields and $\sigma_1, \ldots, \sigma_n$ be the distinct automorphisms of L. Then these are linearly independent over L.

Proof. Follows from previous theorem by viewing the automorphisms as homomorphisms from $L^* \to L^*$. ■

Corollary

Let $L/\mathbb{K}$ be a finite Galois extension of fields of degree n. Suppose that $x_1, \ldots, x_n$ is a basis of L over $\mathbb{K}$ and let $\sigma_1, \ldots, \sigma_n$ be the distinct $\mathbb{K}$-automorphisms of L. Then, $\det(\sigma_j(x_i)) \neq 0$.

Proof. Suppose that this determinant is actually zero. Then, there exist $a_1, \ldots, a_n$ not all zero such that $\sum_j a_j \sigma_j(x_i) = 0$ for all $1 \leq i \leq n$. Now, since $x_1, \ldots, x_n$ make a basis of L, for any $l \in L$, $\sum_j a_j \sigma_j(l) = 0$. Thus, $\sigma_j a_j \sigma_j = 0$ contradicting the previous corrolary. ■

Definition

A discrete subgroup of rank n of $\mathbb{R}^n$ is called a lattice in $\mathbb{R}^n$.

Lemma

The volume $\mu(P_e)$ is independent of the base chosen for H.

Theorem

Let H be a lattice in $\mathbb{R}^n$ and let S be a measurable subset of $\mathbb{R}^n$ such that $\mu(S) > \text{vol}(H)$. Then there exist two distinct points $x, y \in S$ such that $x - y \in H$.

Corollary

Let H be a full-dimensional lattice in $\mathbb{R}^n$ and let $C \subseteq \mathbb{R}^n$ be a convex set symmetric about the origin ($i.e. x \in C \implies -x \in C$). Suppose that either :

1. $(C) > 2^n \cdot (H)$, or
2. $(C) \geq 2^n \cdot (H)$ and C is compact.

Then $\mathbb{C} \cap (H \setminus \{0\}) \neq \varnothing$.

Proposition

If M is a free $\mathbb{Z}$-submodule of K of rank n and if $(x_i)_{1\leq i\leq n}$ is a $\mathbb{Z}$-base for M then $\sigma(M)$ is a lattice in $\mathbb{R}^n$, whose volume is :

$$\mathrm{vol}(\sigma(M)) = 2^{-r_2}|\det_{1\leq i,j\leq n}(\sigma_i(x_j))|.$$

Proposition

Let d be the absolute discriminant of K, let A be the ring of integers in K, and let $\mathfrak{a}$ be a non-zero integral ideal of A. Then $\sigma(A)$ and $\sigma(\mathfrak{a})$ are lattices. Moreover,

$$\text{vol}(\sigma(A)) = 2^{-r_2}|d|^{\frac{1}{2}} \quad \text{and} \quad \text{vol}(\sigma(\mathfrak{a})) = 2^{-r_2}|d|^{\frac{1}{2}} N(\mathfrak{a}).$$

Proposition

Let K be a number field, n its degree, r_1 and r_2 are integers defined earlier, d the absolute discriminant of K, and $\mathfrak{a}$ a non-zero integral ideal of K. Then $\mathfrak{a}$ contains a non-zero element x such that :

$$|N_{K/\mathbb{Q}}(x)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d|^{\frac{1}{2}} N(\mathfrak{a}).$$

Corollary

With the same notations, every ideal class of K contains an integral ideal $\mathfrak{b}$ such that :

$$N(\mathfrak{b}) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d|^{\frac{1}{2}}.$$

Theorem

For any number field K the ideal class group is finite.