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. ∎