

Algebraic numbers & algebraic integers

Lecture 20

21/11/22

Def. 1 a) $z \in \mathbb{C}$ is an algebraic number if it is a root of a polynomial in $\mathbb{Q}[x]$.

b) $z \in \mathbb{C}$ is an algebraic integer if it is a root of a monic polynomial in $\mathbb{Z}[x]$
($x^m + c_1 x^{m-1} + \dots + c_m$, $c_i \in \mathbb{Z}$).

Def. 2. $z \in \mathbb{C}$ is an algebraic number (algebraic integer) if z is an eigenvalue of a matrix with rational (resp. integer) coef.

Prop. Def 1 $\Leftrightarrow$ Def 2.

Proof $\Leftarrow$. If z is an eigenvalue of $A \in \text{Mat}_n(\mathbb{Q})$ (or $\mathbb{Z}$)

z is a root of $\chi_A(x) \in \mathbb{Q}[x]$ (or $\mathbb{Z}[x]$). $p(x)$

$\Rightarrow$. Suppose z is a root of $x^m + c_1 x^{m-1} + \dots + c_m = 0$.

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -c_m \\ 1 & 0 & & & -c_{m-1} \\ 0 & 1 & 0 & & \\ \vdots & 0 & 1 & & \\ 0 & 0 & & 1 & -c_1 \end{pmatrix} = A$$

$$A: \mathbb{Q}[x]/(p(x)) \rightarrow \mathbb{Q}[x]/(p(x))$$

$$f(x) \mapsto x \cdot f(x)$$

□

Notation: $\overline{\mathbb{Q}}$ alg numbers

$\overline{\mathbb{Z}}$ alg. integers

Prop. (a) $\overline{\mathbb{Z}}$ is a ring.

(b) $\overline{\mathbb{Q}}$ is a field. It is an alg. closure of $\mathbb{Q}$.

Proof. Use Def. 2. Let $\alpha, \beta \in \overline{\mathbb{Z}}$.

Let α be ev. of $A \in \text{Mat}_n(\mathbb{C})$, $Av = \alpha v$

β be ev. of $B \in \text{Mat}_m(\mathbb{C})$, $Bw = \beta w$.

$$A \otimes B: \mathbb{C}^n \otimes \mathbb{C}^m \rightarrow \mathbb{C}^n \otimes \mathbb{C}^m. \quad (A \otimes B)(v \otimes w) = \alpha \beta (v \otimes w)$$

$$\alpha, \beta \in \overline{\mathbb{Z}} \quad (\text{or } \overline{\mathbb{Q}}).$$

$\alpha \pm \beta$ is an eigenvalue of $A \otimes Id_m \pm Id_n \otimes B$. (a)

(b): if α is a root of $p(x)$, $\deg p(x) = d$,
then α^{-1} is a root of $x^d \cdot p(1/x)$.

Alg. closure: α algebraic $\Leftrightarrow [Q(\alpha) : Q] < \infty$. $\square$

Prop. $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.

Proof. Let $z \in \overline{\mathbb{Z}}$ be a root of
$$x^n + c_1 x^{n-1} + \dots + c_n = 0, \quad c_i \in \mathbb{Z}.$$

If $\frac{p}{q} = z$, $(p, q) = 1$, then

$$\left(\frac{p}{q}\right)^n + c_1 \left(\frac{p}{q}\right)^{n-1} + \dots + c_n = 0$$

$$p^n + c_1 p^{n-1} q + \dots + c_n q^n = 0.$$

$$\Rightarrow q = \pm 1. \quad p/q \in \mathbb{Z}.$$

if $q \neq \pm 1$,
 $p^n : q \Rightarrow$
 $\square$

Every alg. number $\alpha \in \mathbb{Q}$ has a minimal polynomial

$\mu_\alpha(x)$: a monic polynomial of min degree s.t.

$$\mu_\alpha(\alpha) = 0.$$

Any other $p(x)$, $p(\alpha) = 0$, is divisible by $\mu_\alpha(x)$.
 $\Rightarrow \mu_\alpha(x)$ is unique.

The roots $\alpha = \alpha_1, \alpha_2, \dots, \alpha_m$ are the conjugates of α .

if α  alg integer, these are alg. integers.

Viète $\Rightarrow \mu_\alpha(x) \in \mathbb{Z}[x]$. (also follows from $\mathbb{Z}[x]$ being a UFD).

Lemma: If $\alpha_1, \dots, \alpha_m$ alg numbers, all the conjugates
 $\alpha_1 + \dots + \alpha_m$ are of the form $\alpha'_1 + \dots + \alpha'_m$, α'_i conj to α_i .

Proof: Enough to prove for $m=2$. α_1, α_2 are eigenvalues of
 A_1, A_2 of the smallest size, $\chi_{A_i} = \mu_{\alpha_i}$.

$\alpha_1 + \alpha_2$ is an eigenvalue of $A_1 \otimes I_m + I_n \otimes A_2$.

So is any of its conjugates. All of them have the form $\alpha'_1 + \alpha'_2$, $\alpha'_i \sim \alpha_i$. $\square$

Thm. (Frobenius divisibility thm). Let G be a fin. group, V irred. f.d. complex rep. of G , then $\dim V \mid \#G$.

Proof. Let $C_1, \dots, C_n$ be the conj classes of G .

$$\lambda_i = \chi_V(g_{C_i}) \cdot \frac{|C_i|}{\dim V}, \text{ where } g_i \in C_i$$

Lemma. $\forall i$, λ_i is an alg. integer.

Proof. Let C conj class in G , $P = \sum_{h \in C} h \in \mathbb{Z}[G]$.

P is central, so $P_V = \lambda \cdot I_V$.

So λ is alg. integer: h is integral over $\mathbb{Z}$:

$\Rightarrow h$ satisfies a monic polyn. equation, and so does P .

$$\text{Tr}_V P = \chi_V(g) \cdot |C| = \lambda \cdot \dim V.$$

$$\lambda = \chi_V(g_c) \cdot \frac{|G|}{\dim V} \quad \text{alg. integer.} \quad \square$$

Consider $\sum_{c_i} \lambda_i \overline{\chi_V(g_{c_i})}$. It also belongs to $\mathbb{Z}$. Indeed:

- λ_i alg. integers;
- $\overline{\chi_V(g_c)}$ are sums of eigenvalues of $\rho(g_c)$,
so they are sums of $\sqrt{1}$.

$$\sum_{c_i} \lambda_i \overline{\chi_V(g_{c_i})} = \sum_{c_i} \frac{|C_i| \cdot \chi_V(g_{c_i}) \overline{\chi_V(g_{c_i})}}{\dim V} =$$

$$= \sum_{g \in G} \frac{\chi_V(g) \overline{\chi_V(g)}}{\dim V} = \frac{|G| \cdot (\chi_V, \chi_V)}{\dim V} = \frac{|G|}{\dim V} \in \mathbb{Q}.$$

$$\frac{|G|}{\dim V} \in \mathbb{Q} \cap \mathbb{Z} = \mathbb{Z}, \quad |G| : \dim V. \quad \square$$

Burnside's theorem.

Def. G is solvable if

$$\{e\} = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \dots \triangleleft G_{n-1} \triangleleft G_n = G,$$

G_i/G_{i-1} is abelian $\forall i \in [1, \dots, n]$.

Thm. (Burnside). Any group of order $p^a q^b$, $a, b \geq 0$, is solvable.

Exercise. Prove "by hands" that groups of order: (i) p^n ;

(ii) pq , (iii) p^2q are solvable.

Thm. Let V be an irrep of G , $\#G < \infty$, and $C \subset G$ conj. class s.t. $(\#G, \#C) = 1$. Then $\forall g \in C$, either

$\chi_V(g) = 0$ or g_V is a scalar.

Lemma. Let $\varepsilon_1, \dots, \varepsilon_n$ be roots of 1, $\frac{1}{n}(\varepsilon_1 + \dots + \varepsilon_n) \in \overline{\mathbb{Z}}$. Then either $\varepsilon_1 = \dots = \varepsilon_n$ or $\varepsilon_1 + \dots + \varepsilon_n = 0$.

Proof. $a = \frac{1}{n} (\epsilon_1 + \dots + \epsilon_n)$. If ϵ_i 's are not equal,

$|a| < 1$. Then for any $a' \sim a$,

a' is a sum of roots of 1, div. by $n \Rightarrow |a'| \leq 1$.

a , all a' are alg. integers.

But $\prod_{a' \sim a} a' \in \mathbb{Z}$, so $|\prod a'| < 1$.

So $a = 0$. $\square$

Proof of Theorem. Take $p_V(g)$. Its e.v. $\epsilon_1, \dots, \epsilon_n$ roots of 1,

$\chi_V(g)$ is an alg. integer. Let $n = \dim V$.

$\frac{1}{n} |C| \chi_V(g)$ is an alg integer. (Lemma)

$(n, |C|) = 1$. (Frob. divisibility).

$$1 = a \cdot n + b \cdot |C|.$$

$\frac{\chi_V(g)}{n} = \frac{1}{n} (\epsilon_1 + \dots + \epsilon_n)$ is also an alg. integer.

Indeed: $\frac{\chi_V(g)}{n} = a \cdot \chi_V(g) + b \cdot \frac{|C| \cdot \chi_V(g)}{n}$.

$\uparrow$
 alg integers

Lemma $\Rightarrow$ either $\epsilon_1 = \dots = \epsilon_n \Rightarrow \rho_V(g)$ scalar

or $\epsilon_1 + \dots + \epsilon_n = 0 \Rightarrow$

$\Rightarrow \chi_V(g) = 0$.

Thm. Let G be a fin. group,
 $C \subseteq G$ conj class, $|C| = p^k$. Then G has a
 proper normal subgroup (i.e. nonsimple).

Proof. $g \in C$. $\sum_{V \in \text{Irr } G} \dim V \cdot \chi_V(g) = 0$.

- $\text{Irr } G \rightarrow$
- (a) trivial rep
 - (b) D , s.t. $\dim D \equiv p$
 - (c) N , s.t. $\dim N \not\equiv p$.

Claim: $\exists V \in N$ s.t. $\chi_V(g) \neq 0$

Proof. If $V \in D$, $\frac{1}{p} \dim V \cdot \chi_V(g)$ is an alg. integer,

$a = \sum_{D \supset V} \frac{1}{p} \dim V \chi_V(g)$ is an alg. integer.

$$0 = \chi_C(g) + \sum_{V \in D} \dim V \cdot \chi_V(g) + \sum_{V \in N} \dim V \cdot \chi_V(g) = 1 + pa + \sum_{V \in N} \dim V \chi_V(g)$$

$$\sum \dim V \chi_V(g) \neq 0 \Rightarrow \chi_V(g) \neq 0 \quad \exists V \in N. \quad \square$$

Proof of Thm. Claim $\Rightarrow \exists V \in N \chi_V(g) \neq 0$.

So g acts by a scalar in V , and so do all the elements in C .

$H = \langle ab^{-1} \mid a, b \in C \rangle$ acts trivially on V . $H \triangleleft G$.

But V nontrivial $\Rightarrow H \neq G$. But $H \neq 1$. $\square$

Proof of Burnside's Thm. Assume the contrary.

$\Rightarrow \exists$ a nonsolvable group G , $|G| = p^a q^b$.

The smallest group with this property is simple.

Then every conj class C satisfies $|C|=1$ or
 $|C|=p$.

Then $Z(G) \neq \{e\}$, contradiction. $\square$.