4 Interplay with Galois theory

4.1 Algebraic integers

$\overline{\mathbb{Q}} \subset \mathbb{C}$ algebraic closure of $\mathbb{Q}$

Def: An *algebraic integer* is an element $a \in \overline{\mathbb{Q}}$ that is the root of a monic polynomial $f \in \mathbb{Z}[T]$. We write $\mathbb{Z}^{int}$ for the subset of algebraic integers in $\overline{\mathbb{Q}}$.

Ex: (0) $a \in \mathbb{Z}$ is the root of $T - a \Rightarrow a \in \mathbb{Z}^{int}$.

(1) $\sqrt{2}$ is the root of $T^2 - 2 \Rightarrow \sqrt{2} \in \mathbb{Z}^{int}$.

(2) ζ_n is the root of $T^n - 1 \Rightarrow \zeta_n \in \mathbb{Z}^{int}$.

Prop 1: For $a \in \overline{\mathbb{Q}}$, the following are equivalent:

(1) $a \in \mathbb{Z}^{int}$;

(2) the minimal polynomial $f \in \mathbb{Q}[T]$ of a over $\mathbb{Q}$ is in $\mathbb{Z}[T]$;

(3) a is an eigenvalue of a square matrix with integer coefficients;

(4) the subring $\mathbb{Z}[a] \subset \overline{\mathbb{Q}}$ is finitely generated as a $\mathbb{Z}$-module.

proof: (only (1) ⇒ (2) ⇒ (3) ⇒ (1))

(1) ⇒ (2): · By def., α is the root of a monic $f \in \mathbb{Z}[T]$.

· Let $g \in \mathbb{Q}[T]$ be the min. pol. of α, which is monic.

Then $f = g \cdot h$ for some $h \in \mathbb{Q}[T]$, and also h is monic.

· Since f, g, h monic, $\mathrm{cont}(f)^{-1}$, $\mathrm{cont}(g)^{-1}$, $\mathrm{cont}(h)^{-1}$ are all in $\mathbb{Z}$. Since $f \in \mathbb{Z}[T]$, $\mathrm{cont}(f) = 1$.

$\Rightarrow$ $\mathrm{cont}(g) \cdot \mathrm{cont}(h) = \mathrm{cont}(f) = 1$

(Gauss' Lemma)

$\Rightarrow$ $\mathrm{cont}(g) = \mathrm{cont}(h) = 1$

$\Rightarrow$ $g \in \mathbb{Z}[T]$. Thus (2). ∎

(2) ⇒ (3): The min. pol. $f = T^n + c_{n-1}T^{n-1} + \cdots + c_0$ of α over $\mathbb{Q}$ is the char. pol. of

$$A = \begin{bmatrix} 0 & & & -c_0 \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & \\ 0 & & 1 & -c_{n-1} \end{bmatrix}$$

[companion matrix of f]

Since the roots of f are the eigenvalues of A, α is an eigenvalue of A. Thus (3). ∎

(3) ⇒ (1): If α is an eigenvalue of $A \in \mathrm{Mat}_{n\times n}(\mathbb{Z})$, then α is a root of the char. pol. f of A, which is monic and in $\mathbb{Z}[T]$. Thus (1). ∎

□

Cor 2: $\mathbb{Z}^{int} \cap \mathbb{Q} = \mathbb{Z}$.

proof: • Clearly $\mathbb{Z} \subset \mathbb{Z}^{int} \cap \mathbb{Q}$.

• If $a \in \mathbb{Q} \cap \mathbb{Z}^{int}$, then its min. pol. over $\mathbb{Q}$ is $T - a \Rightarrow T - a \in \mathbb{Z}[T] \Rightarrow a \in \mathbb{Z}$. (Prop 1) □

Prop 3: $\mathbb{Z}^{int}$ is a subring of $\overline{\mathbb{Q}}$.

proof: • Since $\pm 1 \in \mathbb{Z}^{int}$, it suffices to show that $a+b, a \cdot b \in \mathbb{Z}^{int}$ for all $a, b \in \mathbb{Z}^{int}$.

• By Prop. 1, a is an eigenvalue of a matrix $A = (\alpha_{ij}) \in Mat_{n \times n}(\mathbb{Z})$ with eigenvector $v \in \mathbb{C}^n - \{0\}$, and b is an eigenvalue of a matrix $B = (\beta_{ij}) \in Mat_{m \times m}(\mathbb{Z})$ with eigenvector $w \in \mathbb{C}^m - \{0\}$.

Then $a+b$ is an eigenvalue of

$$A \otimes \mathbb{1}_m + \mathbb{1}_n \otimes B = \left(\alpha_{ij} \delta_{kl} + \delta_{ij} \beta_{kl} \right)_{\substack{i,j=1,\dots,n \\ k,l=1,\dots,n}}$$

($\mathbb{1}$: identity matrix; δ: Kronecker symbol)

for the eigenvector $v \otimes w = (v_i \cdot w_k)_{\substack{i=1,\dots,n \\ k=1,\dots,m}}$,

and $a \cdot b$ is an eigenvalue of

$$A \otimes B = \left(\alpha_{ij} \beta_{kl} \right)_{\substack{i,j=1,\dots,n \\ k,l=1,\dots,n}}$$

for the eigenvector $v \otimes w$.

$\Rightarrow a+b, a \cdot b \in \mathbb{Z}^{int}$. □

4.2 Frobenius divisibility

$K = \mathbb{C}$

G finite group

Lemma 1: V irred. G-repr. / $\mathbb{C}[G]$-module

$x \in Z(\mathbb{Z}[G]) = \{x \in \mathbb{Z}[G] \mid xy = yx \ \forall y \in \mathbb{Z}[G]\}$

(center of $\mathbb{Z}[G]$)

Then there is a $\lambda \in \mathbb{C}$ such that $x.v = \lambda v$ for all $v \in V$.

[x acts as a scalar on V]

Proof: Let λ be an eigenvalue of $\vartheta_x : \underset{v}{V} \to \underset{x.v}{V}$ and let $V_\lambda \subset V$ be the λ-eigenspace of the endomorphism

$\vartheta_x : \underset{v}{V} \longrightarrow \underset{x.v}{V}$, i.e. $x.v = \lambda v$ for all $v \in V_\lambda$.

- Given any $y = \sum c_g g \in \mathbb{C}[G]$ and $v \in V_\lambda$, we have

$$x.(y.v) = (x \cdot \textstyle\sum c_g g).v = (\sum c_g xg).v = (\sum c_g gx).v = (yx).v$$

$$= y.(x.v) = y.(\lambda v) = \lambda (y.v),$$

thus $y.v \in V_\lambda$. This shows that V_λ is $\mathbb{C}[G]$-inv.

Since V is irred., $V = V_\lambda$. □

Prop 2: V $\mathbb{C}[G]$-module

$x \in \mathbb{Z}[G]$

Then every eigenvalue of x is an algebraic integer.

proof: Since $\mathbb{Z}[G] = \{\sum a_g g \mid a_g \in \mathbb{Z}\}$ is Noetherian as a finitely generated $\mathbb{Z}$-module, there is a $d \geq 0$ s.t.

$$x^d \in \langle 1, x, \dots, x^{d-1} \rangle_{\mathbb{Z}},$$

i.e. $f(x) = 0$ for a monic $f \in \mathbb{Z}[T]$ of degree d.

- Thus $f(\lambda_x) = 0$ for the endomorphism $\lambda_x : V \to V,\ v \mapsto x.v$ and the min. pol. g of λ_x divides f. Since also g is monic, the Gauss Lemma implies that $g \in \mathbb{Z}[T]$.

Thus all eigenvalues of λ_x, which are the roots of g, are in $\mathbb{Z}^{int}$ by Prop. 4.1.1. ☐

Lemma 3: V irred. G-repr. with character χ
C conj. cl. of G
Then $\frac{\#C}{\dim V} \cdot \chi(C)$ is an algebraic integer.

proof: • The element $z = \sum_{h \in C} h$ is in the center of $\mathbb{Z}[G]$ since for all $g \in G$,

$$gzg^{-1} = \sum_{h \in C} ghg^{-1} = \sum_{h' \in C} h' = z.$$

$(h' = ghg^{-1})$

$\Rightarrow \exists \lambda \in \mathbb{C}$ s.t. $z \cdot v = \lambda v \quad \forall v \in V$.
(Prop. 1)

By Prop. 2, $\lambda \in \mathbb{Z}^{int}$

- Thus

$$\#C \cdot \chi(C) = \sum_{h \in C} \mathrm{tr}\, h = \mathrm{tr}\, z = \lambda \cdot \dim V$$

and $\dfrac{\#C}{\dim V} \cdot \chi(C) = \lambda \in \mathbb{Z}^{int}$. □

Thm. 4: (Frobenius divisibility)

V irred. G-repr. with character χ

Then $\dim V$ divides $\#G$.

proof: - Let $C_1, \dots, C_s$ be the conjugacy classes of G,

- $g_i \in C_i$ representatives $(i = 1, \dots, s)$

- $\lambda_i := \dfrac{\#C_i}{\dim V} \cdot \chi(C_i) \in \mathbb{Z}^{int}$ (by Lemma 3)

- Then

$\chi(C_i) = \mathrm{tr}(g_V(g_i)) = \sum (\text{eigenvalues of } g_i) \in \mathbb{Z}^{int}$,

and also $\overline{\chi(C_i)} \in \mathbb{Z}^{int}$. ($\overline{(\cdot)}$ is an autom. of $\bar{\mathbb{Q}}$ that fixes $\mathbb{Q} \Rightarrow$ a & $\bar{a}$ have the same min. pol.)

$$\Rightarrow z = \sum_{i=1}^{s} \lambda_i \cdot \overline{\chi(C_i)} \in \mathbb{Z}^{int}.$$

- On the other hand,

$$z = \sum_{i=1}^{s} \frac{\#C_i}{\dim V} \chi(C_i) \cdot \overline{\chi(C_i)}$$

$$= \frac{\#G}{\dim V} \cdot \frac{1}{\#G} \underbrace{\sum_{g \in G} \chi(g) \cdot \overline{\chi(g)}}_{= \langle \chi, \chi \rangle = 1 \quad \text{since } V \text{ irred.}}$$

$$= \frac{\#G}{\dim V} \in \mathbb{Q}$$

- Since $\mathbb{Q} \cap \mathbb{Z}^{int} = \mathbb{Z}$ by Cor. 4.1.2,

$\frac{\#G}{\dim V} = z \in \mathbb{Z}$. Thus $\dim V \mid \#G$. □