Chapter 6: Burnside's Theorem

Goal: 6.3.11: No group of order $p^a q^b$ (p, q prime, $a+b \geq 2$) is simple.

Simple: no non-trivial proper normal subgroup.

Proved by Burnside in early 1900's using rep. thy.

6.1: Algebraic numbers

6.2: dimension theorem: $\mathcal{O}$ an integral, degree $\mathcal{O} \mid |G|$.

6.3: Lemmas + proof 6.3.11. (Galois thy.)

§6.1 A little number theory

$y \in \mathbb{C}$ is **algebraic** if it's a root of a polynomial $f \in \mathbb{Z}[z]$.

Ex: m/n is a root of $nz - m$.

$\sqrt{2}$ " " " $z^2 - 2$

i " " " $z^2 + 1$

But e, π not algebraic.

$\bar{\mathbb{Q}} := \{\text{alg. numbers}\}$. Countable.

Def 6.1.1: $y \in \mathbb{C}$ is an **algebraic integer** if it's the root of a monic poly. $f \in \mathbb{Z}[z]$.

$\mathbb{A} := \{\text{alg. ints}\} \subseteq \bar{\mathbb{Q}}$.

Prop 6.1.4: $y \in \mathbb{Q}$ is in $\mathbb{A}$ iff $y \in \mathbb{Z}$.

Pf: Easy. Exercise. (or see text.) □

Ex: $m \in \mathbb{Z} \Rightarrow m \in \mathbb{A}$: $z - m$.

6.1.2: $e^{2\pi i k/n} \in \mathbb{A}$ $z^n - 1$.

$\sqrt[n]{m} \in \mathbb{A}$ $z^n - m$.

Note: $y \in \mathbb{A} \Rightarrow -y \in \mathbb{A}$.

If $f(y) = 0$, then $-y$ is a root of $f(-z)$ and $-f(-z)$, and one is monic.

6.1.4: To prove d/n, it suffices to show that $a/d \in \mathbb{A}$.

6.1.3: $A \in M_n(\mathbb{Z}) \Rightarrow$ e'values of A are in $\mathbb{A}$, since the char. poly. is monic.

Lemma 6.1.5: Let $y \in \mathbb{C}$. Then $y \in \mathbb{A}$ iff $\exists n \exists y_1, \dots, y_n \in \mathbb{C}$ not all zero s.t.

$$y y_i = \sum_{j=1}^{n} A_{ij} y_j, \quad \forall i,$$

where $A_{ij} \in \mathbb{Z}$. That is, y is an e'value of some $A \in M_n(\mathbb{Z})$.

Prof: $\Leftarrow$ is 6.1.3.

$\Rightarrow$ Suppose $f(y) = 0$ where

$f(z) = z^n + a_{n-1} z^{n-1} + \cdots + a_0$,

$a_i \in \mathbb{Z}$. Consider

$$A = \begin{bmatrix} 0 & & & 0 & -a_0 \\ -1 & 0 & & & -a_1 \\ & -1 & \ddots & & \vdots \\ & & \ddots & 0 & \vdots \\ 0 & & & -1 & -a_{n-1} \end{bmatrix} \quad n \times n$$

The char. poly of A is f.

So y is an e'value of A. □

Cor 6.1.6: $\mathbb{A}$ is a subring of $\mathbb{C}$.

Prof: • $0, 1 \in \mathbb{A}$

• $y \in \mathbb{A} \Rightarrow -y \in \mathbb{A}$.

• $y, y' \in \mathbb{A}$. WTS $y + y' \in \mathbb{A}$.

$\exists y_1, \dots, y_n$, $y_1', \dots, y_n'$ as in 6.1.5:

$$y y_i = \sum_j A_{ij} y_j, \quad y' y_k' = \sum_\ell A'_{k\ell} y_\ell'$$

Consider $y_i y_k'$ as i, k vary.

$$(y + y') y_i y_k' = y y_i y_k' + y' y_i y_k'$$

$$= \sum_j A_{ij} y_j y_k' + \sum_\ell A'_{k\ell} y_i y_\ell'$$

So $y + y' \in \mathbb{A}$, by 6.1.5.

• closure under mult. similar. □