## Applications I: A version of Lagrange's thm. for representations

04.11.2019

Recall Lagrange's thm. for (finite) gps. Here we will prove a similar statement for reps (of fin. gps).

We start by recalling algebraic integers.

**Def 1.** A cplx. number $\alpha$ is said to be an <u>alg. integer</u> if it is a root of a <u>monic</u> poly. with <u>int.</u> coefficients, i.e. there is a poly. $p(z) = z^n + a_{n-1}z^{n-1} + \dots + a_0$, $a_i \in \mathbb{Z}$, $p(\alpha) = 0$.

Ex. 1) Roots of integers ($z^n = m$, $p(z) = z^n - m$)

2) Eigenvalues of <u>int.</u> matrices. By def EV are the roots of the char. poly. $p_A(z) = \det(zI - A) \leftarrow$ integral poly.

Q: Is $\frac{2}{3}$ an alg. int? No. ($p(z) = 3z - 2$ but it's not monic)

**Prop 2.** A rational number is an alg. int. iff it is an integer.

Pf: clearly int $\Rightarrow$ alg. int. Let $r = \frac{m}{n}$, $(m,n) = 1$. If $r$ is a root of $z^k + a_{k-1}z^{k-1} + \dots + a_0$ then $0 = \left(\frac{m}{n}\right)^k + a_{k-1}\left(\frac{m}{n}\right)^{k-1} + \dots + a_0 \Rightarrow m^k = -n(a_{k-1}m^{k-1} + \dots + a_1 m n^{k-2} + a_0 n^{k-1})$

$\Rightarrow n \mid m^k \overset{(m,n)=1}{\Rightarrow} n = \pm 1$ and $r = \pm m \in \mathbb{Z}$. $\blacksquare$

We will next show that the set $A$ of alg. int. is a subring of $\mathbb{C}$.

**Lemma 3.** (Characterisation of alg. integers) A number $y \in \mathbb{C}$ is an alg. int. $\Leftrightarrow$ $\exists y_1, \dots, y_t \in \mathbb{C}$, not all zero, s.t.

$$y y_i = \sum_{j=1}^{t} a_{ij} y_j, \quad a_{ij} \in \mathbb{Z}, \quad \forall 1 \le i \le t. \qquad (*)$$

Pf: $\Rightarrow$) If $y$ is a root of $p(z) = z^n + a_{n-1}z^{n-1} + \dots + a_0$ we can just take $y_i = y^{i-1}$, $1 \le i \le n-1$. Then

$$y y_i = \begin{cases} y^i = y_{i+1} & \text{for } i \le n-2 \\ -a_0 - \dots - a_{n-1} y^{n-1} & \text{for } i = n-1 \end{cases}$$

$\Leftarrow$) Supp. $(*)$ holds. Let $A = (a_{ij})$, $Y = \begin{bmatrix} y_1 \\ \vdots \\ y_t \end{bmatrix} \in \mathbb{C}^t$. Then

$[AY]_i = \sum_{j=1}^{t} a_{ij} y_j = y y_i = y[Y]_i$ so $AY = yY \Rightarrow y$ is an EV of $A$ (int. matr.) so from Ex 2) we get that $y \in A$. $\blacksquare$

Cor 4. The set $A$ of alg. int. is a subring of $\mathbb{C}$.

Pf: Clearly, $A$ is closed under taking negatives.
($\alpha \in A \Rightarrow \exists p(x), p(\alpha)=0 \Rightarrow -\alpha$ root of $p(-z)$ or $-p(-z)$ )

$y, y' \in A \Rightarrow y y_i = \sum_{j=1}^{t} a_{ij} y_j, \quad y' y'_k = \sum_{k=1}^{s} b_{kj} y'_j$

$\Rightarrow (y+y') y_i y'_k = \sum_{j=1} a_{ij} y_j + \sum_{k=1}^{s} b_{kj} y'_j \in A$ & $(y \cdot y') y_i y'_k = \sum_{j=1}^{m} c_j y_j \in A$.

∎

Cor 5. Let $\chi$ be the character of a f.g $G$. Then $\chi(g)$ is an alg. int. for all $g \in G$.

Pf: Let $|G|=n$ and $\varphi: G \to GL_m(\mathbb{C})$ a rep with char. $\chi$.

$g^n = 1 \Rightarrow \varphi_g^n = I \xRightarrow{\text{prop from a previos talk}} \cancel{\varphi_g \ldots} \Rightarrow$ EV of $\varphi_g$ are roots of unity $\xRightarrow{\text{Ex 1)}}$ they are alg. integers $\lambda_1, \ldots, \lambda_m$

Now, $\chi(g) = \mathrm{Tr}(\varphi_g) = \lambda_1 + \ldots + \lambda_m$, thus $\chi(g) \in A$ (since $A$ is a ring).

Rmk. $\chi(g)$ is a sum of roots of unity. ∎

Thm 6 (Technical) Let $\varphi$ be an irrep. of a f.g $G$ of deg $d$. Then $\dfrac{h \chi_\varphi(g)}{d}$ is an alg. integer, where $h = |C_g|$, $g \in G$.

Pf: Let $C_1, \ldots, C_s$ be conj. classes of $G$., $h_i = |C_i|$, $\chi_i = \chi_\varphi|_{C_i}$.

Claim 1. The op. $T_i = \sum_{x \in C_i} \varphi_x$ satisfies $T_i = \dfrac{h_i}{d} \chi_i I$.

Pf: First note that

$$\varphi_g T_i \varphi_{g^{-1}} = \sum_{x \in C_i} \varphi_g \varphi_x \varphi_{g^{-1}} = \sum_{x \in C_i} \varphi_{gxg^{-1}} = \sum_{y \in C_i} \varphi_y = T_i$$

making $T_i$ an intertwiner. Thus, from Schur $T_i = \lambda \cdot I$

$\lambda \in \mathbb{C}$. Now, we find $\lambda$ from

$d\lambda = \mathrm{Tr}(\lambda I) \overset{\text{J-W and } G}{=} \mathrm{Tr}(T_i) = \sum_{x \in C_i} \mathrm{Tr}(\varphi_x) = \sum_{x \in C_i} \chi_\varphi(x) = \sum_{x \in C_i} \chi_i = |C_i| \chi_i$

$= h_i \chi_i \Rightarrow \lambda = \dfrac{h_i \chi_i}{d}$.

Claim 2: $T_iT_j = \sum_{k=1}^{s} a_{ijk} T_k$ f.s. $a_{ijk} \in \mathbb{Z}$. (analogous to (*))

Pf: $T_iT_j = \sum_{x\in C_i} e_x \sum_{y \in C_j} e_y = \sum_{x,y\in C_i} e_x e_y = \sum_{g\in G} a_{ijg} e_g$,

where $a_{ijg} \in \mathbb{Z}$ is the number of ways to write $g = xy$ with $x \in C_i$, $y \in C_j$.

Subclaim: $a_{ijg}$ depends only on the conj.-class of $g$. Indeed, let $X_g = \{(x,y) \in C_i \times C_j \mid xy = g\}$ i.e $a_{ijg} = |X_g|$

Let $g'$ be in the same conj.-class as $g$, i.e. $g' = kgk^{-1}$.

We define a bijection $\varphi: X_g \to X_{g'}$ by

$$(x,y) \mapsto (kxk^{-1}, kyk^{-1})$$

Note that $kxk^{-1} \in C_i$, $kyk^{-1} \in C_j$, $(kxk^{-1})(kyk^{-1}) = kgk^{-1} = g'$

so $\varphi(x,y) \in X_{g'}$ and $\varphi$ has inverse $\phi: X_{g'} \to X_g$
$(x',y') \mapsto (k^{-1}x'k, k^{-1}y'k)$

so, $\varphi$ is indeed a bijection meaning $|X_g| = |X_{g'}|$

$\Rightarrow a_{ijg} = a_{ijg'} \Rightarrow a_{ijg}$ only depends on c.class of $g$.

Back to Claim 2: (we have $s$-conj.classes) $T_iT_j = \sum_{g\in G} a_{ijg} e_g = \cancel{\sum_{k=1}^{s} a_{ijk} \sum_{g\in G} a_{ijg} e_g} =$

$= \sum_{k=1}^{s} a_{ijk} \sum_{g\in C_k} e_g = \sum_{k=1}^{s} a_{ijk} T_k$.

Back to thm: Claim (1) & Claim (2) $\Rightarrow$

$$\left(\frac{h_i}{d}\chi_i\right)\left(\frac{h_j}{d}\chi_j\right) = \sum_{k=1}^{s} a_{ijk}\left(\frac{h_k}{d}\chi_k\right) \overset{\text{lemma 3}}{\Rightarrow} \frac{h_i\chi_j}{d} \in A.$$

Thm 7 (A version of Lagrange's thm. for irreps AKA Dimension thm)

Let $\varphi$ be an irrep of a grp. $G$ of degree $d$ (over $\mathbb{C}$). Then $d \mid |G|$.

Pf: As before, let $C_1 \dots C_s$ be c.c. and $\chi_i = \chi_{\varphi}|_{C_i}$, $h_i = |C_i|$

$\varphi$ irrep $\Rightarrow 1 = \langle \chi_\varphi, \chi_\varphi \rangle = \frac{1}{|G|}\sum_{g\in G} \chi_\varphi(g)\overline{\chi_\varphi(g)}$

$\Rightarrow \frac{|G|}{d} = \sum_{g\in G} \frac{\chi_\varphi(g)}{d}\overline{\chi_\varphi(g)} = \sum_{i=1}^{s} \sum_{g\in C_i} \left(\frac{1}{d}\chi_i\right)\overline{\chi_i} = \sum_{i=1}^{s}\left(\frac{h_i}{d}\chi_i\right)\overline{\chi_i}$

$\in A$ from thm 6 & Cor 4 & closure of $A$ under cpl. conj.

So, $\frac{|G|}{d} \in \mathbb{A}$ which together with Prop 2 gives $d \mid |G|$.

Important: Dim. thm. combined with Maschke are very useful for listing irreps of f.gps!

<u>Next time:</u> As a Cor of Thm 7: gps of order $p^2$ with $p$ prime are abelian!

PS: The dims of irreps of $G$ can be $1, p$ or $p^2$.

Maschke $\Rightarrow p^2 = |G| = d_1^2 + \dots + d_s^2$, with $d_1 = \dim \underset{\text{triv. rep}}{\mathbb{C}} = 1$

$\Rightarrow d_2 = \dots = d_s = 1 \Rightarrow$ <u>$G$ abelian</u>.

# Applications II: Burnside's theorem

11.11.2019

Burn. thm was proved by Burnside in 1904 using rep. theory. Proofs avoiding rep. theory happened only in 1970 - 1973.

<u>Recall</u>. The commutator subgp. $G'$ of $G$ is the subgp. gen by el. $g^{-1}h^{-1}gh$ with $g,h \in G$. We have: $G' \trianglelefteq G$ and if $N \trianglelefteq G$ is s.t. $G/N$ is ab. then $G' \subseteq N$ ($G'$ is „minimal")

<u>Lemma 1.</u> Let $G$ be a fin. gp. Then the number of deg one reps of $G$ divides $|G|$. Moreover, if $G'$ is the comm. subgp. of $G$, then there is a bijection between degree one reps. of $G$ and irreps of the <u>ab</u> gp. $G/G'$. Thus, $G$ has $|G/G'| = [G:G']$ deg. one reps.

Pf: Let $\pi: G \to G/G'$, $\pi(g) = gG'$ be the proj. and $\psi: G/G' \to \mathbb{C}^*$ an irrep. of $G/G'$.
Then $\psi\pi: G \to \mathbb{C}^*$ is a deg one rep. of $G$

Now, let $\rho: G \to \mathbb{C}^*$ be a deg. one rep. Then $\operatorname{im}\rho \subset \mathbb{C}^*$ is ab. i.e. $\operatorname{im}\rho \cong G/\ker\rho$ is ab $\overset{G' \text{ comm.}}{\Longrightarrow}$ $G' \subseteq \ker\rho$.
Define $\psi: G/G' \to \mathbb{C}^*$ by $\psi(gG') = \rho(g)$ ($\rho = \psi\pi$)
well def: $gG' = hG' \Rightarrow h^{-1}g \in G' \subseteq \ker\rho \Rightarrow \rho(h^{-1}g) = 1$
$\Rightarrow \rho(h) = \rho(g)$
homo: $\psi(gG' \cdot hG') = \psi(ghG') = \psi(gG')\psi(hG')$.
(ab. gp $G/G'$ has $|G/G'|$ irreps ) ☒

<u>Cor 2.</u> Let $p, q$ be primes, $p<q$, $q \not\equiv 1 \bmod p$. Then any gp. $G$ of order $pq$ is abelian.

Pf: We know by Masche & dim. thm that the degs $d_i$ of irreps of $G$ satisfy $d_i \mid |G|$ & $pq = |G| = \sum_{i=1}^{s} d_i^2$.
$\Rightarrow$ we can have $d_i = 1$ and/or $p$.
Let $m = \#$ deg 1 irreps, $n = \#$ deg $p$ irreps. Then from $pq = m + np^2$ $\overset{m \geq 1,\ p \mid m}{\Longrightarrow}$ $m = p$ or $m = pq$ $\overset{q \not\equiv 1 \bmod p}{\Longrightarrow}$ $m = pq$
We have only deg 1 irreps $\Rightarrow$ $G$ ab. ☒

Recall: Last time we said that if $\varphi: G \to Gl_d(\mathbb{C})$ is an map, $|G|=n$ then $\chi_\varphi(g)$ is a sum of $d$ $n^{th}$ roots of unity.

Lemma 3. Let $\lambda_1, \dots, \lambda_d$ be $n^{th}$ roots of unity. Then $|\lambda_1 + \dots + \lambda_d| \leq d$ with eq iff $\lambda_1 = \dots = \lambda_d$

Pf: Basic property of norm.

$(\|v+w\|^2 = \|v\|^2 + 2\langle v,w\rangle + \|w\|^2 = \|v\|^2 + 2\|v\|\cdot\|w\|\cos\theta + \|w\|^2)$ $v,w \in \mathbb{R}^2$

with eq iff $\theta = 0$.

Brief intro to Galois theory

Let $w_n = e^{\frac{2\pi i}{n}}$ (root of unity). Let $\mathbb{Q}[w_n]$ be the smallest subfield $F$ of $\mathbb{C}$ where $z^n - 1 = (z-\alpha_1)\dots(z-\alpha_n)$ s.t. $\alpha_1, \dots, \alpha_n \in F$. ($F$ splitting field of $z^n-1$).

Recall the Euler function $\phi(n) = \#$ pos. integers $\leq n$ that are relatively prime to $n$.

$\Gamma = Gal(\mathbb{Q}[w_n]:\mathbb{Q}) = \{\sigma \in Aut(\mathbb{Q}[w_n]) \mid \sigma(r) = r, \forall r \in \mathbb{Q}\}$

Lemma 4. $\dim_{\mathbb{Q}} \mathbb{Q}[w_n] = \phi(n)$ ($\mathbb{Q}[w_n]$ is a $\mathbb{Q}$-v.s)

Pf. Ommited. But actually $\dim \mathbb{Q}[w_n] < \infty$ since $w_n \in A$.

Then $|\Gamma| = \phi(n)$ since $\mathbb{Q}[w_n]$ is a sp. field of $z^n - 1$.

Lemma 5. Let $p(z)$ be a poly with rational coeff. and supp. $\alpha \in \mathbb{Q}[w_n]$ is a root of $p$. Then $\sigma(\alpha)$ is also a root of $p$ for all $\sigma \in \Gamma$.

Pf: $p(z) = a_k z^k + a_{k-1} z^{k-1} + \dots + a_0$, $a_i \in \mathbb{Q}$, $p(\alpha) = 0$.

$p(\sigma(\alpha)) = a_k \sigma(\alpha)^k + \dots + a_0 \overset{\sigma(a_i) = a_i}{=} \sigma(a_k \alpha^k + \dots + a_0) \overset{*}{=} \sigma(0) = 0$.

Direct corollaries:

Cor 6. Let $\alpha$ be an $n^{th}$ root of unity. Then $\sigma(\alpha)$ is also an $n^{th}$ root of unity. (take $z^n - 1$)

Cor 7. Let $\alpha \in \mathbb{Q}[w_n]$ be an alg int and $\sigma \in \Gamma$. Then $\sigma(\alpha)$ is an alg. int. ($\alpha$ root of int. mon. poly $\overset{LM5}{\Rightarrow}$ so is $\sigma(\alpha)$)

Thm 8 (w/o proof) Let $\alpha \in \mathbb{Q}[w_n]$. Then $\sigma(\alpha) = \alpha$ for all $\sigma \in \Gamma$ iff $\alpha \in \mathbb{Q}$.

**Cor 9.** Let $\alpha \in \mathbb{Q}[\omega_n]$. Then $\prod_{\sigma\in\Gamma} \sigma(\alpha) \in \mathbb{Q}$.

Pf: Let $\tau \in \Gamma$. Then

$$\tau\left(\prod_{\sigma\in\Gamma}\sigma(\alpha)\right) = \prod_{\sigma\in\Gamma} \tau\sigma(\alpha) \overset{\text{put } \rho=\tau\sigma}{=} \prod_{\rho\in\Gamma} \rho(\alpha)$$

So, $\prod_{\sigma\in\Gamma}\sigma(\alpha)$ is fixed by $\tau\in\Gamma \overset{\text{thm 7}}{\Rightarrow} \prod \sigma(\alpha) \in \mathbb{Q}$. ∎

**Thm 10.** (Technical) Let $G$ be a group of order $n$ and let $C$ be a conj. class of $G$. Supp. that $\varphi: G \to GL_d(\mathbb{C})$ is an irrep. and $h = |C|$ is relatively prime to $d$. Then either:

1. there exist $\lambda \in \mathbb{C}^*$ s.t. $\varphi_g = \lambda \mathrm{Id}$, $\forall g \in C$; or
2. $\chi_\varphi(g) = 0$, $\forall g \in C$.

Pf: since $\chi_\varphi(g)$ is a class fct. it suffices to show that if $\varphi_g \neq \lambda \mathrm{Id}$ f.s. $g\in G$ then $\chi_\varphi(g) = 0$.

Last talk $\Rightarrow$ $\chi_\varphi(g)$ and $\frac{h\chi(g)}{d}$ are algebraic integers.
$(g,h)=1 \Rightarrow \exists k, j \in \mathbb{Z}$ s.t. $kh + jd = 1$. Look at:

$$\alpha = k\left(\frac{h\chi(g)}{d}\right) + j\chi(g) = \frac{kh+jd}{d}\chi(g) = \frac{\chi(g)}{d} \Rightarrow \alpha \in \mathbb{A}$$

Since $\varphi_g$ is diag. with EV $\lambda_1, \dots, \lambda_d$ $n^{th}$ roots of unity then $\lambda_1, \dots, \lambda_d$ are not all equal so $|\lambda_1 + \dots + \lambda_d| < \sum |\lambda_i| = d$

So, $|\alpha| = \left|\frac{\chi(g)}{d}\right| < 1$

On the other hand, $\alpha \in \mathbb{Q}[\omega_n]$ $\left[\alpha = \frac{\chi(g)}{d} = \frac{\lambda_1 + \dots + \lambda_d}{d}\right.$ as a lin. comb of $n^{th}$ roots of unity $\left.\right]$

Let $\sigma \in \Gamma = \mathrm{Gal}(\mathbb{Q}[\omega_n]:\mathbb{Q}) \overset{\text{cor 7}}{\Rightarrow} \sigma(\alpha) \in \mathbb{A}$
Similarly,
$\sigma(\chi(g)) = \sigma(\lambda_1) + \dots + \sigma(\lambda_d) = \lambda_1' + \dots + \lambda_d'$ ← also sum of roots of unity not all equal

$$\Rightarrow |\sigma(\alpha)| = \left|\frac{\sigma(\chi(g))}{d}\right| < 1$$

Then $q = \prod_{\sigma\in\Gamma} \sigma(\alpha) \in \mathbb{A}$ (ring) and $|q| = \left|\prod_{\sigma\in\Gamma}\sigma(\alpha)\right| = \prod_{\sigma\in\Gamma}|\sigma(\alpha)| < 1$
On the other hand
From cor 9 $q \in \mathbb{Q}$ $\overset{\text{last talk}}{\Rightarrow}$ $q \in \mathbb{Z}$ and since $|q| < 1$ then $q = 0 \Rightarrow \sigma(\alpha) = 0$ f.s. $\sigma$ $\overset{\sigma \text{ autom.}}{\Rightarrow} \alpha = 0$ ∎

**Lemma 11** (technical) Let $G$ be a fin. non-ab. gp. Supp. $\exists$ a conj. class $C \neq \{1\}$ s.t. $|C| = p^t$ with $p$ prime $, t \geq 0$. Then $G$ is not simple.

Pf: Assume $G$ is ~~not~~ simple and let $\varphi^{(1)}, \dots, \varphi^{(s)}$ be ~~the~~ a complete set of representatives of eq. classes of irreps. with characters $\chi_1, \dots, \chi_s$ and degrees $d_1, \dots, d_s$.
w.l.o.g $\varphi^{(1)}$ = triv. rep. Now, for $k>1$ since $\ker \varphi^{(k)} \trianglelefteq G$ and $G$ simple either $\ker \varphi^{(k)} = \{1\}$ or $\ker \varphi^{(k)} = G$. But the latter implies $\varphi^{(k)}$ = triv. rep. So, $\ker \varphi^{(k)} = \{1\}$ and $\varphi^{(k)}$ is inj, $k>1$. Thus since $G$ is non-ab and $\mathbb{C}^*$ is ab, we must have $d_k > 1$, for $k>1$.
Moreover, since $G$ is simple, non-ab $Z(G) = 1$ and $t > 0$.
Let $g \in C$, $k > 1$ and let $Z_k = \{x \in G \mid \varphi_x^{(k)} \text{ is a scalar mat.}\}$ ($\lambda \cdot \mathrm{Id}$, $\lambda \in \mathbb{C}^*$)
Let $H = \{\lambda I_{d_k} \mid \lambda \in \mathbb{C}^*\}$. Then $H \leq GL_{d_k}(\mathbb{C})$ contained in the center so it's normal. ~~But~~ $\varphi^{(k)}(Z_k) = H$ so $Z_k$ must be a normal subgp. of $G \overset{d_k > 1}{\Longrightarrow} Z_k \neq G \Rightarrow Z_k = \{1\}$ by def of $Z_k$ & $H$.
Now, assume $p \nmid d_k$ ($(p, d_k) = 1$); then $\chi_k(g) = 0$ by thm 10. ($\varphi^{(k)}$ doesn't act by scalar on $C$)
Let $L$ be the reg. rep. of $G$.
Recall that $L \cong d_1\varphi^{(1)} \oplus \dots \oplus d_s\varphi^{(s)}$ and $\chi_L(g) = \begin{cases} |G|, & g=1 \\ 0, & g \neq 1 \end{cases}$
since $g \neq 1$ ($g \in C$, $|C| = p^t$, $t>0$) we have:

$$0 = \chi_L(g) = d_1\chi_1(g) + \dots + d_s\chi_s(g) = 1 + \sum_{k=2}^{s} d_k\chi_k(g) =$$

$$= 1 + \sum_{p \mid d_k} d_k \chi_k(g) = 1 + pz \quad \text{, where } z \in A.$$

So, $\frac{1}{p} = -z \in A \overset{\text{last talk}}{\Rightarrow} \frac{1}{p} \in \mathbb{Z}$ ↯.

**Thm 12.** (Burnside) Let $G$ be a gp of order $p^a q^b$, $p, q$ primes. Then $G$ is not simple unless it is cyclic of prime order.

Pf: We can assume $G$ is non ab. [Claim: an ab. gp is simple iff cyclic of prime order]

Pf of claim: $\Rightarrow$) $g \in G \setminus \{1\}$, $\langle g \rangle \subseteq G \Rightarrow \langle g \rangle = G$
Sup $|G| = m \cdot n$, $m > 1$, $n > 1$. Then $\langle g^m \rangle \trianglelefteq G$ ↯ $\Rightarrow |G|$ prime.

$\Leftarrow)$ $|G|=p$, $G$ ab., $g \in G \setminus \{1\}$

since $|\langle g\rangle| \,\big|\, |G| \overset{g\neq 1}{\Rightarrow} |\langle g\rangle| = p \Rightarrow G = \langle g\rangle \Rightarrow G$ ab. and

$\forall H \trianglelefteq G$ has ord. $1$ or $p \Rightarrow H=\{1\}$ or $H=G \Rightarrow G$ simple.

Back to thm: We can assume that $G$ is not ab.

Fact from gp.-theory: Gps of prime order have non-triv centers $\boxed{\text{If } G = Z(G)}$ ✓. If $G \neq Z(G)$ from class eq.

$$|G| = |Z(G)| + \underbrace{\sum_{i=1}^{r} |G : C_G(g_i)|}_{\text{conj. class}}$$

centralizer of $g_i$

$g_i \notin Z(G) \Rightarrow C_G(g_i) \underset{\text{proper}}{<} G \Rightarrow p \mid |G : C_G(g_i)|$ and since $p \mid |G|$, $p \mid Z(G)$

$\Rightarrow Z(G) \neq \{1\}$ ┘

Now if $a$ or $b$ is zero we are done. Otherwise, for $a, b \geq 1$ from Sylow's thm, $G$ has a subgp. $H$ of order $q^b$.

Let $1 \neq g \in Z(H)$ and let $N_G(g) = \{x \in G \mid xg = gx\}$ be the normalizer in $G$. Then $H \subseteq N_G(g)$ since $g \in Z(H)$.

Thus, $p^a = [G:H] = [G : N_G(g)][N_G(g) : H]$ so

$[G : N_G(g)] = p^t$ s.s. $t \geq 0$. But $|[G : N_G(g)]| = |C_g|$ conj. class of $g$

$\overset{\text{lemma 11}}{\Longrightarrow}$ $G$ is not simple.

∎

Eg: All gps of order $p^a q^b$ where $p, q$ are primes are solvable

Def. A gp. is solvable if it has a subnorm. series i.e. $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_k = G$, $G_{j-1} \trianglelefteq G_j$, $G_j / G_{j-1}$ ab

┘

# Applications III: Group actions and Permutation reps. 18.11.19

Today we continue the anology of gps and their linear shadows, gp. reps.

$S_X$ = symm. gp on the set $X$.

Recall the following:

**Def 1.** An action of a gp $G$ on a set $X$ is a homomorphism $\sigma: G \to S_X$. The cardinality of $X$ is called the degree of the action.

**Ex.** Define $\lambda: G \to S_G$ by $\lambda_g(x) = gx$. This is the regular action on $G$.

**Def 2.** Let $\sigma: G \to S_X$ be a gp. action. The orbit of $x \in X$ under $G$ is the set $G \cdot x = \{\sigma_g(x) \mid g \in G\}$.

**Rmk.**

**Def 3** A gp. action $\sigma: G \to S_X$ is transitive if $\forall x, y \in X$ there exists $g \in G$ s.t. $\sigma_g(x) = y$, i.e. iff there is just one orbit of $G$ on $X$. (Every el. $y \in X$ can be written as $\sigma_g(x) = y$, for some $g \in G$, $x \in X$)

**Ex.** If $G$ is a gp. and $H$ is a subgp. then the action $\sigma: G \to S_{G/H}$ given by $\sigma_g(xH) = gxH$ is transitive.
(If $xH, yH \in G/H$ then $\sigma_{yx^{-1}}(xH) = yH$ )

Now we define a more general property than transitive

**Def 4.** An action $\sigma: G \to S_X$ of $G$ on $X$ is 2-transitive if for any two distinct ~~pts~~ elements $x, y \in X$, $x', y' \in X$, there exists $g \in G$ s.t. $\sigma_g(x) = x'$ and $\sigma_g(y) = y'$.

**Ex.** The action of $S_n$ on $\{1, \dots, n\}$ for $n \geq 2$ is 2-trans.
Pf: Look at $X = \{1, \dots, n\} \setminus \{i, j\}$, $Y = \{1, \dots, n\} \setminus \{k, \ell\}$. $i \neq j$, $k \neq \ell$
Then $|X| = |Y| = n-2$ and we can choose a bij. $f: X \to Y$. Define an el. $\sigma \in S_n$ by

$$\sigma(m) = \begin{cases} k &, m=i \\ \ell &, m=j \\ f(m) & \text{else} \end{cases}$$ (clearly well-def.)

So, for every two pairs of distinct el. $i,j$ and $k,\ell$ we found $\sigma \in S_n$ s.t. $\sigma(i)=k$, $\sigma(j)=\ell$. ⊠

<u>Def 5.</u> Let $\sigma: G \to S_X$ be a <u>trans</u>. gp. action. Define $\sigma^2: G \to S_{X\times X}$ by:

$$\sigma^2_g(x_1,x_2) = (\sigma_g(x_1), \sigma_g(x_2)) \ . \ (g\in G, x_1,x_2 \in S_X)$$

An orbit of $\sigma^2$ is called an <u>orbital</u> of $\sigma$. The number of orbitals is called the <u>rank</u> of $\sigma$.

<u>Rmk</u> From transitivity of $\sigma$ we have that $\Delta = \{(x,x) \in X\times X\}$ is an orbital (diagonal orbital)

<u>Prop 6</u> (Characterisation of 2-transitivity). Let $\sigma: G \to S_X$ be a gp. action with $|X| \geq 2$. Then $\sigma$ is 2-transitive iff it is transitive with $\operatorname{rank}(\sigma) = 2$.

Pf: First we show that 2-trans $\Rightarrow$ trans.
$\sigma$ is 2-trans. $\Rightarrow$ $\forall x,y \in X$, $x',y' \in X$ $(x\neq x', y \neq y')$ there exists $g \in G$ s.t. $\sigma_g(x)=y$, $\sigma_g(x')=y'$ $\Rightarrow$ $\sigma$ trans.
Now we find out under which conditions is a trans. action 2-transitive. We know that $\Delta$ is always an orbital. We look at its complement $(X\times X)\setminus\Delta = \{(x,y) \mid x \neq y\}$. This is an orbital iff for any two pairs of distinct el. $x \neq y$, $x' \neq y'$ there exists $g \in G$ s.t. $\sigma_g(x) = x'$, $\sigma_g(y) = y'$, i.e. $\sigma$ is 2-transitive.

[Look at an orbit of $(x,y)$ under $\sigma^2$
$G(x,y) = \{\sigma^2_g(x,y) \mid g \in G\} = \{(\sigma_g(x), \sigma_g(y)) \mid g \in G\}$
This is an orbital iff $\sigma_g(x) = x'$, $\sigma_g(y) = y'$, $x' \neq y'$ f.s. $g \in G$.]

<u>Def 7.</u> Let $\sigma: G \to S_X$ be a gp. action. Then we define $\operatorname{Fix}(g) := \{x \in X \mid \sigma_g(x) = x\}$, the <u>fixed points of $g$ on $X$</u>.

For the set of fixed points of $g$ on $X \times X$ we have:

<u>Prop 8.</u> $Fix^2(g) = Fix(g) \times Fix(g)$ and consequently $|Fix^2(g)| = |Fix(g)|^2$.

Pf: For $(x,y) \in X \times X$ and $\sigma^2_g(x,y) = (\sigma_g(x), \sigma_g(y))$ we have

$(x,y) = \sigma^2(x,y)$ iff $\sigma_g(x) = x$ and $\sigma_g(y) = y$, i.e. $Fix^2(g) = (Fix(g))^2$. ∎

Now we <u>linearise</u> group actions, i.e. we build up representations from gp. actions

<u>Def 9.</u> Let $\sigma : G \to S_X$ be a gp. action. We define a rep

$$\tilde{\sigma} : G \to GL(\mathbb{C}X) \text{ by } \tilde{\sigma}_g\Big(\sum_{x\in X} c_x x\Big) = \sum_{x \in X} c_x \sigma_g(x) = \sum_{y \in Y} c_{\sigma_{g^{-1}}(y)}\, y.$$

This is called the <u>permutation rep</u> assoc. to $\sigma$.

<u>Rmk 10.</u> The map $\tilde{\sigma}$ is the lin. extension to $\mathbb{C}X$ of the map defined on its basis $X$ given by $x \mapsto \sigma_g(x)$.

Also, deg. of $\tilde{\sigma}$ = deg. of gp. action $\sigma$.

<u>Ex.</u> For the regular action $\lambda : G \to S_G$ we obtain $\tilde{\lambda} = L$ the regular rep.

<u>Prop. 11.</u> Let $\sigma : G \to S_X$ be a gp. action. Then the perm. rep. $\tilde{\sigma} : G \to GL(\mathbb{C}X)$ is a unitary rep. of $G$.

Pf: See the proof for the reg. rep. from talk VI.

$$\ulcorner \Big\langle \sum_{x\in X} c_x \sigma_g(x), \sum_{y \in Y} c_y \sigma_g(y) \Big\rangle = \Big\langle \sum_{z \in X} c_{\sigma^{-1}_g(z)}\, z, \sum_{w \in Z} c_{\sigma^{-1}_g(w)}\, w \Big\rangle = \sum_{x\in X} c_{\sigma^{-1}_g(x)} \times \overline{c_{\sigma^{-1}_g(x)}}$$

$$= \Big\langle \sum_{x \in X} c_x x, \sum_{y \in Y} c_y y \Big\rangle. \quad \lrcorner$$

Now we see that the characters of permutation reps. are nice.

**Prop 12.** Let $\sigma : G \to S_X$ be a gp. action. Then

$$\chi_{\tilde\sigma}(g) = |Fix(g)|$$

Pf: Let $X = \{x_1, \dots, x_n\}$ and $[\tilde\sigma_g]$ be the matrix of $\tilde\sigma$ w.r.t this basis. Then $\tilde\sigma_g(x_j) = \sigma_g(x_j)$ so

$$[\tilde\sigma_g]_{ij} = \begin{cases} 1, & x_i = \sigma_g(x_j) \\ 0 & \text{else} \end{cases}$$ and in part.

$$[\tilde\sigma_g]_{ii} = \begin{cases} 1, & x_i = \sigma_g(x_i) \\ 0, & \text{else} \end{cases} = \begin{cases} 1, & x_i \in Fix(g) \\ 0, & \text{else} \end{cases}$$

so, $\chi_{\tilde\sigma}(g) = Tr([\tilde\sigma_g]) = |Fix(g)|$. ☐

Now we see that like regular reps, the permutation reps are also reducible.

**Def 13.** Let $\varphi : G \to GL(V)$ be a rep. Then

$V^G = \{v \in V \mid \varphi_g(v) = v, \forall g \in G\}$ is the fixed subspace of G

**Prop 14.** Let $\varphi: G \to GL(V)$ be a rep and $\chi_1$ the trivial char. Then $\langle \chi_\varphi, \chi_1 \rangle = \dim V^G$.

Pf: Let $V = m_1 V_1 \oplus \dots \oplus m_s V_s$ where $V_i$'s are irred. G-inv. subspaces and $m_i$'s are their multiplicities. The associated subrepresentations of $V_i$'s also range over distinct eq. classes of irreps of G.

w.l.o.g $V_1 = \mathbb{C}$ triv. rep. Let $\varphi^{(i)} = \varphi|_{V_i}$ and let $v = v_1 + \dots + v_s \in V$ with $v_i \in m_i V_i$ and

$\varphi_g v = (m_1 \varphi^{(1)})_g v_1 + \dots + (m_s \varphi^{(s)}_g) v_s = v_1 + (m_2 \varphi^{(2)})_g v_2 + \dots + (m_s \varphi^{(s)})_g v_s$.

Thus, $v \in V^G$ iff $v_i \in m_i V_i^G$, $2 \le i \le s$, i.e.

$V^G = m_1 V_1^G + \dots + m_s V_s^G$. Since $V_i$'s are irreducible not eq. to ~~$\mathbb{C}$~~ the triv. rep. we must have $V_i^G = 0$ $i \ge 2$. Thus, $V^G = m_1 V_1$ and $m_1 = \dim V^G$.

**Prop 15.** Let $\sigma : G \to S_X$ be a group action and let $O_1, \dots, O_m$ be the orbits of $G$ on $X$. Then $v_i = \sum_{x \in O_i} x$, where $1 \le i \le m$ is a basis for $\mathbb{C}X^G$ meaning $\dim \mathbb{C}X^G = \#\text{orbits of } G \text{ on } X$.

Pf: $\tilde{\sigma}_g v_i = \sum_{x \in O_i} \sigma_g(x) = \sum_{y \in O_i} y = v_i. \Rightarrow v_1, \dots, v_m \in \mathbb{C}X^G$.

Then $\langle v_i, v_j \rangle = \begin{cases} |O_i| , & i = j \\ 0 , & i \neq j \end{cases}$ since orbits are disjoint.

So, $\{v_1, \dots, v_m\}$ is a set of orthogonal non-zero vectors in $\mathbb{C}X^G$, so it is lin. indep.

Now, supp $v = \sum_{x \in X} c_x x \in \mathbb{C}X^G$. Let $z \in G \cdot y$, i.e. $z = \sigma_g(y)$. Then

$$\sum_{x \in X} c_x x = v = \tilde{\sigma}_g v = \sum_{x \in X} c_x \sigma_g(x)$$

Since $z = \sigma_g(y)$ the coeff of $z$ in LHS is $c_z$ and its coeff. in the RHS is $c_y$. Thus, we must have $c_z = c_y$. So, there are cplx numbers ~~that~~ $c_1, \dots, c_m$ s.t. $c_x = c_i \ \forall x \in O_i$ and

$$v = \sum_{x \in X} c_x x = \sum_{i=1}^{m} \sum_{x \in O_i} c_x x = \sum_{i=1}^{m} c_i \sum_{x \in O_i} x = \sum_{i=1}^{m} c_i v_i .$$

meaning, $v_1, \dots, v_m$ span $\mathbb{C}X^G$.

$\boxtimes$

**Rmk 16.** Since $G$ always has at least one orbit we have ~~that~~ the triv. rep always appears as a summand in $\tilde{\sigma}$, i.e. for $|X| > 1$, $\tilde{\sigma}$ is <u>not</u> irreducible.

**Cor 17.** (Burnside's lemma) Let $\sigma : G \to S_X$ be a gp. action and let $m = \#$ orbits of $G$ on $X$. Then

$$m = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$$

Pf:

$$m = \langle \chi_{\tilde{\sigma}}, \chi_1 \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_{\tilde{\sigma}}(g) \overline{\chi_1(g)} = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)| .$$

**Cor 18.** Let $\sigma : G \to S_X$ be a trans. gp action. Then

$$\underset{\#\text{orbit of } \sigma^2}{\underset{\parallel}{\mathrm{rank}(\sigma)}} = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|^2 = \langle \chi_{\tilde{\sigma}}, \chi_{\tilde{\sigma}} \rangle .$$

Pf: $\langle \chi_{\tilde{\sigma}}, \chi_{\tilde{\sigma}} \rangle = \frac{1}{|G|} \sum |\mathrm{Fix}(g)| |\mathrm{Fix}(g)| = \frac{1}{|G|} \sum |\mathrm{Fix}(g)|^2$.

char of perm. rep.

$= \#$ fixed pts in $X \times X$.

Now, let $\sigma : G \to S_X$ be a transitive g. action and let $v_0 = \sum_{x \in X} x$.

Since $\sigma$ has only one orbit, $\mathbb{C}X^G = \mathbb{C}v_0$ (Prop. 15)

Let $V_0 = \mathbb{C}v_0^{\perp}$. It is a $G$-inv. subspace since $\tilde{\sigma}$ is unitary.

Since $\mathbb{C}X = V_0 \oplus \mathbb{C}v_0$, we have $\chi_{\tilde{\sigma}} = \chi_{\tilde{\sigma}'} + \chi_1$, where $\tilde{\sigma}' = \tilde{\sigma}|_{V_0}$ and $\chi_1 = $ triv. char.

<u>Thm 19.</u> Let $\sigma : G \to S_X$ be a trans. gp. action. The the rep $\tilde{\sigma}'$ (called augmentation rep) is irred. iff $G$ is 2-trans. on $X$.

Pf:

$$\langle \chi_{\tilde{\sigma}'}, \chi_{\tilde{\sigma}'} \rangle = \langle \chi_{\tilde{\sigma}} - \chi_1, \chi_{\tilde{\sigma}} - \chi_1 \rangle = \langle \chi_{\tilde{\sigma}}, \chi_{\tilde{\sigma}} \rangle - \underbrace{\langle \chi_{\tilde{\sigma}}, \chi_1 \rangle}_{1} - \underbrace{\langle \chi_1, \chi_{\tilde{\sigma}} \rangle}_{1}$$

$$+ \underbrace{\langle \chi_1, \chi_1 \rangle}_{\text{irrep.}} \overset{\text{Cor 18 \& Prop 15 \& Cor 17}}{=} \operatorname{rank}(\sigma) - 1 - 1 + 1 = \operatorname{rank}(\sigma) - 1$$

So, $\tilde{\sigma}'$ is irred $\iff \operatorname{rank}(\sigma) = 2 \overset{\sigma \text{ is trans}}{\Longrightarrow} \sigma$ is 2-trans.

<u>Ex. Char. table of $S_4$.</u>

Conj. classes: Id, (12), (123), (1234), (12)(34).

$\chi_1 = $ char of triv. rep, $\chi_2 = $ char of sign rep. is

Since $S_4$ acts 2-trans on $\{1,2,3,4\}$, the augmentation rep $\alpha$ is irred. Let $\chi_4$ be its char. Then $\chi_4(g) = |\mathrm{Fix}(g)| - 1 = \chi_{\text{stand}} - \chi_1$

Let $\chi_5 = \chi_2 \cdot \chi_4$ (the char. of a new rep $d : S_4 \to GL_3(\mathbb{C})$ (3-dim rep.), $d_g = \mathrm{sg} \cdot \alpha_g$. )

We have one more irrep ~~$\chi_5$~~. We find it's dim from:

$$24 = |S_4| = 1^2 + 1^2 + d^2 + 3^2 + 3^2 = 20 + d^2 \Rightarrow d = 2$$

Let $\chi_3$ be its character.

Then $\chi_L = \chi_1 + \chi_2 + 2\chi_3 + 3\chi_4 + 3\chi_5$

For $\mathrm{Id} \neq g \in S_4$ $\chi_L(g) = 0$ so:

$$\chi_3(g) = \frac{1}{2}(-\chi_1(g) - \chi_2(g) - 3\chi_4(g) - 3\chi_5(g)) \quad (*)$$ and we calculate:

| | Id | (12) | (123) | (1234) | (12)(34) |
|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | -1 | 1 | -1 | 1 |
| $\chi_3$ | 2 | 0 | -1 | 0 | 2 |
| $\chi_4$ | 3 | 1 | 0 | -1 | -1 |

from (*)

$|\mathrm{Fix}(g)| - 1$

multiply row 2 and row 4

gps $\rightsquigarrow$ gp reps, ie v. spaces

gp. actions $\rightsquigarrow$ permutation reps