① Let $G = S_5$, and $P \in Syl_5(G)$. ⓘ Show $|N_G(P)| = 20$. ⓘⓘ In the special case that $P = \langle (1\ 2\ 3\ 4\ 5) \rangle$, find a set of generators for $N_G(P)$

Solution: • How many Sylow 5-subgroups are there?

↳ It can't be 1 since every $(1\ 2\ 3\ 4\ 5)$ and $(1\ 2\ 3\ 5\ 4)$ generate distinct 5-subgroups.

Divisors of $120 \div 5 = 24$: $\quad 2,\ 3,\ 4,\ 6,\ 8,\ 12,\ 24$

only divisor of 120 congruent to 1 mod 5

Since conjugation is a transitive action on the Sylow 5-subgroups, by orbit-stabilizer theorem:

$$G = \frac{|G|}{|N_G(P)|} = \frac{120}{|N_G(P)|} \quad \text{thus } |N_G(P)| = 20.$$

$$\langle (1\ 2\ 3\ 4\ 5) \rangle = \{ id,\ (1\ 2\ 3\ 4\ 5),\ (1\ 3\ 5\ 2\ 4),\ (1\ 4\ 2\ 5\ 3),\ (1\ 5\ 4\ 3\ 2) \}$$

• $(1\ 2\ 3\ 4\ 5) \in N_G(P)$ since P normalizes itself.

– Need an element of order 4

× $(1\ 2\ 3\ 4)(1\ 2\ 3\ 4\ 5)(4\ 3\ 2\ 1) = (1\ 5\ 2\ 3\ 4)$

✓ $(1\ 3\ 4\ 2)(1\ 2\ 3\ 4\ 5)(2\ 4\ 3\ 1) = (1\ 4\ 2\ 5\ 3)$

$$\boxed{N_G(P) = \langle (1\ 2\ 3\ 4\ 5), (1\ 3\ 4\ 2) \rangle}$$

② G any group. Say $\alpha \in Aut(G)$ is central if $\forall x \in G$, $x^{-1}\alpha(x) \in Z(G)$. Show that the central automorphisms form a normal subgp $N \trianglelefteq Aut(G)$.

Proof: If i is the identity automorphism, $x^{-1} i(x) = x^{-1}x = e \in Z(G)$, so $i \in N$.

Now if $\alpha, \beta \in N$, then $\alpha\beta \in N$ since $\forall x \in G$,

$$x^{-1}(\alpha\beta)(x) = x^{-1}\alpha(\beta(x))$$
$$= \beta(x)^{-1}\beta(x)x^{-1}\alpha(\beta(x))$$
$$= \beta(x)^{-1}(x\beta(x^{-1}))^{-1}\alpha(\beta(x)) = \underbrace{(x\beta(x^{-1}))^{-1}}_{\in Z(G)}\underbrace{\beta(x)^{-1}\alpha(\beta(x))}_{\in Z(G)} \in Z(G)$$

and if $\alpha \in N$, then $\alpha^{-1} \in N$ as

$$\alpha(x^{-1}\alpha^{-1}(x)) = \alpha(x^{-1})x \in Z(G)$$

• If $\alpha(x^{-1}\alpha^{-1}(x)) \in Z(G)$, then $x^{-1}\alpha^{-1}(x) \in Z(G)$.

How to show if normal? $\alpha \in N$, $\beta \in Aut(G)$

$$x^{-1}(\beta\alpha\beta^{-1})(x) \in Z(G).$$

$$x^{-1}\beta(\alpha(\beta^{-1}(x))) = x^{-1}\beta(\beta^{-1}(x)\beta^{-1}(x^{-1})\alpha(\beta^{-1}(x)))$$
$$= x^{-1}\beta(\beta^{-1}(x^{-1})\alpha(\beta^{-1}(x))\beta^{-1}(x))$$

$$x^{-1}\beta\alpha\beta^{-1}(x) = \beta(\underbrace{\beta^{-1}(x^{-1})\alpha(\beta^{-1}(x))}_{\in Z(G)})$$

$\boxed{\text{• } Z(G) \text{ is a characteristic subgp}}$

③ K a field, R the subring of $K(x)$ generated by $K[x]$ and $1/x$. For a typical nonzero element $p(x) = \sum_{i=-M}^{N} a_i x^i$ of R, define $H(p(x)) = \max\{i \in \mathbb{Z} \mid a_i \neq 0\}$ and $L(p(x)) = \min\{i \in \mathbb{Z} \mid a_i \neq 0\}$. Show R is a Euclidean domain w/ Euclidean norm $N(p(x)) = H(p(x)) - L(p(x))$.

Solution: Want to show $\forall f(x), g(x)$, $\exists q(x), r(x)$ with $N(r(x)) < N(g(x))$ or $r(x) = 0$ s.t.

$$f(x) = g(x)q(x) + r(x).$$

• Note that if $p(x) = \sum_{i=-M}^{N} a_i x^i$ then $N(p(x)) = N+M$

R is automatically an integral domain as $R \leq K(x)$ which is a field.

Let $L_f = -L(f(x))$, $H_f = H(f(x))$, and L_g, H_g defined similarly.

Then $N(g(x)) = H_g + L_g$.

If $H_f \geq H_g$ and $L_f \geq L_g$, then we just need to get the terms of degree $\geq H_g$ and $\leq -L_g$ to agree, then we can fix the rest using $r(x)$.

Suppose first that neither H_g nor L_g is zero, and suppose that

• Problem is symmetric in terms of L_g, H_g

Not Done!

(4) F any field. Show that any 2 elements of order 2 in $SL_2(F)$ are conjugate in $GL_2(F)$. Find a necessary + sufficient condition on F for $SL_2(F)$ to have a unique element of order 2.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a^2+bc & b(a+d) \\ c(a+d) & d^2+bc \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & -a \end{bmatrix}\begin{bmatrix} a & b \\ c & -a \end{bmatrix} = \begin{bmatrix} a^2+bc & 0 \\ 0 & a^2+bc \end{bmatrix}$$

If either of $b, c \neq 0$, then $a = -d$.

But, then $\det\begin{vmatrix} a & b \\ c & -a \end{vmatrix} = -a^2-bc \in \{\pm 1\}$.

And for $\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ to have order 2, $bc = 1-a^2$.

Then $\det \neq 1$, or else

$$1 = -a^2-bc = -a^2-(1-a^2) = -1$$

a contradiction.

So $\det = -1$

and $-a^2-bc = -1$

$$b = \frac{1-a^2}{c}$$

$$c = \frac{1-a^2}{b}$$

• Since in $SL_2(F)$, $\det\begin{vmatrix} a & b \\ c & -a \end{vmatrix} = \pm 1$

If $A^2 = I$, then the minimal polynomial of A is x^2-1 and the characteristic polynomial is also x^2-1, with eigenvalues ± 1.

$$\begin{bmatrix} a & b \\ c & -a \end{bmatrix} \xrightarrow{\text{conjugate}} \begin{bmatrix} d & e \\ f & -d \end{bmatrix}$$

(Note if either of b or c is 0, then

$$\begin{bmatrix} a & 0 \\ c & d \end{bmatrix}\begin{bmatrix} a & 0 \\ c & d \end{bmatrix} = \begin{bmatrix} a^2 & 0 \\ c(a+d) & d^2 \end{bmatrix}$$

Then $\{a, d\} = \{1, -1\}$ since $c(a+d) = 0$ and $a^2 = d^2 = 1$.

(5) Let p be prime, $F = \mathbb{F}_p(t)$ or rational polynomials in t.

(i) Show $g(x) = x^p - x + t$ is separable over F.

(ii) Show if α a root of g, $\alpha+1$ is. Deduce that roots of g are all of $\alpha+b$, $b \in \mathbb{F}_p$

(iii) Show g has no roots in F

(iv) Find Galois group of g over F. ← might be $\mathbb{Z}_p$

Solution (i) Consider the derivative

$$D_g(x) = p x^{p-1} - 1 = -1 \quad (F \text{ has characteristic } p \text{ as the prime subfield is still } \mathbb{F}_p)$$

which has no roots.

Recall α is a multiple root of g iff. α a root of D_g.

Pf) $g(x) = (x-\alpha)^n f(x)$ for some $f(x)$

$D_g(x) = n(x-\alpha)^{n-1} f(x) + (x-\alpha)^n f'(x)$

If $n=1$, α not a root of $f(x)$ and $D_g(\alpha) \neq 0$.

(ii) Let α be a root of g.

Then

$$g(\alpha+1) = (\alpha+1)^p - \alpha - 1 + t \overset{\text{characteristic kills all binom. coeff except } \binom{p}{0}, \binom{p}{p}}{=} \alpha^p + 1 - \alpha - 1 + t = \alpha^p - \alpha + t = g(\alpha) = 0.$$

Inductively this gives the roots of g as $\{\alpha + b \mid b \in \mathbb{F}_p\}$.

(iii) • If g has a root in F, all of its roots lie in F.

• Gauss' Lemma!

— F is the field of fracs of the UFD $\mathbb{F}_p[t]$

- If $g(x)$ is irreducible in $(\mathbb{F}_p[t])[x]$ then it is irreducible in $F[x]$.

• If $\alpha \in F$ is $\alpha = \frac{f(t)}{h(t)}$, with $\deg(f) = m$, $\deg(h) = n$, and

$$\left(\frac{f(t)}{h(t)}\right)^p - \frac{f(t)}{h(t)} + t = 0,$$

$$\frac{f(t)^p}{h(t)^p} = -t + \frac{f(t)}{h(t)}$$

$$f(t)^p = -t\,h(t)^p + f(t)h(t)^{p-1}$$

$\deg = pm$ $\qquad$ $\deg$ is $\max\{pn+1,\ m+pn-n\}$

If RHS has degree $pn+1$, done, as $pm = pn+1 \Rightarrow p(m-n) = 1$.

If RHS has degree $m+pn-n$ ...

$m + pn - n = pm$

$m - n = p(m-n)$ ← only true if $m=n$.

But then $m+pn-n = pn < pn+1$.

(iv) Find the Galois group of $g(x)$ over F:

• Let α be a root of $g(x)$. Then $K = F(\alpha)$ is the splitting field of $g(x)$ as all roots look like $\alpha+b$, $b \in \mathbb{F}_p$. Moreover, as $\mathbb{F}_p \subseteq F$, we have that any automorphism $\sigma \in Gal(K/F)$ is determined by $\sigma(\alpha)$, as $\sigma(\alpha+b) = \sigma(\alpha) + b \quad \forall b \in \mathbb{F}_p$.

The Galois group is $\cong \mathbb{Z}_p$, generated by

$\sigma : \alpha \mapsto \alpha+1$.

(6) Let $f(x)$ be monic of degree $n>0$ over a field K. Let $\Delta(f)$ be its discriminant, and let $g(x) = f(x^2)$. Assume $\Delta(g) = \Delta(f)^2 (-4)^n f(0)$.

(i) Let $f(x) = x^2 + 3x + 1$ so $g(x) = x^4 + 3x^2 + 1$. Show g is irreducible over $\mathbb{Q}$.
(helpful to consider roots of f and g).

(ii) To which familiar group is the Galois group of $x^4 + 3x^2 + 1$ over $\mathbb{Q}$ isomorphic?

• Roots of $f(x)$: $x = \frac{-3 \pm \sqrt{5}}{2}$ $\qquad$ Roots of $g(x)$: $x^2 = \frac{-3 \pm \sqrt{5}}{2}$ ← $\sqrt{5} < 3$, so always negative.

$x = \pm\sqrt{\frac{-3 \pm \sqrt{5}}{2}} = \pm i \sqrt{\frac{3 \pm \sqrt{5}}{2}}$

— g has no roots in $\mathbb{Q}$, so if it is reducible, it has two quadratic factors.

Not Done!