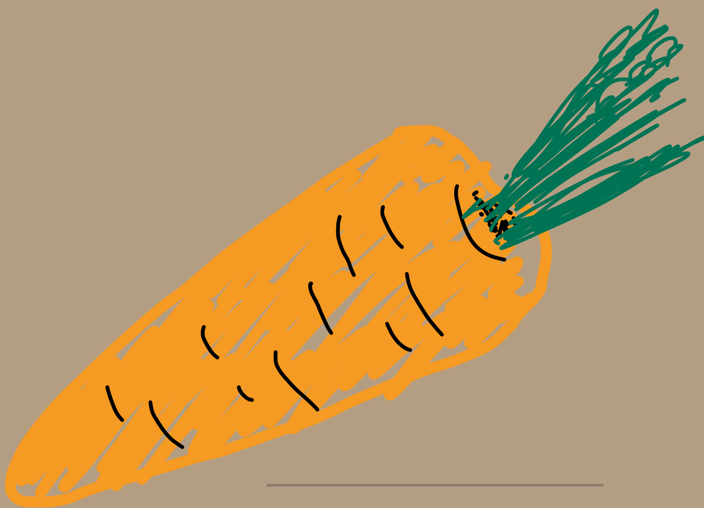
Quals

Algebra



Group theory

- general
- finite groups
- representation theory

Symmetric groups
}
postponed until Galois gp problems

Semidirect product

G any group

$N, H < G$ subgroups.

$N\times H \hookrightarrow G$ subgroup $\iff N \triangleleft G,\ H \triangleleft G,\ N\cap H = \{e\},\ NH = G$

when φ: trivial

More generally for $\varphi : H \to \mathrm{Aut}(N)$ then define $N \rtimes_\varphi H$ by

- as a set $N\rtimes_\varphi H = N\times H$
- group str. $(n_1, h_1)(n_2, h_2) = (n_1\varphi(h_1)n_2,\ h_1h_2)$

If $N\triangleleft G,\ H<G,\ \underline{N\cap H=\{e\}},\ \varphi: H \to \mathrm{Aut}(N)$ conj action
$h \mapsto (n \mapsto hnh^{-1})$

Then $N\rtimes_\varphi H \longrightarrow G$ inj group hom
$(n,h) \longmapsto nh$

($\cong$ if $\underline{NH = G}$)

$\iff H \hookrightarrow G \to G/N$ isom

☺ $(n_1,h_1)\cdot(n_2,h_2) \mapsto n_1h_1n_2h_2$
$= n_1\underbrace{(h_1n_2h_1^{-1})}_{=\varphi(h_1)(n_2)}h_1h_2$

$\|$

$(n_1\varphi(h_1)n_2, h_1h_2) \longmapsto$

Sufficient conditions for $N\rtimes_\varphi H \cong N\rtimes_\psi H$

①
$$\begin{tikzcd} H \arrow[dr, "\varphi"] \arrow[dd, "f", "\cong"'] & \\ & \mathrm{Aut}(N) \\ H \arrow[ur, "\psi"'] & \end{tikzcd}$$

$$N\rtimes_\varphi H \xrightarrow{\cong} N\rtimes_\psi H$$
$$(n,h) \longmapsto (n, f(h))$$

②
$$\begin{tikzcd} & \mathrm{Aut}(N) \arrow[dd, "g\circ(-)\circ g^{-1}"] \\ H \arrow[ur, "\varphi"] \arrow[dr, "\psi"'] & \\ & \mathrm{Aut}(N) \end{tikzcd}$$
for $g\in \mathrm{Aut}\,N$

$$\left(\iff \begin{tikzcd} N \arrow[r, "\varphi_h"] \arrow[d, "g"] & N \arrow[d, "g"] \\ N \arrow[r, "\psi_h"] & N \end{tikzcd} \quad \forall h\in H\right)$$

$$N\rtimes_\varphi H \xrightarrow{\cong} N\rtimes_\psi H$$
$$(n,h) \longmapsto (g(n), h)$$

Classification of $\mathbb{Z}/(p) \rtimes_\varphi \mathbb{Z}/(q)$ (p, q: prime)

$$\mathbb{Z}/(q) \xrightarrow{\varphi} \mathrm{Aut}(\mathbb{Z}/(p)) = (\mathbb{Z}/(p))^\times = \langle \zeta \rangle \cong \mathbb{Z}/(p-1)$$
primitive root

① φ: trivial $\Rightarrow \mathbb{Z}/(p)\times\mathbb{Z}/(q) \cong \mathbb{Z}/(pq)$

② φ: nontrivial
$\Rightarrow q \mid (p-1),\ \varphi(1) = \zeta^{k\cdot\frac{p-1}{q}},\ k\in(\mathbb{Z}/q)^\times$

Such $\mathbb{Z}/p \rtimes_\varphi \mathbb{Z}/q$ are all isomorphic

$$\begin{tikzcd} \mathbb{Z}/q \arrow[r, "\varphi"] \arrow[d, "\cdot k"'] & \mathrm{Aut}(\mathbb{Z}/p) \\ \mathbb{Z}/q \arrow[ur] & \ni \\ 1 \arrow[r, mapsto] & \zeta^{\frac{p-1}{q}} \end{tikzcd}$$

Fall 2016.2 ✓

Fall 2019.2 almost done

G: finite | divisibility results are extremely useful!

- $H < G \Rightarrow G \xrightarrow[|H|:1]{} G/H$, $(G:H) = |G|/|H| \in \mathbb{N}$ (Lagrange)
- $G \curvearrowright X$ (Set) $\Rightarrow G/G_x \xrightarrow{\simeq} Gx$ $\quad |Gx|, |G_x| \mid |G|$ (Orbit-Stabilizer)

(Cauchy's thm $p \mid |G| \Rightarrow \exists g \in G$ order of $g = p$.)

Sylow's theorem(s)

G: finite, p: prime, $\mathrm{Syl}_p(G) := \{\text{Sylow } p\text{-subgp of } G\}$

$n_p := |\mathrm{Syl}_p(G)|$

Sylow p-subgroup: p-group H s.t. $p \nmid (G:H)$

① $n_p \equiv 1 \pmod p$

② $G \curvearrowright \mathrm{Syl}_p(G) \ni H$ by conjugation $H \mapsto gHg^{-1}$; this is transitive

$\mathrm{Stab}(H) = N_G(H) = \{g \in G \mid gH = Hg\}$

$\rightsquigarrow |G|/|N_G(H)| = n_p \mid (G:H)$ ($\rightsquigarrow$ if $n_p = (G:H)$, then $H = N_G(H)$ self-normalizing)

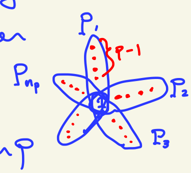
③ Any p-subgroup is contained in a Sylow p-subgroup.

basic techniques: ① find possible n_p's using $n_p \equiv 1$ (p), $n_p \mid (G:H)$ (H: p-Sylow)

② $n_p = 1 \rightsquigarrow$ the Sylow p-subgp is normal
- $\to$ reduce to understand $G \twoheadrightarrow G/N$ (N: Sylow p)
- $\to$ if $\exists$ section (e.g. G/N cyclic) then $G \cong N \rtimes G/N$
- $\to$ G not simple ...

③ If n_p: large, many elements have p-power order

(e.g. when $p^2 \nmid |G|$, # of elements of order p $= n_p(p-1)$)



$P_i \cap P_j = \{e\}$

Note If $N \trianglelefteq G \xrightarrow{p} G/N \cong \langle x \rangle$, $|N|$ coprime to $\mathrm{ord}\, x$ then $\exists$ hom s s.t. $p \circ s = \mathrm{id}$.

☺ Take $g \in p^{-1}(x)$. then $n = \frac{\mathrm{ord}\, g}{\mathrm{ord}\, x}$ divides $|N|$.

let $h = g^n$. then $\mathrm{ord}\, h = \mathrm{ord}\, g$ and $y = p(h)$ generates G/N

define $G/N = \langle y \rangle \longrightarrow G$ by $y \mapsto h$.

Counterexample when $|N|, n$ not coprime: $\mathbb{Z}/p \to \mathbb{Z}/p^2 \to \mathbb{Z}/p$

④ Use $G \xrightarrow{\varphi} \{\text{bijections on } \mathrm{Syl}_q(p)\} \cong S_{n_p}$

know: transitive

$\mathrm{Ker}\, \varphi = \bigcap_{P \in \mathrm{Syl}_p(G)} N_G(P)$ $\left(= \bigcap_{P \in \mathrm{Syl}_p(G)} P \text{ if } n_p = (G:P) \text{ max possible} \right)$

Fall 2019

2. Let p, q be two prime numbers such that $p | q - 1$. Prove that ($p < q$)
   (a) there exists an integer $r \not\equiv 1 \mod q$ such that $r^p \equiv 1 \mod q$;
   (b) there exists (up to an isomorphism) only one noncommutative group of order pq.

F2015 1. Prove that every group of order 15 is cyclic.

S2013.2

$p \mid n_p - 1$, $n_p \mid q$ ($n_p = 1, q$) $\quad n_p = 1$ or q

$q \mid n_q - 1$, $n_q \mid p$ ($n_q = 1, p$) $\quad n_q = 1$

$\mathbb{Z}/q \cong N \triangleleft G \longrightarrow G/N \cong \mathbb{Z}/p \ni 1 \mapsto g \in G$ ($\exists$ order p) $\rightsquigarrow G \cong \mathbb{Z}/q \rtimes \mathbb{Z}/p$. ($\cong \mathbb{Z}/pq$ or $\mathbb{Z}/q \rtimes_\varphi \mathbb{Z}/p$

$\varphi: \mathbb{Z}/q \longrightarrow (\mathbb{Z}/p)^\times$, $1 \mapsto$ order q

F2007 2. Prove that no group of order 148 is simple.

$n_{37} \mid 4 \Rightarrow n_{37} = 1$

F2017 (1) Show that there is no simple group of order 30.

$n_2 = 1, 3, 5, 15$

$n_3 = 1, \underline{10} \rightarrow 2 \cdot 10$ order 3 elements

$n_5 = 1, \underline{6} \rightarrow 4 \cdot 6$ order 5 elements

too many!

F2011 1. a) Let G be a group of order 5046. Show that G cannot be a simple group. *You may not appeal to the classification of finite simple groups.*

$5046 = 2 \cdot 3 \cdot 29^2 \rightsquigarrow n_{29} = 1$

(S2013) b) Let p and q be prime numbers. Show that any group of order p^2q is solvable.

(Note: $N \triangleleft G$ $\rightsquigarrow$ G solvable $\Leftrightarrow N, G/N$ solvable)

b) $p \mid n_p - 1$, $n_p \mid q$ ($1, q$)

$q \mid n_q - 1$, $n_q \mid p^2$ ($1, p, p^2$)

① $q < p \Rightarrow p \nmid q-1$, $\underline{n_p = 1}$ Sylow p $N \triangleleft G \rightarrow G/N \cong \mathbb{Z}/q$, $|N| = p^2$ $\Rightarrow$ abelian (later)

② $q > p \Rightarrow n_q = 1$ or p^2. If $n_q = 1$, $G/(\mathbb{Z}/q) \cong \begin{pmatrix}\text{order } p^2 \\ \text{: abelian}\end{pmatrix}$

If $n_q = p^2$, then $\exists\, p^2(q-1)$ order q-elements $\rightsquigarrow$ only p^2 elements of order $\neq q$ $\rightsquigarrow n_p = 1$. Same as before.

S2016 1. Classify all groups of order 66, up to isomorphism.

$|H| = 3$, $|K| = 11$

$HK < G$ index 2

$\Rightarrow$ normal.

$3 \nmid (11-1) \Rightarrow HK \cong \mathbb{Z}/33$

$HK \hookrightarrow G \twoheadrightarrow \mathbb{Z}/2$

$\rightsquigarrow G \cong \mathbb{Z}/33 \rtimes_\varphi \mathbb{Z}/2$

$\varphi : \mathbb{Z}/2 \rightarrow (\mathbb{Z}/33)^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/10$

$1 \longmapsto (0, 0) \rightsquigarrow \mathbb{Z}/66$

$(1, 0) \rightsquigarrow D_6 \times \mathbb{Z}/11$

$(0, 5) \rightsquigarrow \mathbb{Z}/3 \times D_{22}$

$(1, 5) \rightsquigarrow D_{66}$

S2007 2. Prove that no group of order 224 is simple.

$224 = 32 \cdot 7$

F2008 1. Show that no group of order 36 is simple.

$\rightarrow$ Similar. $n_3 = 4 \rightsquigarrow 36 \nmid 24$. impossible.

G: Simple $\Rightarrow \forall$ hom $G \rightarrow H$ is trivial or injective

$n_2 = 1$ or 7, if $n_2 = 7 \Rightarrow G \longrightarrow \mathrm{Aut}(\mathrm{Syl}_2(G)) = S_7$ transitive $\Rightarrow$ nontrivial $\Downarrow$ injective

but $224 \nmid 7! = 5040 \rightsquigarrow$ impossible

S2014 2. Proof that all groups of order < 60 are solvable.

minimal non-solvable group must be simple $\rightsquigarrow$ enough to check non-simplicity

S2012 1. Let G be a group of order p^3q^2, where p and q are prime integers. Show that for p sufficiently large and q fixed, G contains a normal subgroup other than $\{1\}$ and G.

$p \mid n_p - 1$, $n_p \mid q^2$

if $p > q^2 - 1$, $n_p = 1$

F2014 4. (a) Let G be a group of order p^2q^2, where p and q are distinct odd primes, with $p > q$. Show that G has a normal subgroup of order p^2.

(b) Can a solvable group contain a non-solvable subgroup? **Explain.**

(a) $p \mid n_p - 1$, $n_p \mid q^2$ ($1, q, q^2$)

$p \nmid q-1$, $p \nmid q+1 \rightsquigarrow n_p = 1$

(b) No. $G = G_n \triangleright G_{n-1} \triangleright \cdots \triangleright G_0 = \{e\}$ s.t. G_i/G_{i-1} abelian.

$$\begin{array}{ccccccc} G = G_n & \triangleright & G_{n-1} & \triangleright \cdots \triangleright & G_0 & = \{e\} \\ {\scriptstyle i}\uparrow & & \uparrow & & \uparrow \\ H = H_n & > & H_{n-1} & > \cdots > & H_0 & = \{e\} \end{array}$$

define $H_i = i^{-1}(G_i) = H \cap G_i$.

Applying hom thm to $H_i \hookrightarrow G_i \twoheadrightarrow G_i/G_{i-1}$

$\mathrm{Ker} = H_{i-1} \rightsquigarrow H_i/H_{i-1} \rightarrow G_i/G_{i-1}$

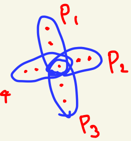
so $H_i \triangleright H_{i-1}$, $H_i/H_{i-1} < G_i/G_{i-1}$ abelian

Question 2. Let G be a group of order 24. Assume that no Sylow subgroup of G is normal in G. Show that G is isomorphic to the symmetric group S_4.

F2018

$\underline{n_2 = 3,\ n_3 = 4}$ $\quad$ idea $G \curvearrowright Syl_3(G) \rightsquigarrow G \xrightarrow{\varphi} S_4$ $\quad$ if φ: injective, we're done.

$Syl_3(G) = \{P_1, P_2, P_3, P_4\}$



$$\operatorname{Ker}\varphi = \bigcap_{i=1}^{4} N_G(P_i)$$

$|N_G(P_i)| = 6 \rightsquigarrow |\operatorname{Ker}\varphi| = 1, 2, 3, 6$

- Note that $P_i \triangleleft N_G(P_i) \rightsquigarrow P_i$: unique 3-Sylow subgp of $N_G(P_i)$, so $|N_G(P_i) \cap N_G(P_j)| < 3$.
- It remains to rule out $|\operatorname{Ker}\varphi| = 2$

$$G \xrightarrow{2:1} G/\operatorname{Ker}\varphi \overset{\text{index } 2}{\subset} S_4$$

$G/\operatorname{Ker}\varphi \cong A_4 \triangleright K$: Klein 4-group

$\rightsquigarrow \varphi^{-1}(K) \triangleleft G$, Sylow 2

Contradiction.

Similar problem: $|G| = 12,\ n_3 \neq 1 \Rightarrow G \cong A_4$ $\quad$ use the same idea: $G \xrightarrow{\varphi} S_4$

- $G \longrightarrow S_4$ injective because $|P_i| \leq |N_G(P_i)| = 12/4 = 3 \rightsquigarrow P_i = N_G(P_i)$
  $\operatorname{Ker}\varphi = \bigcap P_i = \{e\}$
- Contains 8 order 3 elements $\rightsquigarrow \operatorname{Im}\varphi$ contains all 3-cycles, by Lagrange $\operatorname{Im}\varphi = A_4$.

F2001

1. Let G be a finite group and let N be a normal subgroup of G such that N and G/N have relatively prime orders.
(a) Assume that there exists a subgroup H of G having the same order as G/N. Show that $G = HN$. (Here HN denotes the set $\{xy \mid x \in H,\ y \in N\}$.)
(b) Show that $\phi(N) = N$, for all automorphisms ϕ of G.

(a) $G = HN \iff H \hookrightarrow G \twoheadrightarrow G/N$ surjective

$\iff H \hookrightarrow G \twoheadrightarrow G/N$ injective $\iff H \cap N = \langle e \rangle$. : true

$|H| = |G/N|$

(b) $|G| = p_1^{e_1} \cdots p_k^{e_k} \cdots p_n^{e_n}$

$|N| = p_1^{e_1} \cdots p_k^{e_k}$

Let p be one of $p_1, \cdots, p_k$

N contains all the Sylow p-subgroups of G

because $\exists P < N$ Sylow p
$\Rightarrow \forall g^{-1}Pg < g^{-1}Ng = N$.
Any ϕ permutes Sylow p-subgps of G, and $\phi(N)$ is the group generated by the union of p_i-subgroups for $1 \leq i \leq k$.
$= N$

S2001

1. Let G be a finite group and p the smallest prime number dividing the cardinality $|G|$ of G. Let H be a subgroup of G of index p in G. Show that H is necessarily a normal subgroup of G.

$G \curvearrowright G/H$ by left multiplication (G/H: p elements)

$$\rightsquigarrow \begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d] & S_p \\ G/\operatorname{Ker}\varphi \arrow[ur] & \end{tikzcd}$$

$|G/\operatorname{Ker}\varphi| \mid \gcd(|G|, |S_p|) = p$

But we know $\operatorname{Ker}\varphi \subset \operatorname{Stab}(e \cdot H) = H$, so

$p = (G : H) \leq (G : \operatorname{Ker}\varphi) \leq p \quad \rightsquigarrow \operatorname{Ker}\varphi = H$, $\underline{H: \text{normal}}$

p-groups

G: p-group, $p \mid |X| \Rightarrow p$ divides the # of fixed points

e.g. $G \underset{\text{conjugation}}{\curvearrowright} G \rightsquigarrow G = \coprod$ conj class $\rightsquigarrow p^n = \underbrace{1 + \cdots + 1}_{} + (p^k\text{'s for } k \geq 1)$

g: fixed by conjugation $\Longleftrightarrow g \in Z(G)$ $\rightsquigarrow Z(G) \neq \{e\}$

$\rightsquigarrow$ G is nilpotent

$\exists\ 1 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$, $\forall i$ $G_i \triangleleft G$, $G_{i+1}/G_i < G/G_i$ central

proof upper central series $1 \triangleleft Z_1 \triangleleft Z_2 \triangleleft \cdots \triangleleft G$ by $\underset{\neq\{1\}}{Z_1 = Z(G)}$, $Z_2/Z_1 = \underset{\neq\{1\}}{Z(G/Z_1)}, \cdots \rightsquigarrow$ exhaust G

$|G| = p \Rightarrow G \cong \mathbb{Z}/p\mathbb{Z}$

$|G| = p^2 \Rightarrow G \cong \mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$

proof Suppose G: nonabelian and take $g \in G \setminus Z(G)$

The centralizer of g: $Z_G(g) := \{h \in G \mid hg = gh\}$

$\rightsquigarrow \underset{\not\ni g}{Z(G)} \subsetneq \underset{\ni g}{Z_G(g)} \subsetneq G$: impossible
$\uparrow$ $g \notin Z(G)$

p $\quad$? $\quad$ p^2

$|G| = p^3 \Rightarrow$ abelian or $G/Z(G) \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$, $[G,G] = Z(G)$

proof Suppose $G/Z(G) = \langle \bar{g} \rangle$ is cyclic with a generator $\bar{g} = gZ(G)$

$Z_G(g) \ni g \cup Z(G)$ but these generate G, so $Z_G(g) = G$, i.e. $g \in Z(G)$.

which means $\bar{g} = e$, so $Z(G) = G$: abelian.

So if G: nonabelian $\Rightarrow G/Z(G) \cong \mathbb{Z}/p \oplus \mathbb{Z}/p$. : abelian

$Z(G) \supset [G,G] \neq \{e\}$

p elements has to be equal

S2010 **1.** Let G be a non-abelian group of order p^3, here p is prime. Determine the number of distinct conjugacy classes in G.

$|Z(G)| = p$. Take any $g \notin Z(G) \rightsquigarrow Z(G) \subsetneq Z_G(g) \subsetneq G \rightsquigarrow |Z_G(g)| = p^2$,

conj class of g has $|G|/|Z_G(g)| = p$ elements

$\rightsquigarrow$ class formula $p^3 = \underbrace{1 + \cdots + 1}_{p} + \underbrace{p + \cdots + p}_{p^2 - 1}$ $\rightsquigarrow p^2 + p - 1$ in total.

F2013 1. Let $p > 2$ be a prime. Classify groups of order p^3 up to isomorphism.

- Three abelian cases : $\mathbb{Z}/p^3$, $\mathbb{Z}/p^2 \oplus \mathbb{Z}/p$, $\mathbb{Z}/p \oplus \mathbb{Z}/p \oplus \mathbb{Z}/p$

- From now on we take $p \neq 2$. The two nonabelian groups of order p^3, up to isomorphism, will turn out to be

$$\mathrm{Heis}(\mathbf{Z}/(p)) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbf{Z}/(p) \right\} \quad (\mathbb{Z}/p \oplus \mathbb{Z}/p) \rtimes \mathbb{Z}/p$$

(from Keith Conrad, groups of order p^3)

and

$$G_p = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in \mathbf{Z}/(p^2), a \equiv 1 \bmod p \right\} = \left\{ \begin{pmatrix} 1+pm & b \\ 0 & 1 \end{pmatrix} : m, b \in \mathbf{Z}/(p^2) \right\}, \quad \mathbb{Z}/p^2 \rtimes \mathbb{Z}/p$$

$\simeq$ $\simeq$

cf) $p = 2$ D_8 or $Q = \{\pm 1, \pm i, \pm j, \pm k\}$

F2014 5. (a) Prove that every group of order p^2 (p a prime) is abelian. Then classify such groups up to isomorphism.

(b) Give an example of a non-abelian group of order p^3 for $p = 3$. *Suggestion: Represent the group as a group of matrices.*

$G \xrightarrow{\pi} G/Z(G) \cong \mathbb{Z}/p \oplus \mathbb{Z}/p$ if G : nonabelian

<u>claim</u> $\exists g \in G \setminus Z(G)$ has order p

$\because$ G has no element of order p^3, so otherwise $\forall g \in G \setminus Z(G)$ has ord p^2.

$\langle g \rangle \cong \mathbb{Z}/p^2$ has p order p element, so $Z(G) = \langle g^p \rangle \subset \langle g \rangle$

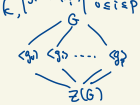
$\langle g \rangle = \langle h \rangle$ iff $\langle g \rangle / Z(G) = \langle h \rangle / Z(G)$, i.e. $\langle \bar{g} \rangle = \langle \bar{h} \rangle$ in $\mathbb{F}_p \oplus \mathbb{F}_p$, $\iff \bar{g} = \bar{h}$ in $\mathbb{P}^1(\mathbb{F}_p)$

and otherwise $\langle g \rangle \cap \langle h \rangle = Z(G)$.

i.e. G decomposes G into $\langle g_0 \rangle \sqcup_{Z(G)} \langle g_1 \rangle \sqcup_{Z(G)} \cdots \sqcup_{Z(G)} \langle g_p \rangle$ for representatives $\left\{ g_i \in \pi^{-1}(\ell_i \setminus 0) \;\middle|\; \begin{array}{l} \ell_i : \mathbb{F}_p \hookrightarrow \mathbb{F}_p^{\oplus 2} \\ 0 \le i \le p \end{array} \right\}$

Now since $\langle g_1^p \rangle = Z(G) = [G, G]$, $g_0 g_1 g_0^{-1} g_1^{-1} = g_1^{kp}$ for some k,

i.e. $\mathrm{Ad}_{g_0} : G \to G$ sends g_1 to g_1^{kp+1}.



$g_0^p \in Z(G)$ so $\mathrm{Ad}_{g_0^p} = (\mathrm{Ad}_{g_0})^p$ must be trivial, but

$(\mathrm{Ad}_{g_0})^p (g_1) = g_1^{(kp+1)^p} = g_1^{1+p} \neq g_1$ contradiction.

Take such g and consider a projection $G \to G/Z(G) \cong \mathbb{Z}/p \oplus \mathbb{Z}/p \overset{\exists}{\twoheadrightarrow} \mathbb{Z}/p$. this admits a section.

$g \longmapsto \neq 0 \longmapsto \neq 0$.

So $G \cong H \rtimes \mathbb{Z}/p$ where H is either ① $\mathbb{Z}/p \oplus \mathbb{Z}/p$ or ② $\mathbb{Z}/p^2$

$$\mathbb{Z}/p \longrightarrow \mathrm{Aut}(H) = GL_2(\mathbb{F}_p) \text{ or } (\mathbb{Z}/p^2)^\times$$

$$(\mathbb{Z}/p^2)^\times = \mathbb{Z}/p(p-1) = \mathbb{Z}/p \oplus \mathbb{Z}/p-1$$

nontrivial, i.e. $1 \mapsto$ order p element

② $\mathbb{Z}/p \longrightarrow \mathbb{Z}/p \oplus \mathbb{Z}/p-1 \cong (\mathbb{Z}/p^2)^\times$

$1 \longmapsto (a, 0)$ all equivalent $\left(\begin{array}{c} \mathbb{Z}/p \xrightarrow{(1,0)} \mathbb{Z}/p \oplus \mathbb{Z}/p-1 \\ \downarrow a \nearrow_{(a,0)} \\ \mathbb{Z}/p \end{array} \right)$

e.g. $1+p \in (\mathbb{Z}/p^2)^\times$ has order p

$\rightsquigarrow \mathbb{Z}/p \circlearrowright \mathbb{Z}/p^2$ m acts by multiplication by $(1+p)^m = 1+mp$

$\hookrightarrow$ multiplication on $\mathbb{Z}/p^2 \rtimes \mathbb{Z}/p \ni (l, m)$ is $(l_1, m_1)(l_2, m_2) = (l_1 + (1+m_1p) l_2, m_1 m_2)$

$$\cong \left\{ \begin{pmatrix} 1+mp & l \\ 0 & 1 \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{Z}/p^2) \right\}$$

① order p element in $GL_2(\mathbb{F}_p)$ has min. poly that divides $X^p - 1 = (x-1)^p$

and not diagonalizable ($(\mathbb{F}_p^\times)^2$ has no order p element)

$\rightsquigarrow$ min poly $= (x-1)^2$, Jordan form $\rightsquigarrow$ conjugate to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

i.e. $\mathbb{Z}/p \circlearrowright (\mathbb{Z}/p \oplus \mathbb{Z}/p)$ by

$m \mapsto$ mult. by $\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a' \\ b' \end{pmatrix} = \begin{pmatrix} a' + mb' \\ b' \end{pmatrix}$

$(\mathbb{Z}/p \oplus \mathbb{Z}/p) \rtimes \mathbb{Z}/p$

$$\left(\begin{pmatrix} a \\ b \end{pmatrix}, m \right) \left(\begin{pmatrix} a' \\ b' \end{pmatrix}, m' \right) = \left(\begin{pmatrix} a + a' + mb' \\ b + b' \end{pmatrix}, m + m' \right)$$

$$\rightsquigarrow \cong \left\{ \begin{pmatrix} 1 & m & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{Mat}_3(\mathbb{F}_p) \right\}$$

F2019 S2015 4. Find all irreducible representations of a finite p-group G over a field k of characteristic p.

<u>A.</u> Only the trivial one ($k \circlearrowleft_{\mathrm{triv}} G$)

<u>proof</u> Enough to show : $\forall V$: $k[G]$-mod, $\exists$ nonzero G-fixed point

Take any $v \in V \setminus \{0\}$, Consider $W \subset V$: $\mathbb{F}_p[G]$-submod generated by v

W : fin. dim. vector sp $/\mathbb{F}_p$ $\rightsquigarrow$ $p \mid |W| < \infty$.

$G \curvearrowright W$ orbit decomp $\underbrace{1 + \cdots + 1}_{n \text{ fixed pts}} + (p^k\text{'s for } k \ge 1)$

$\rightsquigarrow \begin{cases} n \ge 1 & (0 \text{ is fixed}) \\ p \mid n \end{cases} \Rightarrow n \ge p$. ☑

Group Theory random problems

F2010 **1.** Let G be a group. Let H be a subset of G that is closed under group multiplication. Assume that $g^2 \in H$ for all $g \in G$. Show that H is a normal subgroup of G and G/H is abelian.

H: subgroup $\quad h \in H \Rightarrow h \cdot \underbrace{(h^{-1})^2}_{G^2 \subset H} = h^{-1} \in H$

H: normal $\quad g \in G, h \in H \Rightarrow gh = (gh)^2 h^{-1} g^{-2} g \in Hg$

G/H: abelian $\quad$ enough to show $g_1 g_2 H \subset g_2 g_1 H$

$g_1 g_2 h \in g_2 g_1 H \iff (g_2 g_1)^{-1} g_1 g_2 h \in H \iff (g_2 g_1)^{-2} (g_2 g_1^2)^2 g_1^{-2} h \in H$: true.

S2014

1. Find the number of colouring of faces of a cube in 3 colours. Two colourings are equal if they are the same after a rotation of the cube. [Hint Use the Burnside formula

proof: both sides are additive in X ($\sqcup \rightsquigarrow +$) so enough to check when X is G/H. $|X^g| = |X|$ if $g \in H$, 0 otherwise.

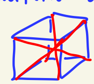
$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|, \quad \overset{X^g \cong X^{hgh^{-1}}}{=} \frac{1}{|G|} \sum_{C_g:\text{conj classes}} |C_g||X^g|$$

where a group G acts on a set X, X/G is the set of orbits, and, for every $g \in G$, X^g is the fixed subset of g in X.]

$X = (\{\text{six faces}\} \to \{\text{three colours}\})$

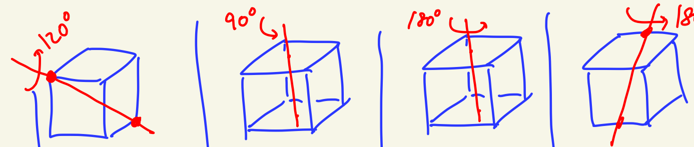
$|X| = 3^6$,

Fact the subgroup of $SO(3)$ which preserves the cube $\cong S_4$.
permutation of diagonals



$\rightsquigarrow G = S_4 \curvearrowright X$.

The desired # $= |X/G|$



g: 120°, 90°, 180°, 180°, id

Cycle type in S_4	$1+3$	4	$2+2$	$1+1+2$	$1+1+1+1$
$\lvert C_g\rvert$	8	6	3	6	1
$\lvert X^g\rvert$	3^2	3^3	3^4	3^3	3^6

$\rightsquigarrow \frac{1}{24} \sum |C_g||X^g| = 57$.

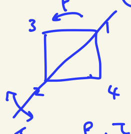
S2019 4. Let f be a polynomial with n variables and put

$$\mathrm{Sym}\, f = \{\sigma \in S_n \mid f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = f(x_1, x_2, \ldots, x_n)\}.$$

Prove that Sym f is a subgroup of S_n.

Prove that the group D_4 (of symmetries of the square) is isomorphic to Sym $(x_1x_2 + x_3x_4)$.

$D_4 \xrightarrow{\varphi} S_4$ injective.



$\rho \mapsto (1324)$

$\tau \mapsto (34)$

ρ, τ fix $x_1x_2 + x_3x_4$

$\Rightarrow \mathrm{Im}\,\varphi \subset \mathrm{Sym}(x_1x_2+x_3x_4)$

There are 8 σ's s.t.
$x_1x_2 + x_3x_4 = x_{\sigma(1)}x_{\sigma(2)} + x_{\sigma(3)}x_{\sigma(4)}$
(4 choices for $\sigma(1)$, then $\sigma(2)$ determined
2 choices for $\sigma(3)$ $\quad\sigma(4)$)

$\boxed{\text{TG}}$

F2004

S2011

1. (a) Let H be a subgroup of a finite group G with $H \neq \{1\}$ and $H \neq G$. Prove that G is not the union of all the conjugates of H in G.

(b) Give an example of an infinite group G for which the assertion in part (a) is false.

(a) $\underbrace{G \supset N_G(H)}_{k} \underbrace{\supset H}_{m}$ index $\rightsquigarrow \left|\bigcup_{g\in G} gHg^{-1}\right| = \left|\bigcup_{[g]\in G/N_G(H)} gHg^{-1}\right|$

$$\le 1 + \sum_{[g]\in G/N_G(H)} \left(|gHg^{-1}| - 1\right)$$

$\forall g,\ e \in gHg^{-1}$; $|gHg^{-1}| = |H|$

$$= 1 + k\cdot\left(|G|/km - 1\right) = 1 - k + |G|/m \le |G|.$$

equality holds only when $k = m = 1$

(b) $B = \left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\} \subset GL_2(\mathbb{C})$ (See S2008, Problem 1 (b))

S2009

1. Let H and K be two solvable subgroups of a group G such that $G = HK$.

(a). Show that if either H or K is normal in G, then G is solvable.

(b). Give an example that G may not be solvable without the assumption in (a).

(a) assume $H \lhd G$.
$K \hookrightarrow G \twoheadrightarrow G/H$ the composition φ is surjective by $HK = G$, so $G/H \cong K/\mathrm{Ker}\,\varphi$ is solvable. Since $H, G/H$ is solvable, so is G.

(b) $G = A_5$, $H = \langle(1\,2\,3\,4\,5)\rangle$, $K = A_4$ on $\{1,2,3,4\}$

$\rightsquigarrow \forall g \in G,\ \exists h \in H\ \ h^{-1}g(5) = 5 \rightsquigarrow h^{-1}g \in K$, so $G = HK$

solvable

not solvable

F2003

1. In a group G, let 1 denote the identity element and let $[x,y] = xyx^{-1}y^{-1}$ denote the commutator of the elements $x, y \in G$.

a) Express $[z, xy]x$ in terms of x, $[z,x]$ and $[z,y]$.

b) Prove that if the identity $[[x,y],z] = 1$ holds in a group G, then the identities

$$[x, yz] = [x,y][x,z] \quad \text{and} \quad [xy, z] = [x,z][y,z] \quad \text{hold in } G.$$

S2005

1. Let k be a field. Let $G = GL_n(k)$ be the general linear group. Here $n > 0$. Let D be the subgroup of diagonal matrices. Let $N = N_G(D)$ be the normalizer of D. Determine the quotient group N/D.

S_n ?

F2009

1. Let G be a finite group. Let $Aut(G)$ be the group of automorphisms of G. Consider the group action $\phi : Aut(G) \times G \to G$ where $\phi(\sigma, g) = \sigma(g)$. Assume G has exactly two orbits under the action of $Aut(G)$.

(a). Determine all such G, up to isomorphism.

(b). List all cases in which $Aut(G)$ is a solvable group.

F2016 1. Determine $Aut(S_3)$.

$$S_3 \xrightarrow{f} Aut(S_3) \xrightarrow{g} S_{\{(12)(23)(31)\}} \cong S_3$$

- f: conjugate action, injective because $\mathrm{Ker} f = Z(S_3) = \{e\}$
- $\alpha \in Aut(S_3) \rightsquigarrow g(\alpha)$: permutation on order 2 elements, g: injective because $(12), (23)$ generates S_3.

Representation Theory

G finite

representation of $G/_k$ = $k[G]$-module V = $G \to GL(V)$

<u>Maschke's thm</u> when $|G| \in k^\times$, $W \subset V$ G-repn's $\Rightarrow V \cong W \oplus V/W$ as G-rep'ns
($\Leftrightarrow$ any fin dim repn = $\bigoplus$ irrep $\Leftrightarrow k[G]$ semisimple)

<u>Schur's Lemma</u> • if $V_1 \xrightarrow{f} V_2$ between irrep is not isomorphic, then it's 0.
• If k: alg closed, V: fin dim irrep $\rightsquigarrow \mathrm{End}_{k[G]}(V) \simeq k$
($V \xrightarrow{f} V$ only scalar multiplication)

characters

$$\begin{tikzcd} G \arrow[r, "\rho"] \arrow[rr, bend right, "\chi_\rho \ (\text{or } \chi_V)"'] & GL_n(\mathbb{C}) \arrow[r, "tr"] & \mathbb{C} \end{tikzcd}$$

(# of irrep) = (# of conj classes)

<u>properties</u> • χ_ρ is a class function (i.e. $\{\text{conj classes}\} \to \mathbb{C}\} =: C(G)$)

• $\chi_\rho(1) = \dim \rho$
• $\chi_{V \oplus W} = \chi_V + \chi_W$
• $\chi_{V \otimes W} = \chi_V \chi_W$
• $\chi_{\wedge^2 V}(g) = \frac{1}{2}\left(\chi_V(g)^2 - \chi(g^2)\right)$
• $\chi_{\mathrm{Sym}^2 V}(g) = \frac{1}{2}\left(\chi_V(g)^2 + \chi_V(g^2)\right)$
• $\chi_{V^*} = \overline{\chi_V}$
(• $\chi_{\mathrm{Hom}(V,W)} = \overline{\chi_V}\,\chi_W$)

and $\{\chi_\rho \mid \rho : \text{irrep}\}$ forms an ONB of $C(G)$ w.r.t. the inner prod
$$(\chi_1, \chi_2) = \frac{1}{|G|}\sum_{g \in G} \overline{\chi_1(g)}\,\chi_2(g)$$

• $|G| = \sum_{\rho:\text{irrep}} (\dim \rho)^2 \quad (\Leftarrow k[G] \cong \bigoplus_{\rho:\text{irrep}} \rho^{\oplus \dim \rho})$
• χ: irr. ch. $\Leftrightarrow (\chi, \chi) = 1$
• χ': character $\rightsquigarrow$ irr. factor χ appears (χ', χ) times

$$\dim \mathrm{Hom}_G(V, W) = \frac{1}{|G|}\sum_{g \in G} \overline{\chi_V}(g)\,\chi_W(g) = \langle \chi_V, \chi_W \rangle$$

$$\dim V^G = \frac{1}{|G|}\sum_{g \in G} \chi_V(g)$$

if V, W irrep: $\begin{cases} 0 & V \not\cong W \\ 1 & V \cong W \end{cases}$ by Schur

• $\rho = \rho_1^{\oplus n_1} \oplus \cdots \oplus \rho_k^{\oplus n_k}$ irred decomp
$\Leftrightarrow n_i = \langle \chi_\rho, \chi_{\rho_i} \rangle$

$k = \mathbb{C}$ • $\rho(g)$ finite order $\Rightarrow$ diagonalizable $\sim \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$ with λ_i: roots of unity
$\rightsquigarrow \rho(g) = id \Leftrightarrow \chi_\rho(g) = \dim \rho$ (ρ: faithful $\Leftrightarrow [g \neq 1 \Rightarrow \chi(g) \neq \chi(1)]$)

k: any • 1-dim'l character = 1-dim'l repn = 1-dim'l repn of G^{ab}
= irrep of G^{ab}

$$\begin{tikzcd} G \arrow[r] \arrow[d] & k^\times \\ G^{ab} \arrow[ur, dashed] & \end{tikzcd}$$

(in particular # of 1-dim'l characters = $|G^{ab}|$)

alg. cl. char = 0 • dim of irrep divides $|G|$
(or even stronger, dim of irrep divides $|G/N|$ for N: abelian normal)

character table

S_3

# →	① 1	③ (12)	② (123)
triv	1	1	1
sgn	1	-1	1
Std_3	2	0	-1

$\left\{ \begin{array}{l} (n-1)\text{-dim } (S_n \overset{perm}{\curvearrowright} \mathbb{C}^n) - (\text{triv}) \\ \quad \chi(\sigma) = \#(\text{fixed pts of } \sigma) - 1 \\ \text{always irred} \quad \text{see the problem below)} \end{array} \right.$

Note: $G \overset{surj}{\twoheadrightarrow} H \xrightarrow{irred} GL_n(\mathbb{C})$ is again irred

S_4

	① 1	⑥ (12)	⑧ (123)	⑥ (1234)	③ $(12)(34)$
triv	1	1	1	1	1
sgn	1	-1	1	-1	1
$Std_3 \circ \phi$	2	0	-1	0	2
Std_4	3	1	0	-1	-1
$sgn \otimes Std_4$	3	-1	0	1	-1

Composition

$S_4 \overset{\phi}{\twoheadrightarrow} S_4/\text{Klein 4-gp} \cong S_3 \xrightarrow{Std_3} GL_2(\mathbb{C})$

Symmetry of (tetrahedron) $\mapsto$ Symmetry of (triangle)

A_4

	① 1	④ (123)	④ (132)	③ $(12)(34)$
triv	1	1	1	1
Std_4	3	0	0	-1
$\rho\circ\phi$	1	ω	ω^2	1
$\overline{\rho\circ\phi}$	1	ω^2	ω	1

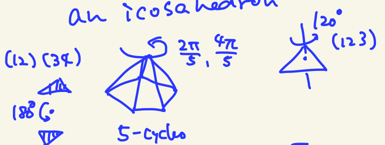
$A_4 \overset{\phi}{\twoheadrightarrow} \mathbb{Z}/3 \overset{\rho}{\curvearrowright} \mathbb{C}$ by rotation (multiplication by ω)

A_5

	① 1	⑳ (123)	⑮ $(12)(34)$	⑫ (12345)	⑫ (13524)
triv	1	1	1	1	1
Std_5	4	1	0	-1	-1
$Sym^2 Std_5 - triv - Std_5$	5	-1	1	0	0
χ	3	0	-1	$\frac{1+\sqrt5}{2}$	$\frac{1-\sqrt5}{2}$
$\bar\chi$	3	0	-1	$\frac{1-\sqrt5}{2}$	$\frac{1+\sqrt5}{2}$

$\left(\Lambda^2 Std_5 = \chi \oplus \bar\chi\right)$

$A_5 \subset SO(3)$ rotation group of an icosahedron



5-cycle

$1 + 2\cos\left(\frac{2\pi}{5}\right) = \frac{1+\sqrt5}{2}$

$1 + 2\cos\left(\frac{4\pi}{5}\right) = \frac{1-\sqrt5}{2}$

S_5

	① 1	⑩ (12)	⑳ (123)	㉚ (1234)	㉔ (12345)	⑮ $(12)(34)$	⑳ $(123)(45)$
triv	1	1	1	1	1	1	1
sgn	1	-1	1	-1	1	1	-1
Std_5	4	2	1	0	-1	0	-1
$Std_5 \otimes sgn$	4	-2	1	0	-1	0	1
$\Lambda^2 Std_5$	6	0	0	0	1	-2	0
$Sym^2 Std_5 - triv - Std_5$	5	1	-1	-1	0	1	1
$(\text{——}) \otimes sgn$	5	-1	-1	1	0	1	-1

S 2008 **4.** Let $V \cong \mathbb{C}^n$ be an n-dimensional complex vector space with the standard basis $e_1, \ldots, e_n$. Consider the permutation group action $S_n \times V \to V$ where $\sigma(e_i) = e_{\sigma(i)}$. Decompose V into simple $\mathbb{C}[S_n]$-modules.

$V \cong \underbrace{\mathbb{C}(e_1 + \cdots + e_n)}_{\text{triv}} \oplus Std$

To prove V have only 2 irreducible components, it's enough to show that $\langle \chi_V, \chi_V \rangle = 2$.

$\chi_V(\sigma) = (\#\text{ of fixed pts of } \sigma) \in \mathbb{Z}$

$\rightsquigarrow \langle \chi_V, \chi_V \rangle = \frac{1}{n!} \sum_{\sigma \in S_n} \chi_V(\sigma)^2$

$= \frac{1}{n!} \sum_{\sigma\in S_n} \#\left\{(i,j) \,\middle|\, \begin{array}{l}\sigma(i)=i \\ \sigma(j)=j\end{array}\right\}$

$= \frac{1}{n!} \#\left\{(\sigma, i, j) \,\middle|\, \begin{array}{l}\sigma\in S_n \\ \sigma(i)=i \\ \sigma(j)=j\end{array}\right\}$

$= \frac{1}{n!} \sum_{i,j} \#\left\{\sigma \in S_n \,\middle|\, \begin{array}{l}\sigma(i)=i \\ \sigma(j)=j\end{array}\right\}$, where $\#\{\ldots\} = \left\{\begin{array}{l}(n-2)! \text{ if } i \neq j \\ (n-1)! \text{ if } i = j\end{array}\right.$

$= \frac{1}{n!}\left(n\cdot(n-1)! + n\cdot(n-1)(n-2)!\right)$

$= 2.$

5. Find the table of characters for S_4. (S2014)

6. Find a table of characters for the alternating group A_5. (-2016)

3. Let $G = S_4$ (the symmetric group on four letters).

(a) Prove that G has two non-equivalent irreducible complex representations of dimension 3; call them ρ_1 and ρ_2.

(b) Decompose $\rho_1 \otimes \rho_2$ (as a representation of G) into a direct sum of irreducible representations. (F2015)

$\chi_{\rho_1\otimes\rho_2}$	9	-1	0	-1	1

$\Downarrow$

Compute $(\text{triv}, \chi_{\rho_1\otimes\rho_2})$, $(\text{sgn}, \chi_{\rho_1\otimes\rho_2})$, etc.

4. Let $\rho : S_3 \to \mathbb{C}^2$ be a two-dimensional irreducible representation of the symmetric group S_3. Decompose $\rho^{\otimes 2}$ and $\rho^{\otimes 3}$ into a direct sum of irreducible representations of S_3. (F2011)

3. Let $G = S_3$.

(a) Prove that G has an irreducible complex representation of dimension 2,—call it ρ— but none of higher dimension.

(b) Decompose $\rho \otimes \rho \otimes \rho$ (as a representation of G) into a direct sum of irreducible representations. (F2014)

6. Let S_4 be the symmetric group of 4 elements.

(1). Give an example of non-trivial 8-dimensional representation of the group S_4.

(2). Show that for any 8-dimensional complex representation of S_4, there exists a 2-dimensional invariant subspace. (S2006, F2003)

8 cannot be written as (at most 1) + (sum of 3's)

5. Prove the existence of a 1-dimensional invariant subspace for any 5-dimensional representation of the group A_4 (the *alternating* group of degree 4). (S2003, F2007)

6. Consider complex representations of a finite group G. Let $\sigma_1 \dots \sigma_s$ be representatives from the conjugacy classes of G, and let $\chi_1 \dots \chi_s$ be all the different simple characters of G.

(a). Define an inner product on the $\mathbb{C}$-space of class functions on G, so that $\{\chi_1 \dots \chi_s\}$ forms an orthogonal basis for this space.

(b) Let $A = (a_{ij})$ be the matrix of the character table of G, i.e., $a_{ij} = \chi_i(\sigma_j)$ $(1 \le i, j \le s)$. Show that A is invertible. (S2004)

S2018
S2007

4. Is S_4 isomorphic to a subgroup of $GL_2(\mathbf{C})$?

$\Longleftrightarrow$ Is there a faithful 2-dim'l cpx repn of S_4?

No, because
$$\chi_{\text{triv}}((12)(34)) = \dim(\text{triv})$$
$$\chi_{\text{sgn}}((12)(34)) = \dim(\text{sgn})$$
$$\chi_{\text{std}_3\circ\phi}((12)(34)) = \dim(\text{std}_3\circ\phi)$$

and all 2-dim'l repns are sum of these, so $\forall \rho$: 2-dim $\rho((12)(34)) = \text{id}$. in particular ρ not faithful. $\square$

S2010

6. Let G be a group with 24 elements. **Use representation theory** to show that $G \neq [G, G]$. (Here $[G, G]$ is the commutator subgroup of G.)

$G = [G,G] \Longleftrightarrow G^{ab} = \{e\} \Longleftrightarrow$ only trivial 1-dim'l repn.

but it's impossible to have $1^2 + k_1^2 + \dots + k_n^2 = 24$ $(k_i \ge 2)$

$\left(\begin{array}{l} k_i^2 \equiv 1 \mod 4 \text{ when } k_i \text{ odd} \\ 0 \text{ when even} \\ \rightsquigarrow \text{need at least three odd } k_i\text{'s} \\ 1^2 + 3^2 + 3^2 + 3^2 = 28 > 24 \end{array} \right)$

F2017 (6) Let G be a finite group with center $Z \subset G$. Show that if G admits a faithful irreducible representation $G \xrightarrow[\rho]{} \mathrm{GL}_n(k)$ for some positive integer n and some field k, then Z is cyclic.

$p \nmid$ char k $|G|$ because if not take a Sylow p-sub $P \hookrightarrow G \to \mathrm{GL}_n(k)$ must be trivial by F2009, problem 4

For any $g \in Z$, $V \xrightarrow[\rho(g)]{} V$ commutes with all $\rho(g')$, $g' \in G$

i.e. $k[G]$-homomorphism.

If k: alg. closed, by Schur's lemma $\rho(g) \in k^\times$ (scalar matrix)

So we have an injection $Z \to k^\times$. Now note that any finite subgroup of $k^\times$ is cyclic (because # of element of order $d \le \varphi(d)$)

$\Rightarrow Z$: cyclic

If k is not alg. cl, consider $G \overset{\rho}{\hookrightarrow} GL_n(k) \hookrightarrow GL_n(\bar{k})$.

$\rho \otimes_k \bar{k} = \underbrace{\sigma_1 \oplus \cdots \oplus \sigma_m}_{\text{Galois conjugates}}$, $\circlearrowleft \mathrm{Gal}(\bar{k}/k)$

Ker of σ_i's are the same, $\bigcap \mathrm{Ker}\, \sigma_i = \mathrm{Ker}\, \rho \leadsto \sigma_i$ are faithful. $\square$

$G \xrightarrow{\sigma_i} GL_?(\bar{k})$

S2005 **6.** Let V be a finite dimensional vector space over a field k. Let G be a finite group. Let $\varphi : G \to GL(V)$ be an irreducible representation of G. Suppose that H is a finite abelian subgroup of $GL(V)$ such that H is contained in the centralizer of $\varphi(G)$. Show that H is cyclic.

same.

F2010 **6.** Let G be a non-abelian group of order p^3. Here p is a prime number. $Z(G) = [G,G] \cong \mathbb{Z}/p$, $G/Z(G) = G^{ab} \cong \mathbb{Z}/p \times \mathbb{Z}/p \leadsto p^2$ 1-dim'l irrep

(a) Determine the number of (isomorphic classes of) irreducible complex representations of G, and find their dimensions.

(b) Which of the irreducible complex representations of G are faithful? Explain your answer.

(a) using the fact that $\dim V \mid |G|$ for V irred,

$\underbrace{1^2 + \cdots + 1^2}_{p^2} + \underbrace{d_1^2 + \cdots + d_{p-1}^2}_{p-1}$ is satisfied only when $d_i = p$. $\begin{cases} p^2 \text{ irreps of dim } 1 \\ p-1 \text{ irreps of dim } p \end{cases}$

(b) $G \twoheadrightarrow G^{ab} \longrightarrow \mathbb{C}^\times$ is not injective. so dim 1 irreps are not faithful.

Let $G \xrightarrow{\rho} GL_p(\mathbb{C})$ is irrep. If ρ is not injective, it factors through the quotient $G/\ker\rho$ but since $|G/\ker\rho| = 1, p, p^2$, $G/\ker\rho$ is abelian, so it splits into $\bigoplus$(1-dim). Contradiction

So p-dim'l irreps are faithful.

S2011 5. Let K be a field, and $\Phi : G \to GL_n(K)$ an n-dimensional matrix representation of the group G. Define an action of G on the full matrix ring $M_n(K)$ by $(g, A) \mapsto \Phi(g) \cdot A$ when $g \in G$ and $A \in M_n(K)$ (that's a matrix product on the right-hand side). This in turn induces a group homomorphism $\Psi : G \to GL(M_n(K))$. Express the character $\chi(\Psi)$ of Ψ in terms of $\chi(\Phi)$.

Let $E_{ij} = \begin{array}{c} \\ i \end{array}\!\!\begin{pmatrix} & & j & \\ & & \vdots & \\ & \cdots & 1 & \\ & & & \end{pmatrix} \in M_n(K)$. Then $\{E_{ij}\}$ is a basis of $M_n(K)$.

For any $\underset{(p_{ij})}{P} \in GL_n(K)$, $PE_{ij} = \sum_{k=1}^{n} p_{ki} E_{kj}$.

($\hookrightarrow$ only coef. of E_{ij} ($= p_{ii}$) counts in trace.)

So the trace of $\begin{pmatrix} M_n(K) \longrightarrow M_n(K) \\ A \longmapsto PA \end{pmatrix}$ is $\sum_{i,j} p_{ii} = n \cdot \mathrm{tr}(P)$.

Therefore $\chi(\Psi)(g) = \mathrm{tr}(M_n(K) \xrightarrow[\Phi(g)\cdot(-)]{} M_n(K)) = n \cdot \mathrm{tr}(K^n \xrightarrow[\Phi(g)]{} K^n) = n \cdot \chi(\Phi)(g)$.

S2015 5. Prove that a tensor product of irreducible representations over an algebraically closed field is irreducible.

S2001 3. Calculate the complete character table for $\mathbb{Z}/3\mathbb{Z} \times S_3$, where S_3 is the symmetric group in 3 letters.

$\begin{Bmatrix} \text{trivial} \\ 1 \mapsto \omega \\ 1 \mapsto \omega^2 \end{Bmatrix} \times \begin{Bmatrix} \text{trivial} \\ \text{sgn} \\ \text{std} \end{Bmatrix}$

In general

$$\begin{tikzcd} & G \arrow[r, "\rho"'] & GL(V)^{\dim = n} \\ G \times H \arrow[ur, "pr_1"] \arrow[dr, "pr_2"'] & & \\ & H \arrow[r, "\pi"'] & GL(W)^{\dim = m} \end{tikzcd}$$

ρ, π : irrep

$\Rightarrow \rho \circ pr_1,\ \pi \circ pr_2$ irrep

$\rightsquigarrow \rho \boxtimes \pi := (\rho \circ pr_1) \otimes (\pi \circ pr_2)$ external tensor prod.

Prop If k alg cl. G, H finite. $\{\text{(fin dim) irrep of } G \times H\} = \{\rho \boxtimes \pi \mid \rho, \pi : \text{irrep}\}$ (i.e. $G \curvearrowright V$, $H \curvearrowright W$ $\rightsquigarrow G \times H \curvearrowright V \otimes W$)

☹ π, ρ irrep $\Longleftrightarrow$ $\rho \boxtimes \pi$ irrep

($\Leftarrow$) if π or ρ reducible, then $\rho \boxtimes \pi$ reducible by the distributivity of $\otimes$ and $\oplus$

($\Rightarrow$) Note that $\mathrm{Hom}_{k[G]}(V, \mathrm{Res}_G^{G \times H} V \otimes W) \simeq \mathrm{Hom}_{k[G]}(V, V \otimes \underset{\text{triv}}{\mathbb{C}^m}) \simeq \mathrm{Hom}_{k[G]}(V, V)^m \underset{\text{Schur's lemma}}{\simeq} \mathbb{C}^m \simeq W$

This identification is H-equivariant.

Now suppose $U < V \otimes W$ is $G \times H$-invariant. Then

$W' = \mathrm{Hom}_{k[G]}(V, \mathrm{Res}_G^{G \times H} U) \hookrightarrow \mathrm{Hom}_{k[G]}(V, \mathrm{Res}_G^{G \times H} V \otimes W) \simeq W$ is an H-invariant subspace.

So $W' = W$ or $W' = 0$. Now since $V \otimes W' \longrightarrow U$ is an isomorphism, we have $U = 0$ or $V \otimes W$.

Any irrep$_\sigma$ is of this form: again $\mathrm{Res}_G^{G \times H} \sigma \simeq \rho_1^{\oplus a_1} \oplus \cdots \oplus \rho_k^{\oplus a_k}$ action of H is a $k[G]$-hom, by Schur's lem $\hookrightarrow \begin{cases} \cdot\ \rho_i \longrightarrow \rho_i : \text{scalar} \\ \cdot\ \rho_i \xrightarrow{0} \rho_j \end{cases}$

So each $\rho_i^{\oplus a_i}$: H-inv,

$\underline{k=1}$ and H acts on $\rho_1^{\oplus a_1}$ by each block matrix is a scalar.

i.e. $H \to GL_{a_1}(k)$ ∎

Induced repn

$H < G \rightsquigarrow \mathrm{Mod}_{k[H]} \underset{\mathrm{Res}^G_H}{\overset{\mathrm{Ind}^G_H = k[G]\otimes_{k[H]}}{\rightleftarrows}} \mathrm{Mod}_{k[G]}$ (⊥)

$\mathrm{Ind}^G_H V = k[G] \otimes_{k[H]} V = \bigoplus_{[\sigma]\in G/H} \langle\sigma\rangle \otimes_k V$ ($\langle\sigma\rangle$: 1-dim k-vect sp gen by σ; G acts) $\left((\dim V)\cdot(G:H)\text{-dim'l repn} \right)$

<u>character of induced repn:</u> $\chi_{\mathrm{Ind}V}(g) = \sum_{\substack{[\sigma]\in G/H \\ g[\sigma]=[\sigma]}} \chi_V(\sigma^{-1} g \sigma)$

∵ if $g[\sigma]\neq[\sigma]$, then it doesn't appear in the trace.

(if $g[\sigma]=[\sigma]$ ($\Leftrightarrow g\sigma\in\sigma H \Leftrightarrow \sigma^{-1}g\sigma = h\in H$), then $g(\sigma \otimes_H v) = (\sigma h)\otimes_H v = \sigma\otimes_H hv$, so the trace of the block $g:[\sigma]\otimes V \to [\sigma]\otimes V$ is $\chi_V(h) = \chi_V(\sigma^{-1}g\sigma)$.

S2009 **6.** Let $G = S_4$. Consider the subgroup $H = <(12),(34)>$. $\simeq \mathbb{Z}/2\times\mathbb{Z}/2$

(a). How many simple characters over $\mathbb{C}$ does H have? $|H^{ab}| = |H| = 4$

(b). Choose a non-trivial simple character ψ of H over $\mathbb{C}$ such that $\psi((12)(34)) = -1$. Computer the values of the induced character $\mathrm{ind}^G_H(\psi)$ on conjugacy classes of G, then write the induced character as sum of simple characters.

$\psi : H \longrightarrow \mathbb{C}^\times$

$1_H \longmapsto 1$

$(12) \longmapsto 1$ $\left(\text{or } -1\right)$

$(34) \longmapsto -1$ $\left(\text{or } 1\right)$

$(12)(34) \longmapsto -1$

$V \in \mathbb{C}[H]$-mod (1-dim/$\mathbb{C}$)

$\mathrm{Ind}^G_H \psi$: 6-dim'l repn. $\bigoplus_{[g]\in G/H} [g]V = [1_G]V$

write χ for its character

$\rightsquigarrow \chi : G \longrightarrow \mathbb{C}^\times$

$\chi(1_G) = 6$

$\chi((12)) = \sum_{\substack{[\sigma]\in G/H \\ \sigma^{-1}(12)\sigma\in H}} \chi(\sigma^{-1}(12)\sigma) = \chi(12) + \chi(34) = 0$

$\sigma^{-1}(12)\sigma = (\sigma^{-1}(1)\ \sigma^{-1}(2)) = \begin{cases} (12) & \text{if } \sigma\in H \\ (34) & \text{if } \sigma\in(13)(24)H \end{cases}$

$\chi((123)) = 0$ (no $[\sigma]\in G/H$ satisfies $\sigma^{-1}(123)\sigma\in H$)

$\chi((1234)) = 0$

$\chi((12)(34)) = \sum_{\substack{[\sigma]\in G/H \\ \sigma^{-1}(12)(34)\sigma\in H}} \chi(\sigma^{-1}(12)(34)\sigma) = 2\chi((12)(34)) = -2$

$\sigma^{-1}(12)(34)\sigma = (12)(34) \Leftrightarrow \sigma\in H$ or $(13)(24)H$

Using the character table,

$\mathrm{Ind}^G_H \psi \simeq \mathrm{Std}_4 \oplus \mathrm{Sgn}\otimes\mathrm{Std}_4$

<u>Frobenius Reciprocity</u> $\mathrm{Hom}_G(\mathrm{Ind}^G_H V, W) \cong \mathrm{Hom}_H(V, \mathrm{Res}^G_H W)$ (extension of scalars)

$\dim_k \downarrow$

$\langle \chi_{\mathrm{Ind}V}, \chi_W\rangle_G = \langle \chi_V, \chi_{\mathrm{Res}W}\rangle_H$

S2017

(6) Let G be a finite group and H an abelian subgroup. Show that every irreducible representation of G over $\mathbb{C}$ has dimension $\leq [G:H]$.

Let ρ : irrep of $G/\mathbb{C}$, dim $= d$

$\rightsquigarrow \mathrm{Res}\,\rho \simeq \pi_1 \oplus \cdots \oplus \pi_d$ as repn of H (H abelian $\Rightarrow$ irrep π_i are 1-dim'l)

$\langle \chi_\rho, \chi_{\mathrm{Ind}^G_H \pi_1}\rangle_G = \langle \chi_{\mathrm{Res}\rho}, \chi_{\pi_1}\rangle_H \geq 1$

So ρ is an irred factor of $\mathrm{Ind}^G_H \pi_1$, thus $\dim\rho \leq \dim \mathrm{Ind}^G_H \pi_1 = (G:H)$

S2008 **6.** Give an example of non-isomorphic finite groups with same character table. Construct the character table in detail. D_8 and Q ($D_8^{ab} \cong \mathbb{Z}/2\times\mathbb{Z}/2 \cong Q^{ab}$, + one 2-dim irrep)

char is determined by row orthogonality.

S2012 4. Let Q denote the finite group of quaternions, with presentation

$$Q = \{t, s_i, s_j, s_k \,|\, t^2 = 1,\ s_i^2 = s_j^2 = s_k^2 = s_i s_j s_k = t\}.$$

(a) Determine four non-isomorphic representations of Q of dimension 1 over $\mathbb{R}$.

(b) Show that the natural embedding of Q into the algebra $\mathbb{H}$ of real quaternions ($t \mapsto -1$, $s_i \mapsto i$, $s_j \mapsto j$, $s_k \mapsto k$) defines an irreducible real representation of Q, of dimension 4 over $\mathbb{R}$.

(c) Determine all irreducible representations of Q over $\mathbb{C}$ (up to isomorphism).

(a) $[Q,Q]=\{\pm1\} \rightsquigarrow Q^{ab} = Q/\{\pm1\} \cong \mathbb{Z}/2\times\mathbb{Z}/2$

$\pm1 \longmapsto (0,0)$

$\pm i \longmapsto (1,0)$

$\pm j \longmapsto (0,1)$

$\pm k \longmapsto (1,1)$

$\rightsquigarrow$ 1-dim reprresentations $Q \xrightarrow{\pi} \mathbb{Z}/2\times\mathbb{Z}/2 \xrightarrow{\chi_i} \mathbb{C}^\times$

χ_0 = triv: $(1,0) \longmapsto 1$, $(0,1) \longmapsto 1$

χ_1: $(1,0) \longmapsto 1$, $(0,1) \longmapsto -1$

χ_2: $(1,0) \longmapsto -1$, $(0,1) \longmapsto 1$

χ_3: $(1,0) \longmapsto -1$, $(0,1) \longmapsto -1$

(b) $Q \cong \{\pm1,\pm i,\pm j,\pm k\} \hookrightarrow \mathbb{H}^\times \subset \mathbb{H} = \mathbb{R}1\oplus\mathbb{R}i\oplus\mathbb{R}j\oplus\mathbb{R}k$

$\xrightarrow[\text{group hom}]{\rho} GL_4(\mathbb{R})$ multiplication from the left

No nontrivial subspace is invariant because for any $x\in\mathbb{H}\setminus\{0\}$, x, ix, jx, kx are orthogonal to each other and in particular spans $\mathbb{H}$.

(c) Consider $\mathbb{H}$ as 2-dimensional $\mathbb{C}$-vector space $\mathbb{C}1\oplus\mathbb{C}j$, then this is irreducible (by the same reasoning or computing the character)

Now we have four 1-dim irrep, one 2-dim irrep, and $1^2+1^2+1^2+1^2+2^2=8$, So these are all the $\mathbb{C}$-irreps of Q

	1	-1	$\{\pm i\}$	$\{\pm j\}$	$\{\pm k\}$
triv	1	1	1	1	1
χ_1	1	1	1	-1	-1
χ_2	1	1	-1	1	-1
χ_3	1	1	-1	-1	1
ρ	2	-2	0	0	0

$\rho(\pm i) = \begin{pmatrix} \pm i & 0 \\ 0 & \mp i \end{pmatrix}$, $\rho(\pm j) = \begin{pmatrix} 0 & \pm1 \\ \mp1 & 0 \end{pmatrix}$, $\rho(\pm k) = \begin{pmatrix} 0 & \pm i \\ \pm i & 0 \end{pmatrix}$

(or by column orthogonality)

F2004 **6.** Let D_8 be the dihedral group of order 8, given by generators and relations

$$< r, s \,|\, r^4 = 1 = s^2,\ rs = sr^{-1} >$$

(a) Determine the conjugacy classes of D_8.

(b) Determine the commutator subgroup D_8' of D_8. Determine the number of distinct degree one characters of D_8.

(c) Write down the complete character table of D_8.

More generelly $D_{4n} = \langle \sigma, \tau \,|\, \sigma^{2n} = \tau^2 = 1,\ \sigma\tau = \tau\sigma^{-1} \rangle$

$1+2\cdot(n-1)+1+n+n=4n$

check: $(n+3)$ conj classes $\{1\}$, $\{\sigma^{\pm j}\}$ for $j=1,\dots,n-1$, $\{\sigma^n\}$, $\{\sigma^j\tau \,|\, j:\text{even}\}$, $\{\sigma^j\tau \,|\, j:\text{odd}\}$

$[D_{4n}, D_{4n}] = \{\sigma^{2i} \mid i = 0, \dots, n-1\}$

$$\begin{array}{ccc} D_{4n} & \longrightarrow & D_{4n}^{ab} \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \\ \sigma & \longmapsto & (1, 0) \\ \tau & \longmapsto & (0, 1) \end{array}$$

↳ four 1-dim repn

$1^2 + 1^2 + 1^2 + 1^2 + d_1^2 + \dots + d_{n-1}^2 = 4n$

$\rightsquigarrow \underline{d_i = 2 \quad \forall i}$

	$\{1\}$	$\{\sigma^{\pm j}\}$ $\times n-1$	$\{\sigma^n\}$	$\{\sigma^j\tau \mid j:\text{even}\}$	$\{\sigma^j\tau \mid j:\text{odd}\}$
triv	1	1	1	1	1
χ_1	1	$(-1)^j$	$(-1)^n$	1	-1
χ_2	1	1	1	-1	-1
χ_3	1	$(-1)^j$	$(-1)^n$	-1	1
χ_{ψ_i} $1 \le i \le m-1$	2	$\zeta_{2n}^{ij} + \zeta_{2n}^{-ij}$	$2(-1)^i$	0	0

by explicit calculation $\langle \chi_{\psi_i}, \chi_{\psi_i} \rangle = 1$

Consider the subgroup $H = \langle \sigma \rangle \simeq \mathbb{Z}/2n$

characters $H \xrightarrow{\phi_i} \mathbb{C}^\times$ $(i = 1, \dots, m-1)$ $\quad G/H = \{1, \tau\}$

$\sigma \longmapsto \zeta_{2n}^i \qquad \zeta_{2n} = e^{\frac{\pi i}{n}}$

Let $\psi_i = \mathrm{Ind}_H^G \phi_i \rightsquigarrow \chi_{\psi_i}(\sigma^j) = \phi_i(\sigma^j) + \phi_i(\underbrace{\tau\sigma^j\tau}_{=\sigma^{-j}}) = \zeta_{2n}^{ij} + \zeta_{2n}^{-ij}, \ \chi(\sigma^j\tau) = 0$

F2000

7. Let D_{10} be the dihedral group of order 10, given by the usual generators and relations

$$D_{10} = \langle r, s \,|\, r^5 = 1 = s^2, rs = sr^{-1} \rangle$$

(1) Compute the conjugacy classes of D_{10}.
(2) Compute the commutator subgroup D'_{10} of D_{10}.
(3) Show that D_{10}/D'_{10} is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and conclude that D_{10} has precisely two distinct characters of degree 1.
(4) Write down the complete character table of D_{10}.

$G = D_{4n+2} = \langle \sigma, \tau \mid \sigma^{2n+1} = \tau^2 = 1, \ \sigma\tau = \tau\sigma^{-1} \rangle$

Conj classes $\{1\}, \{\sigma^{\pm j}\}$ $j = 1, \dots, n$, $\{\sigma^j\tau \mid j = 0, \dots, 2n\}$

$[G, G] = \langle \sigma \rangle \rightsquigarrow G^{ab} \simeq \mathbb{Z}/2$

$\psi_i = \mathrm{Ind}_{\langle\sigma\rangle}^G \phi_i, \quad \phi_i : \langle \sigma \rangle \longrightarrow \mathbb{C}^\times$

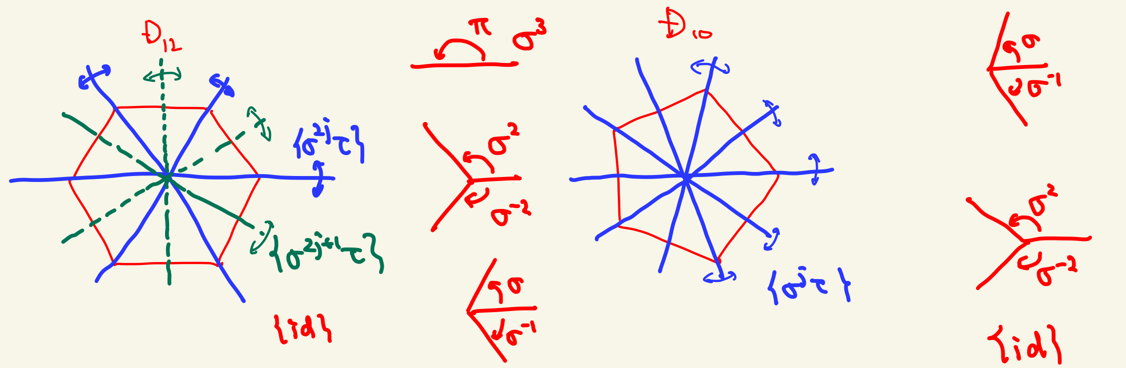
$\sigma \longmapsto \zeta_{2n+1}^i \qquad \zeta_{2n+1} = e^{\frac{2\pi i}{2n+1}}$

	1	$\{\sigma^{\pm j}\}$	$\{\sigma^j\tau\}$
1	1	1	1
sgn	1	1	-1
χ_{ψ_i}	2	$\zeta_{2n+1}^i + \zeta_{2n+1}^{-i}$	0

→ 2-dim irreps (on $\mathbb{R}$) are $\sigma \mapsto \begin{pmatrix} \cos\frac{2\pi j}{n} & -\sin\frac{2\pi j}{n} \\ \sin\frac{2\pi j}{n} & \cos\frac{2\pi j}{n} \end{pmatrix}$, $\tau \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

(one can do the same ind technique for $\mathbb{Z}/p \rtimes \mathbb{Z}/n$ and this is harder to do explicitly)

Conjugacy class of dihedral groups are easily seen geometrically :



Semisimple algebra A (noncommutative) ring (with 1)

- M: (left) A-mod is <u>simple</u> $\Leftrightarrow$ nonzero, no nontrivial proper submod

  <u>semisimple</u> $\Leftrightarrow M \simeq \bigoplus M_i$, M_i: simple $\Leftrightarrow \forall N \subset M\ \exists P\ M \simeq N \oplus P$ (Zorn)

  possibly infinite

- A is simple $\Leftrightarrow$ nonzero, no nontrivial proper two-sided ideal ($\rightsquigarrow$ semisimple modules are closed under sub/quotients)

  (left) <u>semisimple</u> $\Leftrightarrow$ semisimple as left A-mod ($\Leftrightarrow \bigoplus_{\text{finite}}$ minimal left ideals)

  $\Leftrightarrow \forall$ (left/right) A-module is semisimple (or right) $\Leftrightarrow \forall$ mod is completely reducible

  $\Leftrightarrow \forall$ exact sequence of A-mods splits

  Artin-Wedderburn $\Leftrightarrow R \cong \mathrm{Mat}_{n_1}(D_1) \times \cdots \times \mathrm{Mat}_{n_r}(D_r)$ where $D_1, \dots, D_r$ division rings

  $\Leftrightarrow \forall A$-mod is projective $\Leftrightarrow \forall A$-mod is injective

  $r, n_1, \dots, n_r, D_1, \dots, D_r$: uniquely determined by R up to ordering

F2019 5. How many two-sided ideals has the group algebra $\mathbb{C}[S_3]$, where S_3 is the group of permutations of $\{1,2,3\}$?

Wedderburn decomposition

$\mathbb{C}[S_3] \simeq \mathrm{Mat}_1(\mathbb{C}) \times \mathrm{Mat}_1(\mathbb{C}) \times \mathrm{Mat}_2(\mathbb{C})$ all two-sided ideals are sum of these, so

(as left mod $\underset{\text{triv}}{\cong}$, $\underset{\text{sgn}}{\cong}$, $\mathrm{End}_{\mathbb{C}}(\mathrm{std}) \simeq \mathrm{std}^{\oplus 2}$ ← 2-dim irrep) there are $2^3 = 8$ of those.

F2009
F2001

6. Let $\rho : G \to Gl_n(\mathbb{C})$ be a complex irreducible representation of a finite group G. Let χ be its associated character and let C be the center of G.

(a). Show that, for all $s \in C$, $\rho(s)$ is a <u>scalar multiple</u> of the identity matrix I_n. ← Schur's lemma λ: roots of unity

(b). Use (a) to show that $|\chi(s)| = n$, for all $s \in C$. $\rightarrow |\chi(s)| = |\mathrm{tr}(\lambda I)| = n$.

(c). Prove the inequality $n^2 \le [G : C]$, where $[G : C]$ denotes the index of C in G.

(d). Show that, if ρ is faithful (i.e., an injective group homomorphism), then C is cyclic. ← finite subgroup of $\mathbb{C}^\times$ is cyclic

(c)
$$\begin{tikzcd} G \arrow[r, "\rho"] \arrow[d, hook] & GL(V) \arrow[d, hook] \\ \mathbb{C}[G] \arrow[r, "\bar\rho"] & \mathrm{End}_{\mathbb{C}}(V) \end{tikzcd}$$

ρ extends to a $\mathbb{C}$-algebra hom $\bar\rho$ and, if (V, ρ) is irreducible (i.e. $\mathbb{C}[G] \to \mathrm{End}(V)$ exhibits V as a simple $\mathbb{C}[G]$-module), then $\bar\rho$ is a projection onto is Wedderburn component, in particular surjective.

Therefore $\dim_{\mathbb{C}}(\mathbb{C}[G]/\ker\bar\rho) = n^2$. Now it suffices to see that representatives of cosets G/C generate $\mathbb{C}[G]/\ker\bar\rho$, in fact, if $g = g'c$, then $\bar\rho(g) = \bar\rho(g') \cdot \lambda_c$ where $\lambda_c \in \mathbb{C}^\times$ (by (a)). $\square$

S2017 (5) Prove directly from the definition of (left) semisimple ring that every such ring is (left) Noetherian and Artinian. (You may freely use facts about semisimple, Noetherian, and Artinian modules.)

R: left semisimple $\underset{\text{def}}{\Longleftrightarrow}$ R: semisimple left R-module, so $R \cong \bigoplus_{i \in I} L_i$ for L_i: simple left ideals.

$1 \mapsto (e_i)$ (only finitely many $e_i \neq 0$ $\Rightarrow \bigoplus$: finite sum)

So let $R = L_1 \oplus \cdots \oplus L_n$. We need to prove that its length is finite.

Consider $0 \subsetneq L_1 \subsetneq L_1 \oplus L_2 \subsetneq \cdots \subsetneq L_1 \oplus \cdots \oplus L_{n-1} \subsetneq R$. We prove that it is a composition series.

If any other left ideal M satisfies $L_1 \oplus \cdots \oplus L_k \subset M \subset L_1 \oplus \cdots \oplus L_{k+1}$, then taking the quotient module $0 \subset M/L_1 \oplus \cdots \oplus L_k \subset L_{k+1}$, so by simplicity of L_{k+1}, M must be either $L_1 \oplus \cdots \oplus L_k$ or $L_1 \oplus \cdots \oplus L_{k+1}$.

S2005 **4.** Let R be a ring. Let L be a minimal left ideal of R (i.e., L contains no nonzero proper left ideal of R). Assume $L^2 \neq 0$. Show that $L = Re$ for some non-zero idempotent $e \in R$.

$\exists x \in L$ s.t. $Lx \neq 0$, since Lx is a nonzero submodule of L, we have $Lx = L$.
$\leadsto \exists e \in L$ s.t. $ex = x$, so $(e^2 - e)x = 0$. Now $\mathrm{Ann}_L(x) = \{y \in L \mid yx = 0\} \subsetneq L$ is a left submodule, so $\mathrm{Ann}_L(x) = 0$, and thus e is a nonzero idempotent.
Since Re is a nonzero left submodule of L, $Re = L$. $\square$

S2016 F2006 F2008 6. Let A be a semi-simple finite dimensional algebra over $\mathbb{C}$, and let V be a direct sum of two isomorphic simple A-modules. Find the automorphism group of the A-module V.

$V \cong E \oplus E$, where E: simple A-mod. Note that by Schur's lemma, $\mathrm{End}_V(E) \cong \mathbb{C}$
Therefore $\mathrm{End}_A(V) \cong \mathrm{Mat}_2(\mathbb{C})$. Its invertible elements are $\mathrm{Aut}_A(V) \cong GL_2(\mathbb{C})$.

S2010 **5.** Classify all non-commutative semi-simple rings with 512 elements. (You can use the fact that finite division rings are fields.)

By Artin-Wedderburn's theorem, semi-simple rings are of the form
$A = \mathrm{Mat}_{n_1}(k_1) \times \cdots \times \mathrm{Mat}_{n_\ell}(k_\ell)$, where k_i's are division rings. If k_i is infinite, then A is infinite as well, so we have k_i: finite division rings, i.e. $k_i \cong \mathbb{F}_{q_i}$ (q_i: power of a prime). Now we need to classify $\{(n_i, q_i)\}$ such that $q_1^{n_1^2} \cdot q_2^{n_2^2} \cdot \cdots \cdot q_\ell^{n_\ell^2} = 512$ with at least one $n_i > 1$ (since A: noncomm.)
We may assume $n_1 \geq 2$. If $n_1 = 3$, then $A \cong \mathrm{Mat}_3(\mathbb{F}_2)$.
If $n_1 = 2$, then $A \cong \mathrm{Mat}_2(\mathbb{F}_4) \times \mathbb{F}_2$ or $A \cong \mathrm{Mat}_2(\mathbb{F}_2) \times \mathrm{Mat}_2(\mathbb{F}_2) \times \mathbb{F}_2$ or $A \cong \mathrm{Mat}_2(\mathbb{F}_2) \times \begin{cases} \mathbb{F}_{32} \\ \mathbb{F}_{16} \times \mathbb{F}_2 \\ \mathbb{F}_8 \times \mathbb{F}_4 \\ \mathbb{F}_4^2 \times \mathbb{F}_2 \\ \mathbb{F}_8 \times \mathbb{F}_2^2 \\ \mathbb{F}_4 \times \mathbb{F}_2^3 \\ \mathbb{F}_2^5 \end{cases}$

Comm. semisimple ring with 32 elements

F2011 5. Let A be a finite-dimensional semisimple algebra over $\mathbb{C}$, and V an A-module of finite type (i.e., finitely-generated as an A-module). Prove that V has only finitely many A-submodules if and only if V is a direct sum of pairwise non-isomorphic irreducible (i.e., simple) A-modules.

By Artin-Wedderburn theorem $A \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_k}(\mathbb{C})$. Since A-module is a product of modules over $M_{n_i}(\mathbb{C})$, we may assume A is simple $\cong M_n(\mathbb{C})$.
In this case there is only one simple A-module, namely $M = \mathbb{C}^n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \middle| x_1, \dots, x_n \in \mathbb{C} \right\}$, up to isomorphism.
It has only two submods (0 and itself), and conversely, $M \oplus M \cong \left\{ \begin{pmatrix} x_{11} & x_{12} \\ \vdots & \vdots \\ x_{n1} & x_{n2} \end{pmatrix} \middle| x_{ij} \in \mathbb{C} \right\}$ has infinitely many submodules $A \cdot \begin{pmatrix} 1 & \lambda \\ 0 & 0 \\ \vdots & \vdots \\ 0 & 0 \end{pmatrix}$ $(\forall \lambda \in \mathbb{C})$ isomorphic to M. $\square$

f.g. modules / PID, triangularization, diagonalization, Jordan can. form, etc.

Structure theorem of f.g. modules / Dedekind domain A

$$M \cong \mathfrak{a} \oplus A^{\oplus r} \oplus A/\mathfrak{b}_1 \oplus \cdots \oplus A/\mathfrak{b}_s, \quad \begin{cases} \cdot\ \mathfrak{b}_1 \subset \cdots \subset \mathfrak{b}_s \subsetneq A & \text{elementary divisors} \\ \cdot\ r \in \mathbb{Z}_{\geq 0} & \text{rank} \\ \cdot\ \mathfrak{a} : \text{fractional ideal, uniquely determined} \\ \quad \text{up to principal fractional ideal} \\ (\rightsquigarrow [\mathfrak{a}] \in Cl_A \text{ ideal class gp : Steiniz class} \end{cases}$$

$\}$ when A: PID

$$M \cong A^{\oplus r} \oplus A/(b_1) \oplus \cdots \oplus A/(b_s)$$
$$(b_s \mid b_{s-1} \mid \cdots \mid b_1 \in A)$$

$\boxed{\text{Fall 2018}}$

Question 1. Let V be an n-dimensional vector space over a field k and let $\alpha\colon V \to V$ be a linear endomorphism.
Prove that the minimal and characteristic polynomials of α coincide if and only if there is a vector $v \in V$ so that:

$$\{v, \alpha(v), \ldots, \alpha^{n-1}(v)\}$$

is a basis for V.

Question 3. (a) Fix a positive integer n and classify all finite modules over the ring $\mathbb{Z}/n$.

(b) Prove, either using (a) or from first principles, for a fixed prime p that all finite modules over $\mathbb{Z}/p$ are free.

<u>Q3</u> ⚠ $\mathbb{Z}/n$ not PID

(a) M: finite module over $\mathbb{Z}/n$

$\iff$ finite module over $\mathbb{Z}$, $n\mathbb{Z}$ act on M by 0 (i.e. $n\mathbb{Z} \subset \mathrm{Ann}_{\mathbb{Z}} M$)

By the structure thm

$$\underline{M \cong \mathbb{Z}/m_1 \oplus \mathbb{Z}/m_2 \oplus \cdots \oplus \mathbb{Z}/m_k, \quad 1 < m_k \mid \cdots \mid m_1,}$$

annihilated by $n \iff \underline{m_1 \mid n}$.

(b) $n = p \rightsquigarrow m_1 = \cdots = m_k = p$. free $\mathbb{Z}/p$-mod of rank k.

<u>Q1</u> k-module V with $V \xrightarrow{\alpha} V \iff k[\alpha]$-module

$$k[\alpha] = k[X]/(f(X)) \quad f(X): \text{minimal polynomial of } \alpha.$$

PID

V is a $k[X]$-module with $\mathrm{Ann}_{k[X]} V = (f(X))$

Structure thm $\rightsquigarrow V \cong k[X]/(g_1(X)) \oplus \cdots \oplus k[X]/(g_k(X))$, $\deg g_k > 0$, $g_k(X) \mid \cdots \mid g_1(X)$

· Now $\mathrm{Ann}_{k[X]} V = (g_1(X))$, i.e. $(g_1(X)) = (f(X))$ (may assume both are monic $\rightsquigarrow f = g_1$

· characteristic polynomial $= g_1(X) g_2(X) \cdots g_k(X)$ ($\because \det(A_1 \oplus \cdots \oplus A_k) = \det(A_1) \cdots \det(A_k)$)

So char. poly = min. poly $\iff k = 1 \iff V$ is generated by one element as an $k[\alpha]$-module

$\boxed{\text{Q}}$

F2017

(2) Let Λ be a free abelian group of finite rank n, and let $\Lambda' \subset \Lambda$ be a subgroup of the same rank. Let $x_1, \ldots, x_n$ be a $\mathbb{Z}$-basis for Λ, and let $x'_1, \ldots, x'_n$ be a $\mathbb{Z}$-basis for Λ'. For each i, write $x'_i = \sum_{j=1}^{n} a_{ij} x_j$, and let $A := (a_{ij}) \in \mathrm{Mat}_{n\times n}(\mathbb{Z})$. Show that the index $[\Lambda : \Lambda']$ equals $|\det A|$.

$$\begin{array}{ccccc}
\Lambda' & \xhookrightarrow{f} & \Lambda & \twoheadrightarrow & \operatorname{cok} f \\
\wr\| & & \wr\| & & \wr\| \\
\mathbb{Z}^n & \xrightarrow{\cdot(a_{ij})} & \mathbb{Z}^n & \twoheadrightarrow & \mathbb{Z}/m_1 \oplus \cdots \oplus \mathbb{Z}/m_k \\
\in & & \in & & \\
e_i & \longmapsto & a_{ij}e_j & &
\end{array}$$

- $[\Lambda : \Lambda'] = |\operatorname{Cok} f| = m_1 \cdots m_k$.
- In general. $A \in M_n(\mathbb{Z})$ can be turned into
$$\left(\begin{array}{c|c} \begin{matrix} m_1 & & & \\ & m_2 & & \\ & & \ddots & \\ & & & m_k \end{matrix} & \\ \hline & 0 \end{array}\right)$$
using row & column operations.

$m_1 | \cdots | m_k$, $m_i \in \mathbb{Z}_{>0}$

In our case $k = n$ since Λ' is of full rank,
So $|\det A| = m_1 \cdots m_k = [\Lambda : \Lambda']$.

S2001

5. (a) Prove that an $n \times n$ matrix A with entries in the field $\mathbb{C}$ of complex numbers, satisfying $A^3 = A$, can be diagonalized over $\mathbb{C}$. min poly divides $\lambda^3 - \lambda \rightsquigarrow$ product of distinct linear factors.
(b) Does the statement in (a) remain true if one replaces $\mathbb{C}$ by an arbitrary algebraically closed field F ? Why or why not ? No, if char $k=2$, min poly can be $(\lambda-1)^2$.

F2001

3. Assume that A is an $n\times n$ matrix with entries in the field of complex numbers $\mathbb{C}$ and $A^m = 0$ for some integer $m > 0$. minimal polynomial is $f(x) = x^m$ for the smallest such m.
(a) Show that if λ is an eigenvalue of A, then $\lambda = 0$. $f(\lambda) = 0 \Rightarrow \lambda = 0$
(b) Determine the characteristic polynomial of A. x^n
(c) Prove that $A^n = 0$. Cayley-Hamilton
(d) Write down a 5×5 matrix B for which $B^3 = 0$ but $B^2 \neq 0$.
$$\left(\begin{array}{ccc|cc} 0 & 1 & 0 & & \\ 0 & 0 & 1 & \multicolumn{2}{c}{0} \\ 0 & 0 & 0 & & \\ \hline \multicolumn{3}{c|}{0} & \multicolumn{2}{c}{0} \end{array}\right) \quad \left(\text{or } \left(\begin{array}{ccc|cc} 0 & 1 & 0 & & \\ 0 & 0 & 1 & \multicolumn{2}{c}{0} \\ 0 & 0 & 0 & & \\ \hline \multicolumn{3}{c|}{0} & 0 & 1 \\ & & & 0 & 0 \end{array}\right)\right)$$
(e) If M is any 5×5 matrix over $\mathbb{C}$ with $M^3 = 0$ and $M^2 \neq 0$, must M be similar to the matrix B you found in part (d) ? Justify your answer.

No. There are two $k[x]$-mod of $\dim = 5$ with annihilator $= (x^3)$: $k[x]/(x^3) \times k[x]/(x) \times k[x]/(x)$
and $k[x]/(x^3) \times k/(x^2)$

2018F

Question 4. In this question all modules are left modules.

Let k be a field of characteristic different from 2 and let $G = \{e, g\}$ be the multiplicative group with two elements. Consider the group ring $A = k[G] \cong k[x]/(x^2-1)$

(a) Show that the A-module A is a direct sum of two ideals of A.
List all proper ideals of A $\quad k[x]/(x^2-1) \cong k[x]/(x-1) \times k[x]/(x+1)$
Is A a principal ideal domain? no (not an integral domain)

each of these are sum of copies of $k[x]/(x-1)$, $k[x]/(x+1)$

(b) Show that every A-module decomposes into a direct sum of simple A-modules. $f : M \to M$ be the action of $X \rightsquigarrow M \xrightarrow{\left(\frac{f+1}{2}, \frac{1-f}{2}\right)} \operatorname{Ker}(f-1) \oplus \operatorname{Ker}(f+1)$
$a \longmapsto (a_1, a_2)$ $\quad \left(a_1 + a_2 = \frac{f(a)+1}{2} + \frac{1-f(a)}{2} = a\right)$

Assume now that the characteristic of the field k is 2

(c) Give an example of an A-module that cannot be decomposed into a direct sum of two simple A-modules. A itself : $A \cong k[x]/(x-1)^2$

The only nontrivial ideal is $(x-1)/(x-1)^2$.

S2003

3. Prove that if a linear operator on a complex vector space is diagonal in some basis, then its restriction on any invariant subspace L is also diagonal in some basis of L.

$V \xrightarrow[f]{} V$ diagonalizable $\Longleftrightarrow$ minimal polynomial P of $f = \prod (x - \lambda_i)$ for λ_i distinct

$P(f|_L) = P(f)|_L = 0 \Rightarrow$ min poly of $f|_L$ divides P. satisfies the same.

S2017
F2006

(4) Let M be an invertible $n \times n$ matrix with entries in an algebraically closed field k of characteristic not 2. Show that M has a square root, i.e. there exists $N \in \mathrm{Mat}_{n\times n}(k)$ such that $N^2 = M$.

Consider the Jordan canonical form $P^{-1}MP = \begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_k \end{pmatrix}$

It suffices to find K_i s.t. $J_i = K_i^2$, because then $N = P\begin{pmatrix} K_1 & & \\ & \ddots & \\ & & K_{k} \end{pmatrix}P^{-1}$ satisfies $N^2 = K$.

Now for $J_i = \begin{pmatrix} \lambda & 1 & & \\ & \lambda & 1 & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix} = \underset{\neq 0}{\lambda} I + A$, $A = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & & 1 \\ & & & 0\end{pmatrix}$, we can take $K_i = \lambda^{1/2} \sum_{i=0} \binom{1/2}{i} (\lambda^{-1}A)^i$ ▨

use char $k \neq 2$

S2008

1. Let k be a field. Consider the subgroup $B \subset GL_2(k)$ where

$$B = \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in k,\ ad \neq 0\}.$$

(a). Let Z be the center of $GL_2(k)$. Show that

$$\bigcap_{x \in GL_2(k)} x^{-1}Bx = Z.$$

(b). Assume k is algebraically closed. Show that

$$\bigcup_{x \in GL_2(k)} x^{-1}Bx = GL_2(k).$$ $\Leftrightarrow$ Any matrix is triangulizable

(c). Assume k is a finite field. Can the statement in (b) still be true?

(a)
$y \in$ LHS
$\Leftrightarrow \forall x\ xyx^{-1} \in B$
$\Leftrightarrow \forall x\ xyx^{-1}\begin{pmatrix}0\\1\end{pmatrix} \in \langle\begin{pmatrix}0\\1\end{pmatrix}\rangle$
$\Leftrightarrow \forall x\ x^{-1}\begin{pmatrix}0\\1\end{pmatrix}$ is an eigenvector of y
$\Leftrightarrow$ The whole k^2 is the eigensp of y
$\Leftrightarrow y$: scalar $\Leftrightarrow y \in Z$

2×2 matrix is triangulizable iff $\exists$ eigenvector.
This is not always the case for $k = \mathbb{F}_q$ because there exists a irred poly of degree 2.
e.g. take any $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, then $\mathbb{F}_{q^2} \xrightarrow{\alpha} \mathbb{F}_{q^2}$ is a linear map of 2-dim $\mathbb{F}_q$-vect. sp.
whose minimal polynomial is irreducible ($\Rightarrow$ no root)

S2009

4. Let E be a finite-dimensional vector space over an algebraically closed field k. Let A, B be k-endomorphisms of E. Assume $AB = BA$. Show that A and B have a common eigenvector.

Let λ be an eigenvalue of A, and $V = \mathrm{Ker}(A - \lambda I) \subset E$.
V is B-invariant, since $v \in V \Rightarrow ABv = BAv = B\lambda v = \lambda Bv \Rightarrow Bv \in V$.
Taking any eigenvector of $V|_B$ we are done.

F2005

6. Let E be a finite-dimensional vector space over a field k. Assume $S, T \in \mathrm{End}_k(E)$. Assume $ST = TS$ and both of them are diagonalizable. Show that there exists a basis of E consisting of eigenvectors for both S and T.

The same argument $\Rightarrow$ $A = \bigoplus_\lambda \mathrm{Ker}(A - \lambda I)$ each eigenspace is B-invariant, by S2003 (previous page)
(or use induction & S2009.4 above)
each eigenspace decompose into B-eigenspaces

S2015

2. Let A, B be two commuting operators on a finite dimensional space V over $\mathbb{C}$ such that $A^n = B^m$ is the identity operator on V for some positive integers n, m. Prove that V is a direct sum of 1-dimensional invariant subspaces with respect to A and B simultaneously.

The data of $(V, A, B) \leftrightarrow \mathbb{C}$-repn of $\underset{G=}{\mathbb{Z}/n \times \mathbb{Z}/m}$. Decompose into irreps, and irrep of abelian group is 1-dim'l.

can be taken as circular reasoning. direct proof:

If not 1-dim'l, may assume $\exists g \in G$ acts not by a scalar. Any eigensp of $g \curvearrowright V$ is a proper G-invariant subsp (so V: not irred)

Exterior power, Tensor Algebra, traces, determinants

F2016

5. Let A be a linear transformation of a finite dimensional vector space V over a field of characteristic $\neq 2$.

(1). Define the wedge product linear transformation $\wedge^2 A = A \wedge A$.

(2). Prove that

$$tr(\wedge^2 A) = \frac{1}{2}(\,tr(A)^2 - tr(A^2)\,).$$

(1) Let $V \times V \xrightarrow{f} V \wedge V$ be the canonical map.

Since

$$\begin{tikzcd} V \times V \arrow[r, "A \times A"] \arrow[d, "f"] & V \times V \arrow[r, "f"] & V \wedge V \\ V \wedge V \arrow[urr, dashed] & & \end{tikzcd}$$

is alternating bilinear

$\exists !\, A \wedge A$: linear map making the diagram commute. (which sends $v_1 \wedge v_2 \longmapsto Av_1 \wedge Av_2$)

(2) May extend the scalar to $\bar{k}$.

Take a basis $e_1, \dots, e_n$ that triangulize A with $Ae_i = \lambda_i e_i$. $\rightsquigarrow (A \wedge A)\, e_i \wedge e_j = \lambda_i \lambda_j (e_i \wedge e_j)$.

so $Tr(A \wedge A) = \sum_{i<j} \lambda_i \lambda_j = \frac{1}{2}\left((\sum \lambda_i)^2 - \sum \lambda_i^2\right) = \frac{1}{2}\left((tr A)^2 - tr(A^2)\right)$.

S2006 **5.** Let V be a finite-dimensional vector space over a field k. Let $T \in End_k(V)$. Show that $tr(T \otimes T) = (tr(T))^2$. Here $tr(T)$ is the trace of T. Similar

S2016 4. Let V and W be two finite dimensional vector spaces over a field K. Show that for any $q > 0$,

$$\bigwedge^q (V \oplus W) \cong \sum_{i=0}^{q} (\bigwedge^i (V) \otimes_K \bigwedge^{q-i}(W)).$$

$$\begin{tikzcd} \underbrace{V \times \cdots \times V}_{i} \times \underbrace{W \times \cdots \times W}_{q-i} \arrow[r, hook] \arrow[d] & (V \oplus W) \times \cdots \times (V \oplus W) \arrow[r] & \wedge^q (V \oplus W) \\ (V \wedge \cdots \wedge V) \otimes (W \wedge \cdots \wedge W) \arrow[urr, dashed, "f_i"] & & \end{tikzcd}$$

$(v_1, \dots, v_i, w_1, \dots, w_{q-i}) \longmapsto v_1 \wedge \cdots \wedge v_i \wedge w_1 \wedge \cdots \wedge w_{q-i}$

is multilinear, and alternating in V and W factors separately, so this map factors through

Then $f: \bigoplus_{i=0}^{q} (\wedge^i V) \otimes (\wedge^{q-i} W) \xrightarrow[(f_0, \dots, f_q)]{} \wedge^q (V \oplus W)$ is surjective (because elements of the form $v_1 \wedge \cdots \wedge v_i \wedge w_1 \wedge \cdots \wedge w_{q-i}$ generate the codomain)

and since $\dim\left(\bigoplus_{i=0}^{q} (\wedge^i V) \otimes (\wedge^{q-i} W)\right) = \sum_{i=0}^{q} \left(\binom{\dim V}{i} \cdot \binom{\dim W}{q-i}\right) = \binom{\dim V + \dim W}{q} = \dim(\wedge^q V \oplus W)$, f is an isomorphism.

S2011 4. Let F be a field, and V a finite-dimensional vector space over F, with $\dim_F V = n$.

(a) Prove that if $n > 2$, the spaces $\bigwedge^2(\bigwedge^2(V))$ and $\bigwedge^4(V)$ are not isomorphic. $n \geq 2 \rightsquigarrow$ dimension: $\binom{\binom{n}{2}}{2} = \binom{n}{4}$ iff $(n-2)(n+3) = 0$, so this does not happen when $n \geq 3$.

(b) Let k be a positive integer. Prove that when $v \in \bigwedge^k(V)$ and $0 \neq x \in V$, $v \wedge x = 0$ holds if and only if $v = x \wedge y$ for some $y \in \bigwedge^{k-1}(V)$.

$V = \langle x \rangle \oplus W$

$\rightsquigarrow \wedge^k V \cong \bigoplus_{i+j=k} (\wedge^i \langle x \rangle) \otimes_F (\wedge^j W)$

$\cong (\wedge^k W) \oplus (\langle x \rangle \otimes \wedge^{k-1} W)$.

Therefore

$$\begin{tikzcd} \wedge^{k-1} V \arrow[r, "x \wedge"] \arrow[d, phantom, "\text{\rotatebox{90}{$\cong$}}"] & \wedge^k V \arrow[r, "x \wedge"] \arrow[d, phantom, "\text{\rotatebox{90}{$\cong$}}"] & \wedge^{k+1} V \arrow[d, phantom, "\text{\rotatebox{90}{$\cong$}}"] \\ \wedge^{k-1} W \oplus \langle x \rangle \otimes \wedge^{k-2} W \arrow[r, "\cong"] & \wedge^k W \oplus \langle x \rangle \otimes \wedge^{k-1} W \arrow[r, "\cong"] & \wedge^{k+1} W \oplus \langle x \rangle \otimes \wedge^k W \end{tikzcd}$$

is exact.

S2010

4. Let V be a n-dimensional vector space over a field k. Let $T \in End_k(V)$.
(a). Show that $tr(T \otimes T \otimes T) = (tr(T))^3$. Here $tr(T)$ is the trace of T.
(b). Find a similar formula for the determinant $det(T \otimes T \otimes T)$.

(b) For any V, $f \in End(V)$,

$$\begin{tikzcd} \Lambda^{\dim V} V \arrow[r, "\Lambda^{\dim V} f"] \arrow[d, "\varphi"', "\cong"] & \Lambda^{\dim V} V \arrow[d, "\varphi", "\cong"'] \\ k \arrow[r, "\det f"] & k \end{tikzcd}$$

For any $V \xrightarrow{T} V$, $\dim = n$
$W \xrightarrow{S} W$, $\dim = m$

$\Lambda^{nm}(V\otimes W) \xrightarrow{f} U$

$\Longleftrightarrow \prod_{i=1}^{nm} V\times W \xrightarrow{f} U$; linear on each component.

$\cong \prod_{i=1}^{nm} V \times \prod_{i=1}^{nm} W$ · alternating on on perm of $\prod_{i=1}^{nm}$ factors.

$\Longleftrightarrow (\Lambda^n V)^{\otimes m} \otimes (\Lambda^m W)^{\otimes n} \longrightarrow U$

$S_n \times S_m \hookrightarrow S_{nm}$

$$\begin{tikzcd} k \arrow[d, "\det(T\otimes S)"'] & \Lambda^{nm}(V\otimes W) \arrow[l, "\cong"'] \arrow[r, "\cong"] \arrow[d, "\Lambda^{nm}(T\otimes S)"] & (\Lambda^n V)^{\otimes m} \otimes (\Lambda^m W)^{\otimes n} \arrow[r, "\cong"] \arrow[d, "(\Lambda^n T)^{\otimes m} \otimes (\Lambda^m S)^{\otimes n}"] & k \arrow[d, "(\det T)^m (\det S)^n"] \\ k & \Lambda^{nm}(V\otimes W) \arrow[l, "\cong"'] \arrow[r, "\cong"] & (\Lambda^n V)^{\otimes m} \otimes (\Lambda^m W)^{\otimes n} \arrow[r, "\cong"] & k \end{tikzcd}$$

So $\det(T\otimes S) = (\det T)^m (\det S)^n$.

Now $\det(T\otimes T\otimes T) = (\det T)^{n^2} \det(T\otimes T)^n = (\det T)^{n^2} ((\det T)^n \det T)^n)^n$
$= (\det T)^{3n^2}$

Random problems (linear algebra, etc.)

S2013 5. Let A and B be $n \times n$ matrices with complex coefficients. Assume that $(A-I)^n = 0$ and $A^kB = BA^k$ for some natural number k. Prove that $AB = BA$ (Hint: Prove that A can be expressed as a function of A^k).

$A = I + N$, $N^n = 0$ $\rightsquigarrow$ $A^k = I + kN + \binom{k}{2}N^2 + \cdots + \binom{k}{n-1}N^{n-1}$

$$A^{2k} = I + (2k)N + \binom{2k}{2}N^2 + \cdots + \binom{2k}{n-1}N^{n-1}$$

$$\vdots$$

i.e.

$$\begin{pmatrix} A^k \\ A^{2k} \\ \vdots \\ A^{nk} \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & k & \binom{k}{2} & \cdots & \binom{k}{n-1} \\ 1 & 2k & \binom{2k}{2} & \cdots & \binom{2k}{n-1} \\ \vdots & & & \ddots & \vdots \\ 1 & nk & & \cdots & \binom{nk}{n-1} \end{pmatrix}}_{P} \begin{pmatrix} I \\ N \\ N^2 \\ \vdots \\ N^{n-1} \end{pmatrix} \text{ in } \mathrm{End}(\mathbb{C}^n).$$

If $\det P \neq 0$, then $\exists P^{-1} \in GL_n(\mathbb{C})$, so

$$\begin{pmatrix} I \\ N \\ \vdots \\ N^{n-1} \end{pmatrix} = P^{-1} \begin{pmatrix} A^k \\ \vdots \\ A^{nk} \end{pmatrix} \text{ and}$$

in particular $A = I + N$ is a $\mathbb{C}$-coeff linear combination of A^{ik} $(0 \leq i \leq n)$, so $AB = BA$.

Now by successively applying elementary column operations we see that

$$\det P = \det \begin{pmatrix} 1 & k & k^2 & \cdots & k^{n-1} \\ 1 & 2k & (2k)^2 & \cdots & \vdots \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & nk & (nk)^2 & \cdots & (nk)^{n-1} \end{pmatrix} \underset{\text{Vandermonde}}{=} \prod_{1 \leq i < j \leq n} (j-i)k \neq 0.$$

F2011 2. Consider the special orthogonal group $G = SO(3, \mathbb{R})$, namely,

$$G = \{A \in GL(3, \mathbb{R}) : \ A^T A = \mathrm{I}_3, \ det(A) = 1\}$$

(a) Show that for any element A in G, there exists a real number α with $-1 \leq \alpha \leq 3$ such that

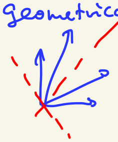
$$A^3 - \alpha A^2 + \alpha A - \mathrm{I}_3 = 0.$$

(b) For which real numbers α with $-1 \leq \alpha \leq 3$ does there exist an element A in G whose minimal polynomial is $x^3 - \alpha x^2 + \alpha x - 1$? *Explain your answer.*

$$A \sim \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

F2007 3. Let $A = \binom{a\,b}{c\,d}$ be a real matrix such that $a, b, c, d > 0$. (1) Prove that A has two distinct real eigenvalues, $\lambda > \mu$. (2) Prove that λ has an eigenvector in the first quadrant and μ has an eigenvector in the second quadrant.

geometrically:



but the proof is just some explicit calculation

S2007 1. Prove that the integer orthogonal group $O_n(\mathbf{Z})$ is a finite group. (By definition, an $n \times n$ square matrix X over $\mathbf{Z}$ is orthogonal if $XX^t = I_n$.)

Compact + discrete $\Rightarrow$ finite

F2008
F2007
S2003

4. A differentiation of a ring R is a mapping $D : R \to R$ such that, for all $x, y \in R$,

(1) $D(x+y) = D(x) + D(y)$; and

(2) $D(xy) = D(x)y + xD(y)$.

If K is a field and R is a K-algebra, then its differentiation are supposed to be over K, that is,

(3) $D(x) = 0$ for any $x \in K$.

Let D be a differentiation of the K-algebra $M_n(K)$ of $n \times n$-matrices. Prove that there exists a matrix $A \in M_n(K)$ such that $D(X) = AX - XA$ for all $X \in M_n(K)$.

too much prerequisite
more direct solution?

R: assoc. alg $/k$ $\rightsquigarrow$ cyclic bar construction $\cdots \to R^{\otimes 4} \to R^{\otimes 3} \to R\otimes R \to R \to 0$ (free resolution of R as a (R,R)-bimodule)

$(\otimes = \otimes_k)$

$x\otimes y \mapsto xy - yx$

$x\otimes y\otimes z \mapsto xy\otimes z - x\otimes yz + zx\otimes y$

$\mathrm{Hom}(-,R)$

$\rightsquigarrow$ Hochschild cohomology $HH^\bullet(R/k) = H^\bullet(\mathrm{Hom}_k(R^{\otimes n}, R))$

$HH^1(R) = (\text{derivation})/(\text{inner derivation})$

$HH^1(M_n(k)) \underset{\uparrow}{=} HH^1(k) = 0$

- Morita equivalence $M_n(k) \underset{M_{1,n}(k)}{\overset{M_{n,1}(k)}{\rightleftarrows}} k$ $\quad$ $M_{n,1}(k) \rightsquigarrow$ $n\times 1$-matrices: left $M_n(k)$, right k-mod
- $HH^\bullet$ only depends on the category of bimodules

$\left\{ \begin{array}{ll} M_{1,n}(k) \otimes_{M_n(k)} M_{n,1}(k) \xrightarrow[\cong]{} k & A\otimes B \mapsto AB \\ M_{n,1}(k) \otimes_k M_{1,n}(k) \xrightarrow[\cong]{} M_n(k) & B\otimes A \mapsto BA \end{array} \right.$

F2006

1. Let $SL_n(k)$ be the special linear group over a field k, i.e, $n\times n$ matrices with determinant 1. Let I be the identity matrix, and E_{ij} be the elementary matrix that has 1 at (i,j)-entry and 0 elsewhere. Here $1 \le i \neq j \le n$.

(1). Let C_{ij} be the centralizer of the matrix $I + E_{ij}$. Find explicit generators of C_{ij}.

(2). Find the intersection

$$\bigcap_{1\le i\neq j\le n} C_{ij}.$$

(3). Determine all the elements in the conjugacy class of $I + E_{ij}$.

just do by hand.

S2018
S2019
$(i^2=\alpha)$

1. Let F be a field of characteristic not equal to 2. Let D be the non-commutative algebra over F generated by elements i, j that satisfy the relations

$$i^2 = j^2 = 1, \quad ij = -ji.$$

Define $k = ij$.

(a) Verify that D is isomorphic to the algebra $M_2(F)$ of 2×2 matrices in such a way that

$$1 \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, i \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, j \leftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, k \leftrightarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

(b) Write $q = x + yi + zj + uk$ for $x, y, z, u \in F$. Verify that the norm

$$N(q) = x^2 - y^2 - z^2 + u^2$$

corresponds to the determinant under the isomorphism of part (a).

(c) What does the involution $q \mapsto \overline{q} = x - yi - zj - uk$ on D correspond to on the matrix side?

S2006

3. Let V be a n-dimensional vector space over a field k, with a basis $\{e_1, \ldots, e_n\}$. Let A be the ring of all $n \times n$ diagonal matrices over k. V is a A-module under the action:

$$\operatorname{diag}(\lambda_1, \ldots, \lambda_n) \cdot (a_1 e_1 + \cdots + a_n e_n) = (\lambda_1 a_1 e_1 + \cdots + \lambda_n a_n e_n).$$

Find all A-submodules of V.

$A \cong \underbrace{k \times \cdots \times k}_{n}$, $V \cong A$ as an A-module

ideals of A are $\prod_{i=1}^{n} I_i \subset k^n$, $I_i = 0$ or k

$\rightsquigarrow$ Submod of V are $\langle e_i \mid i \in I \rangle$ for some $I \subset \{1, \ldots, n\}$

S2006

1. Let $\mathbb{F}_p$ be the field with p elements, here p is prime. Let $SL_2(\mathbb{F}_p)$ be the group of 2x2 matrices over $\mathbb{F}_p$ with determinant 1.

(1). Find the order of $SL_2(\mathbb{F}_p)$. Deduce that

$$H = \{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{F}_p\}$$

is a Sylow-subgroup of $SL_2(\mathbb{F}_p)$.

(2). Determine the normalizer of H in $SL_2(\mathbb{F}_p)$ and find its order.

$GL_2(\mathbb{F}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \begin{matrix} a,b,c,d \in \mathbb{F}_p \\ ad-bc \neq 0 \end{matrix} \right\}$ choice of $\begin{pmatrix} a \\ b \end{pmatrix}$: $(p^2 - 1)$ [$\leftarrow 0$] choice of $\begin{pmatrix} c \\ d \end{pmatrix}$: $(p^2 - p)$ [$\leftarrow \mathbb{F}_p \begin{pmatrix} a \\ b \end{pmatrix}$]

$\# GL_2(\mathbb{F}_p) = (p^2-1)(p^2-p)$

$\# SL_2(\mathbb{F}_p) = \#(\ker GL_2 \xrightarrow[\det]{} \mathbb{F}_p^\times)$

$= \frac{1}{p-1}(p^4 - p^3 - p^2 + p) = p^3 - p$

directly: $ad - bc = 1 \iff \cdot\, a \in \mathbb{F}_p^\times \rightsquigarrow p^2 \cdot (p-1)$; $\cdot\, a = 0 \rightsquigarrow bc = -1 \rightsquigarrow p(p-1)$; $\rightsquigarrow p^3 - p$

Sylow p-subgp = order p

$\begin{pmatrix} s & t \\ u & v \end{pmatrix} \underset{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}}{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}} \begin{pmatrix} v & -t \\ -u & s \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -asr & as^2 \\ -au^2 & asu \end{pmatrix} \in H$ for all $a \in \mathbb{F}_p$

$\iff u = 0$, i.e. of the form $\begin{pmatrix} s & t \\ 0 & s^{-1} \end{pmatrix}$

order $= p(p-1)$

($\rightsquigarrow$ there are $p+1$ Sylow p-subgp)

S2004

1. Let $\mathbb{F}_2$ be the finite field with 2 elements.

(a) What is the order of $GL_3(\mathbb{F}_2)$, the group of 3×3 invertible matrices over $\mathbb{F}_2$?

(b) Assuming the fact that $GL_3(\mathbb{F}_2)$ is a simple group, find the number of elements of order 7 in $GL_3(\mathbb{F}_2)$.

$(p^3-1)(p^3-p)(p^3-p^2)$

$= 7 \cdot 6 \cdot 4 = 168$

$n_7 = \# Syl_7(\underbrace{GL_3(\mathbb{F}_7)}_{\text{simple} \Rightarrow n_7 \neq 1}) \rightsquigarrow n_7 \mid 24,\ n_7 \equiv 1 \pmod 7$

$\rightsquigarrow n_7 = 8 \rightsquigarrow \#(\text{order 7 elements}) = 8 \cdot (7-1) = 48$

S2002

4. For a field K, let $SL_2(K)$ be the special linear group over K, i.e. the group of $2 \times 2-$ matrices over K with determinant 1, and let $PSL_2(K)$ be the quotient of $SL_2(K)$ by its center, i.e. the projective special linear group. Find the order of $PSL_2(\mathbf{F_7})$ where $\mathbf{F_7}$ denotes the finite field of 7 elements.

center $= \{\pm 1\}$ scalar matrices (check $\begin{pmatrix} s & t \\ u & v \end{pmatrix} \underset{\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}}{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}} \begin{pmatrix} v & -t \\ -u & s \end{pmatrix} = \underset{\begin{pmatrix} 1 & 0 \\ a & 0 \end{pmatrix}}{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}}$

(intuitively: lin. trans. whose matrix representation is indep of the basis.

$\rightsquigarrow$ any vector must be an eigenvector

$\# PSL_2(\mathbb{F}_7) = \# SL_2(\mathbb{F}_7)/2 = (7^3 - 7)/2 = 168$

S2007 4. Find the invertible elements, the zero divisors and the nilpotent elements in the following rings:

(a) $\mathbf{Z}/p^n\mathbf{Z}$, where n is a natural number, p is a prime one.

(b) the upper triangular matrices over a field.

(a) $\bar{a} \in \mathbb{Z}/p^n\mathbb{Z}$ represented by $a \in \mathbb{Z}$ is
- invertible if $\gcd(a, p) = 1$ (by Euclidean algorithm)
- nilpotent (in particular a zero divisor) if $p \mid a$, in fact, $\bar{a}^n = 0$.

(b) $\underset{(a_{ij})_{1 \le i \le j \le n}}{A} = D + N$ D: diagonal, N: strictly uppertriangular

A: nilpotent $\iff D = 0$

$(\Leftarrow)$: $N^n = 0$

$(\Rightarrow)$ If $a_{ii} \neq 0$, then (i,i)-th component of A^k is $a_{ii}^k \neq 0$.

A: invertible $\iff \det A = a_{11} \cdots a_{nn} \neq 0$

$(\Rightarrow)$ obvious

$(\Leftarrow)$ $A^{-1} \in GL_n(k)$ is upper triangular because A restricts to an automorphism of the subspaces $V_k = \langle e_1, e_2, \ldots, e_k \rangle$ $(1 \le k \le n)$, so does A^{-1}.

A: zero divisor $\iff a_{11} \cdots a_{nn} = 0$

$(\Rightarrow)$ otherwise it is invertible

$(\Leftarrow)$ A has a nontrivial kernel, take $x \in \operatorname{Ker} A \setminus \{0\}$.

Then $A \cdot \begin{pmatrix} 0 & \boxed{x} \end{pmatrix} = 0$.

(How about two-sided zero divisors?)

Homological properties of rings & modules

A : ring, M, N : A-modules $\rightsquigarrow$ $M \otimes_A N$, $\mathrm{Hom}_A(M,N)$: A-mod if A commutative.

<u>Universal properties</u> (i) represents A-bilinear maps $\quad \mathrm{Hom}_A(M\otimes_A N, L) \cong \mathrm{Hom}_A(M, \mathrm{Hom}_A(N,L))$

($\Leftrightarrow$ left adjoint to Hom_A)

(ii) M : A-mod, B : A-alg $\rightsquigarrow$ <u>extension of scalars</u> $\forall N$: B-mod, $\mathrm{Hom}_B(M\otimes_A B, N) \cong \mathrm{Hom}_A(M,N)$

(iii) B, C : A-alg $\rightsquigarrow$ coproduct of A-algebras (or pushout of rings) :

$$\begin{tikzcd} A \arrow[r] \arrow[d] & B \arrow[d] \arrow[ddr, bend left] & \\ C \arrow[r] \arrow[drr, bend right] & B\otimes_A C \arrow[dr, dashed, "\exists !"] & \\ & & D \end{tikzcd}$$

in the category of comm. rings.

$\left(\Leftrightarrow \mathrm{Hom}_{Alg_A}(B,D) \times \mathrm{Hom}_{Alg_A}(C,D) \cong \mathrm{Hom}_{Alg_A}(B\otimes_A C, D) \right)$

(i) formally implies the following: ① $M\otimes -$ preserves all colimits (direct sums & cokernels) $\to$ right exactness $\quad N_1 \to N_2 \to N_3 \to 0$ ($M\otimes$ applied to each term)

② $\mathrm{Hom}(N,-)$ preserves all limits (direct products & kernels)

③ $\mathrm{Hom}(-,L)$ turns colimits into limits

any $0 \to M_1 \to M_2 \to N \to 0$ splits $\Updownarrow$ any $0 \to L \to M_1 \to M_2 \to 0$ splits

<u>Def</u> ①' M is <u>flat</u> if $M\otimes -$: exact ($\Leftrightarrow$ preserves kernels, or injections)

②' N is <u>projective</u> if $\mathrm{Hom}(N,-)$: exact ($\Leftrightarrow$ preserves cokernel, or surjections)

③' L is <u>injective</u> if $\mathrm{Hom}(-,L)$: exact ($\Leftrightarrow$ turns ker into cok, or injections to surjections)

$$\begin{tikzcd} & L' \arrow[d] \\ N \arrow[ur, dashed, "\exists"] \arrow[r] & L \end{tikzcd} \qquad \begin{tikzcd} N \arrow[r] & L : \mathrm{inj} \\ N' \arrow[u, hook] \arrow[ur, dashed, "\exists"'] & \end{tikzcd}$$

proj

<u>Properties</u> · free $\Rightarrow$ proj $\Leftrightarrow$ direct summand of free

(proj $\Rightarrow$ free: fin. gen / PID) $\quad$ direct summand of free $\Downarrow$ flat

torsion-free $\Leftarrow$ flat ($\Leftrightarrow$ directed colim of free (Lazard's thm)); (torsion-free $\Rightarrow$ flat: f.g. / Dedekind dom)

flatness, injectivity of A-mod: enough to check

$$\begin{tikzcd} I\otimes M \arrow[d] \\ A\otimes M \end{tikzcd} \qquad , \qquad \begin{tikzcd} I \arrow[r] \arrow[d, hook] & M \\ A \arrow[ur, dashed, "\exists"'] & \end{tikzcd}$$

for $I \subset A$ f.g. ideal

· $S \subset A$ multiplicative subset $\rightsquigarrow S^{-1}M \cong S^{-1}A \otimes M$, $S^{-1}(-)$: exact ($\Leftrightarrow S^{-1}A$: flat A-mod)

· injective $\Rightarrow$ divisible $\left(\forall x \in M \ \forall a : \text{non zerodiv of } A, \exists y \in M \text{ s.t. } ay = x \right)$

$\Leftarrow$ (A : PID (use Zorn))

<u>five lemma</u>

$$\begin{tikzcd} M_1 \arrow[r] \arrow[d, "f_1"] & M_2 \arrow[r] \arrow[d, "f_2"] & M_3 \arrow[r] \arrow[d, "f_3"] & M_4 \arrow[r] \arrow[d, "f_4"] & M_5 \arrow[d, "f_5"] \\ N_1 \arrow[r] & N_2 \arrow[r] & N_3 \arrow[r] & N_4 \arrow[r] & N_5 \end{tikzcd} \quad : \mathrm{ex}$$

f_1 surj, f_2 inj, f_4 inj $\Rightarrow f_3$: inj

f_2 surj, f_4 surj, f_5 inj $\Rightarrow f_3$ surj

<u>snake lemma</u>

$$\begin{tikzcd} & \mathrm{Ker} \arrow[r] \arrow[d] & \mathrm{Ker} \arrow[r] \arrow[d] & \mathrm{Ker} \arrow[d] \arrow[ddll, bend left] & \\ & M_1 \arrow[r] \arrow[d] & M_2 \arrow[r] \arrow[d] & M_3 \arrow[r] \arrow[d] & 0 \quad : \mathrm{ex} \\ 0 \arrow[r] & N_1 \arrow[r] \arrow[d] & N_2 \arrow[r] \arrow[d] & N_3 \arrow[d] & \quad : \mathrm{ex} \\ & \mathrm{Cok} \arrow[r] & \mathrm{Cok} \arrow[r] & \mathrm{Cok} & : \mathrm{exact} \end{tikzcd}$$

$0 \to M_1 \to M_2 \to M_3 \to 0$: exact $\Rightarrow \exists$ the following long exact seq

<u>$\mathrm{Tor}^A_\bullet(-,-)$</u> $\qquad M_1\otimes N \to M_2 \otimes N \to M_3 \otimes N \to 0$

$\mathrm{Tor}_0 = \otimes \qquad \mathrm{Tor}_1(M_3,N) \to \mathrm{Tor}_1(M_2,N) \to \mathrm{Tor}_1(M_3,N)$

$\cdots \to \mathrm{Tor}_2(M_3,N)$

· $\mathrm{Tor}_i(M,-) = 0 \ \forall i > 0 \Leftrightarrow M$: flat

· $\mathrm{Ext}^i(N,-) = 0 \ \forall i > 0 \Leftrightarrow N$: projective

· $\mathrm{Ext}^i(-,L) = 0 \ \forall i > 0 \Leftrightarrow N$: injective

actually can be replaced by $i = 1$

<u>$\mathrm{Ext}^\bullet_A(-,-)$</u> $\qquad 0 \to \mathrm{Hom}(N,M_1) \to \mathrm{Hom}(N,M_2) \to \mathrm{Hom}(N,M_3)$

$\mathrm{Ext}^0 = \mathrm{Hom} \qquad \mathrm{Ext}^1(N,M_1) \to \mathrm{Ext}^1(N,M_2) \to \mathrm{Ext}^1(N,M_3)$

$\mathrm{Ext}^2(N,M_1) \to \cdots$

$\mathrm{Hom}(M_1,N) \leftarrow \mathrm{Hom}(M_2,N) \leftarrow \mathrm{Hom}(M_3,N) \leftarrow 0$

$\mathrm{Ext}^1(M_1,N) \leftarrow \mathrm{Ext}^1(M_2,N) \leftarrow \mathrm{Ext}^1(M_3,N)$

$\cdots \leftarrow \mathrm{Ext}^2(M_3,N)$

S2012 2. (a) Prove that if M is an abelian group and n is a positive integer, the tensor product $M \otimes_{\mathbb{Z}} Z/n\mathbb{Z}$ can be naturally identified with M/nM.

(b) Compute the tensor product over $\mathbb{Z}$ of $\mathbb{Z}/n\mathbb{Z}$ with each of $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$. Also compute the tensor products $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$, $\mathbb{Q} \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z})$, and $(\mathbb{Q}/\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z})$.

(c) Let $\mathbb{Z}^{\mathbb{N}}$ denote the (abelian) group of sequences $(a_i)_{i\in\mathbb{N}}$ in $\mathbb{Z}$ under termwise addition, and $\mathbb{Z}^{(\mathbb{N})}$ the subgroup of sequences for which $a_i = 0$ for all but finitely many i. Define $\mathbb{Q}^{\mathbb{N}}$ and $\mathbb{Q}^{(\mathbb{N})}$ analogously. Compare $\mathbb{Z}^{(\mathbb{N})} \otimes_{\mathbb{Z}} \mathbb{Q}$ to $\mathbb{Q}^{(\mathbb{N})}$, and $\mathbb{Z}^{\mathbb{N}} \otimes_{\mathbb{Z}} \mathbb{Q}$ to $\mathbb{Q}^{\mathbb{N}}$.

(a) $\mathbb{Z} \xrightarrow{n} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$ $\quad \big\downarrow \otimes M$

$M \xrightarrow{n} M \longrightarrow \underset{\substack{\shortparallel \\ M/nM}}{M \otimes \mathbb{Z}/n\mathbb{Z}} \longrightarrow 0$

(b) $\mathbb{Z}/m\mathbb{Z} \xrightarrow[n]{} \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/d\mathbb{Z} \qquad \mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z}$

$\mathrm{Im} = n\mathbb{Z}/m\mathbb{Z} = d\mathbb{Z}/m\mathbb{Z} \quad d = \gcd(n,m)$

$\mathbb{Q} \xrightarrow[n]{\cong} \mathbb{Q} \longrightarrow 0 \qquad \mathbb{Q} \otimes \mathbb{Z}/n\mathbb{Z} = 0$

$\mathbb{Q}/\mathbb{Z} \xrightarrow[n]{} \mathbb{Q}/\mathbb{Z} \longrightarrow 0 \qquad \mathbb{Q}/\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} = 0$

$\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q}$ because the action of $\mathbb{Z}\setminus\{0\}$ on $\mathbb{Q}$ is invertible.

$\mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0 \quad \big\downarrow \otimes \mathbb{Q} \quad \rightsquigarrow \mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} = 0$

$\mathbb{Q} \xrightarrow{\cong} \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \otimes \mathbb{Q} \to 0$

$\otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}$

$\mathbb{Q}/\mathbb{Z} \to 0 \to \mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} \to 0 \quad \rightarrow \mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0$

(c) • $\mathbb{Z}^{(\mathbb{N})} = \bigoplus_{n\in\mathbb{N}} \mathbb{Z}$, $\mathbb{Q}^{(\mathbb{N})} = \bigoplus_{n\in\mathbb{N}} \mathbb{Z}$

$\rightsquigarrow \mathbb{Z}^{(\mathbb{N})} \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q}^{(\mathbb{N})}$

since $\otimes$ commutes with arbitrary coproduct.

(the map is given by $(a_i) \otimes r \longmapsto (ra_i)$)

• $\exists f : \mathbb{Z}^{\mathbb{N}} \otimes_{\mathbb{Z}} \mathbb{Q} \longrightarrow \mathbb{Q}^{\mathbb{N}} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}^{\mathbb{N}}$

$(a_i) \otimes r \longmapsto (ra_i)$

which is injective ($\mathbb{Q}$: flat)

but not surjective :

$(1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \cdots) \notin \mathrm{Im} f.$

Universal property of localization : $M \xrightarrow{\forall f} \forall N$ (S acts on N invertibly), $M \to S^{-1}M \dashrightarrow N$, $\exists!$, $m/s \mapsto f(m)/s$.

$\rightsquigarrow M \to S^{-1}M$ isom if S already acts on M by isomorphisms.

or directly : $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \xrightarrow{m} \mathbb{Q}$, so enough to check $(1\otimes id) \otimes m = id$.

$\begin{array}{ccc} \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} & \xrightarrow{m} & \mathbb{Q} \\ \uparrow {\scriptstyle 1\otimes id} & \nearrow_{=} & \\ \mathbb{Q} & & \end{array}$

explicitly : $\frac{a}{b} \otimes \frac{c}{d} \underset{m}{\longmapsto} \frac{ac}{bd} \underset{1\otimes id}{\longmapsto} 1 \otimes \frac{ac}{bd}$

and $1 \otimes \frac{ac}{bd} = a \otimes \frac{c}{bd} = (b \cdot \frac{a}{b}) \otimes \frac{c}{bd}$
$= \frac{a}{b} \otimes \frac{c}{d}$.

F2006 **4.** Let R be a commutative ring. Let M be an R-module.
(1). Write down the definition of $\mathcal{T}(M)$, the tensor algebra of M.
(2). Assume $R = \mathbb{Z}$ and $M = \mathbb{Q}/\mathbb{Z}$. Compute $\mathcal{T}(M)$.
(3). If M is a vector space over a field R, show that $\mathcal{T}(M)$ contains no zero divisors.

(1) $T(M) = \bigoplus_{n=0}^{\infty} T_n(M)$, $T_n(M) = \underbrace{M \otimes_R \cdots \otimes_R M}_{n}$

$\otimes : T_i(M) \otimes_R T_j(M) \xrightarrow{\cong} T_{i+j}(M)$

ring structure: $T(M) \otimes T(M) \simeq \bigoplus_{i,j} T_i(M) \otimes T_j(M) \longrightarrow \bigoplus_n T_n(M) = T(M)$

(2) $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0$, so $T_n(M) = 0 \quad \forall n \geq 2$.

So $T(M) = \mathbb{Z} \oplus \mathbb{Q}/\mathbb{Z}$.

(3) Take $a = \sum_{i=0}^{m} a_i$, $b = \sum_{i=0}^{n} b_i \in T(M)$, where $a_i, b_i \in T_i(M)$, $a_m, b_n \neq 0$.

Since $ab = \sum_{k=0}^{m+n} \underbrace{\sum_{i+j=k} a_i \otimes b_j}_{\in T_k(M)}$. it suffices to prove $T_m(M) \times T_n(M) \xrightarrow[f]{} T_m(M) \otimes_R T_n(M) \simeq T_{m+n}(M)$ is injective

This follows by eg. choosing a basis $\{v_\alpha\}$ of M

and observing f sends $(v_{\alpha_1} \otimes \cdots \otimes v_{\alpha_m}, v_{\beta_1} \otimes \cdots \otimes v_{\beta_n}) \mapsto v_{\alpha_1} \otimes \cdots \otimes v_{\beta_n}$

the basis of $T_m(M) \times T_n(M)$ to a part of the basis $v_{\alpha_1} \otimes \cdots \otimes v_{\alpha_{m+n}}$

S2009 **5.** Consider the $\mathbb{Z}$-modules $M_i = \mathbb{Z}/2^i\mathbb{Z}$ for all positive integers i. Let $M = \prod_{i=1}^{\infty} M_i$. Let $S = \mathbb{Z} - \{0\}$.

(a). Show that

$$\mathbb{Q} \otimes_{\mathbb{Z}} M \cong S^{-1}M.$$

Here $S^{-1}M$ is the localization of M.

(b). Show that

$$\mathbb{Q} \otimes_{\mathbb{Z}} \prod_{i=1}^{\infty} M_i \neq \prod_{i=1}^{\infty} (\mathbb{Q} \otimes_{\mathbb{Z}} M_i).$$

(a) True for any M. (e.g. by the universality + $\mathbb{Q}$-mod $\Leftrightarrow$ $S \subset A$ acts invertibly on M)

(b) $\mathbb{Q} \otimes_{\mathbb{Z}} M_i = 0 \quad \forall i$, so RHS $= 0$.

We have a map $\mathbb{Z} \xrightarrow{i} M$ induced by the quotient maps $\mathbb{Z} \to \mathbb{Z}/2^i\mathbb{Z} = M_i$.

Since i is injective and $\mathbb{Q}$ is flat, $\mathbb{Q} \simeq \mathbb{Q} \otimes \mathbb{Z} \longrightarrow \mathbb{Q} \otimes M$ is injective. So LHS $\neq 0$.

S2013 1. Prove that, as a $\mathbb{Z}$-module, $\mathbb{Q}$ is flat but not projective.

$\mathbb{Q}$ is flat because $- \otimes \mathbb{Q}$ is a localization and therefore exact.

It is not projective, because it can't be a submodule of a free $\mathbb{Z}$-module;
$\forall x = (x_i)_{i \in I} \in \mathbb{Z}^{\oplus I} \setminus \{0\}$, if $x_{i_0} \neq 0$, then there is no element $y \in \mathbb{Z}^{\oplus I}$ s.t. $(|x_{i_0}|+1)y = x$, whereas $\mathbb{Q}$ is divisible.

F2008 **5.** For each $n \in \mathbb{Z}$, define the ring homomorphism

$$\phi_n : \mathbb{Z}[x] \to \mathbb{Z} \text{ by } \phi_n(f) = f(n).$$

This gives a $\mathbb{Z}[x]$-module structure on $\mathbb{Z}$, i.e,

$$f \circ a = f(n) \cdot a \text{ for all } f \in \mathbb{Z}[x] \text{ and } a \in \mathbb{Z}.$$

Now given two integers $m, n \in \mathbb{Z}$, compute the tensor product $\mathbb{Z} \otimes_{\mathbb{Z}[x]} \mathbb{Z}$ where the left-hand copy of $\mathbb{Z}$ uses the module structure from ϕ_n and the right-hand copy of $\mathbb{Z}$ uses the module structure from ϕ_m. (Note: The answer depends on the numbers n and m.)

$$\begin{tikzcd} x \in \mathbb{Z}[x] \arrow[r, "ev_n"] \arrow[d, "ev_m"] & \mathbb{Z} \ni n \arrow[d] \\ m \in \mathbb{Z} \arrow[r] & A \ni n = m \end{tikzcd}$$

Commutes iff $n = m$ in A, i.e. A is a $\mathbb{Z}/(n-m)\mathbb{Z}$-algebra.

Therefore $\mathbb{Z}/(n-m)\mathbb{Z}$ is universal among such A, so by the universality $\mathbb{Z} \otimes_{\mathbb{Z}[x]} \mathbb{Z} \simeq \mathbb{Z}/(n-m)\mathbb{Z}$.

F2014 2. Let $R = \mathbb{Q}[X]$, I and J the principal ideals generated by $X^2 - 1$ and $X^3 - 1$ respectively. Let $M = R/I$ and $N = R/J$. Express in simplest terms [the isomorphism type of] the R-modules $M \otimes_R N$ and $\mathrm{Hom}_R(M, N)$. **Explain.**

We have a exact sequence $R \xrightarrow{\cdot(X^2-1)} R \twoheadrightarrow M \to 0$

Since $\otimes_R N$ and $\mathrm{Hom}_R(-, N)$ preserves this exactness, we have

$$N \xrightarrow{\varphi} N \to M \otimes_R N \to 0$$

$$0 \to \mathrm{Hom}_R(M,N) \to \underset{\underset{N}{\wr\wr}}{\mathrm{Hom}_R(R,N)} \to \underset{\underset{N}{\wr\wr}}{\mathrm{Hom}_R(R,N)}, \qquad N \xrightarrow{\varphi} N$$

where φ is the multiplication by (x^2-1).

By CRT $N \xrightarrow{\simeq} \mathbb{Q}[x]/(x-1) \oplus \mathbb{Q}[x]/(x^2+x+1)$ as $\mathbb{Q}[x]$-mod

$$\begin{tikzcd} N \arrow[r, "\simeq"] \arrow[d, "\varphi"] & \mathbb{Q}[x]/(x-1) \oplus \mathbb{Q}[x]/(x^2+x+1) \arrow[d, "\boxed{0 \oplus \text{isom}}"] \\ N \arrow[r, "\simeq"] & \mathbb{Q}[x]/(x-1) \oplus \mathbb{Q}[x]/(x^2+x+1) \end{tikzcd}$$

$x^2 - 1 \in (x-1)$, x^2-1 and x^2+x+1 coprime.

So $\mathrm{Hom}_R(M,N) \simeq \mathrm{Ker}\,\varphi \simeq \mathrm{Ker}\left(\mathbb{Q}[x]/(x-1) \xrightarrow{0} \mathbb{Q}[x]/(x-1)\right) \simeq \mathbb{Q}[x]/(x-1)$

$M \otimes_R N \simeq \mathrm{Cok}\,\varphi \simeq \mathrm{Cok}(\text{——} \,\text{"}\, \text{——}) \simeq \mathbb{Q}[x]/(x-1)$

F2004

5. Consider the ideal $I = (2, x)$ in $R = \mathbb{Z}[x]$.
(a) Construct a non-trivial R-module homomorphism $I \otimes_R I \to R/I$, and use that to show that $2 \otimes x - x \otimes 2$ is a non-zero element in $I \otimes_R I$.
(b) Determine the annihilator of $2 \otimes x - x \otimes 2$.

$(m, X) \to \mathbb{Z}[X] \to \mathbb{Z}/m$. (m,X) maximal $\Leftrightarrow \mathbb{Z}/m$ field $\Leftrightarrow m$: prime

S2002 **2.** Let m be an integer ≥ 2 and $\mathbf{Z}[X]$ be the polynomial ring over $\mathbf{Z}$. Find a condition on m so that the ideal (m, X) in the ring is maximal.

(a) Since I is the kernel of $\mathbb{Z}[x] \to \mathbb{F}_2$, $x \mapsto 0$, I is ~~maximal~~ maximal and $R/I \cong \mathbb{F}_2$

So we need to construct a nontrivial (and nonsymmetric) R-bilinear map $I \times I \xrightarrow{\varphi} \mathbb{F}_2$.

Define $\varphi\big((\underset{\in 2\mathbb{Z}}{a_0} + a_1x + \cdots + a_nx^n), (\underset{\in 2\mathbb{Z}}{b_0} + b_1x + \cdots + b_mx^m)\big) = \frac{a_0}{2} \cdot b_1 \mod 2$

It is obviously $\mathbb{Z}$-bilinear, and since $\varphi(xf(x), g(x)) = \varphi(f(x), xg(x)) = 0$ $\forall f(x), g(x) \in I$, so it's $\mathbb{Z}[x]$-bilinear

$\big(= x \cdot \varphi(f(x), g(x))$, x acts on $\mathbb{F}_2$ by $0\big)$

Now extending this to $I \otimes I \xrightarrow{\bar{\varphi}} \mathbb{F}_2$, we see that

$\bar{\varphi}(2 \otimes x - x \otimes 2) = 1 - 0 = 1$. So $2 \otimes x - x \otimes 2 \neq 0$ in $I \otimes_R I$.

(b) Since
$$2(2 \otimes x) = 2 \otimes (2x) = x(2 \otimes 2) = 2x \otimes 2 = 2(x \otimes 2)$$
$$x(2 \otimes x) = (2x) \otimes x = 2(x \otimes x) = x \otimes 2x = x(x \otimes 2)$$
in $I \otimes_R I$

we see that $I = (2, x) \subset \mathrm{Ann}_R(2 \otimes x - x \otimes 2) \underset{\text{by (a)}}{\subsetneq} R$

Since I is a maximal ideal,
$\mathrm{Ann}_R(2 \otimes x - x \otimes 2) = I$.

S2018

5. Let n be a positive integer and A an abelian group. Prove that
$$\mathrm{Ext}^1(\mathbf{Z}/n\mathbf{Z}, A) \cong A/nA.$$

$0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0 \quad \xrightarrow{\mathrm{Ext}^i(-, A)}$

$$\underset{\cong A}{\mathrm{Hom}(\mathbb{Z}, A)} \xleftarrow{n} \underset{\cong A}{\mathrm{Hom}(\mathbb{Z}, A)} \leftarrow \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, A)$$
$$\cdots \leftarrow \underset{= 0 \text{ free}}{\mathrm{Ext}^1(\mathbb{Z}, A)} \leftarrow \underset{\cong A/nA}{\mathrm{Ext}^1(\mathbb{Z}/n\mathbb{Z}, A)}$$

F2002

(3) (3 points) Working over the integers, calculate (and show your work in a readable fashion) $\mathrm{Tor}(\mathbb{Z}/(p), \mathbb{Z}/(p))$.

$0 \to \mathbb{Z} \xrightarrow{p} \mathbb{Z} \to \mathbb{Z}/p \to 0 \quad \xrightarrow{\otimes \mathbb{Z}/p} \quad \underset{\cong \mathbb{Z}/p}{\mathrm{Tor}(\mathbb{Z}/p, \mathbb{Z}/p)} \to \mathbb{Z}/p \xrightarrow{p = 0} \mathbb{Z}/p \to \underset{\cong \mathbb{Z}/p}{\mathbb{Z}/p \otimes \mathbb{Z}/p} \to 0$

(4) (3 points) Working over the integers, calculate (and show your work in a readable fashion) $\mathrm{Ext}(\mathbb{Z}/(p), \mathbb{Z}/(p))$.

$0 \to \mathrm{Hom}(\mathbb{Z}/p, \mathbb{Z}/p) \to \underset{\mathbb{Z}/p}{\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/p)} \xrightarrow{p = 0} \underset{\mathbb{Z}/p}{\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/p)}$

$\mathbb{Z}/p \cong \mathrm{Ext}(\mathbb{Z}/p, \mathbb{Z}/p) \to \mathrm{Ext}(\cancel{\mathbb{Z}, \mathbb{Z}/p}) = 0$

S2018 **2.** Let R be a commutative ring. An R-module M is said to be *finitely presented* if there exists a right-exact sequence
$$R^m \longrightarrow R^n \longrightarrow M \longrightarrow 0$$
for some non-negative integers m, n. Prove that any finitely generated projective R-module P is finitely presented.

P: fin.gen. $\Leftrightarrow \exists n\ \exists f : R^n \twoheadrightarrow P$.

Then $R^n \cong P \oplus \ker f$ because P: projective, so

$$R^n \longrightarrow R^n \xrightarrow{f} P \to 0 \quad \text{is exact} \quad \square$$

$R^n \xrightarrow{pr_2} \ker f \hookrightarrow R^n$

F2013

3. Let R be a commutative ring with unity. Given an R-module A and an ideal $I \subset R$, there is a natural R-module homomorphism $A \otimes_R I \to A \otimes_R R \simeq A$ induced by the inclusion $I \subset R$. In the following three steps you shall prove the flatness criterion: *A is flat if and only if for every finitely generated ideal $I \subset R$ the natural map $A \otimes_R I \to A \otimes_R R$ is injective.*

$I = \bigcup_{I_\lambda : \text{f.g.}} I_\lambda$: direct limit

$\Rightarrow A \otimes I = \bigcup A \otimes I_\lambda \to A \otimes R$

if $a \in A \otimes I$, $a \mapsto 0$, $\exists \lambda$: $a \in A \otimes I_\lambda$

$\rightsquigarrow$ by $A \otimes I_\lambda \to A \otimes R$ inj., $a \mapsto 0$, $a = 0$, so $A \otimes I \to A \otimes R$ inj.

(a) Prove that if A is flat and $I \subset R$ is a finitely generated ideal then $A \otimes_R I \to A \otimes_R R$ is injective. $A \otimes -$ preserve injections

(b) If $A \otimes_R I \to A \otimes_R R$ is injective for every finitely generated ideal I, prove that $A \otimes_R I \to A \otimes_R R$ is injective for every ideal I. Show that if K is any submodule of a free module F then the natural map $A \otimes_R K \to A \otimes_R F \simeq A$ induced by the inclusion $K \subset F$ is injective (*Hint*: the general case reduces to the case when F has finite rank).

(c) Let $\psi\colon L \to M$ be an injective homomorphism of R-modules. Prove that the induced map $1 \otimes \psi\colon A \otimes_R L \to A \otimes_R M$ is injective (*Hint*: Write M as a quotient $f\colon F \to M$ of a free module F, giving a short exact sequence $0 \to K \to F \to M \to 0$ and consider the commutative diagram

$$\begin{tikzcd}
\cancel{0} \arrow[r] & A\otimes K \arrow[r] \arrow[d, "\mathrm{id}"] & A\otimes J \arrow[r] \arrow[d, "\text{inj}"] & A\otimes L \arrow[r] \arrow[d, "\psi"] & 0 \\
0 \arrow[r] & A\otimes K \arrow[r, "\text{inj}"] & A\otimes F \arrow[r, "f"] & A\otimes M \arrow[r] & 0,
\end{tikzcd}$$

: exact

by part (b)

check: $0 \to K \to J \to L \to 0$ exact; after $A \otimes -$ we still have right part exact

$\rightsquigarrow$ conclude by snake lemma or five lemma

where $J = f^{-1}(\psi(L))$.)

4. (a) Let R be a P.I.D. Prove that a finitely generated R-module M is flat if and only if M is torsion-free (hence, free by the structure theorem).

(b) Give an example of an integral domain R and a torsion-free R-module M such that M is not free.

(a) flat $\Rightarrow$ torsion-free is always true:

$a \in R$ non-zero div $\Leftrightarrow R \xrightarrow{a} R$ is injective. If M is flat,

$M \otimes_R R \xrightarrow{a} M \otimes_R R$ is injective, i.e. M is torsion-free

$M \otimes_R R \cong M$, $M \otimes_R R \cong M$

By the structure thm tor-free $\xRightarrow{\text{f.g./PID}}$ free $\Rightarrow$ flat. $\blacksquare$

(b) In general: free $\Rightarrow$ projective $\Rightarrow$ flat $\Rightarrow$ tor free

	free	projective	flat	tor free
$R = \mathbb{Z}$, $M = \mathbb{Q}$ (PID but not fin. gen.)	No	No	Yes	Yes
$R = k[x,y]$, $m = (x,y)$ (not PID or not even Dedekind; fin. gen.)	No	No	No	Yes

$m \otimes m \xrightarrow{\text{incl.} \otimes \text{id}} R \otimes m \xrightarrow{\cong} m$ is the multiplication map $m \otimes m \xrightarrow{\mu} m^2 \subset R$.

$m \otimes m \to k[x,y]/(x,y)$ is a nontrivial R-hom, so
$f \otimes g \mapsto \frac{\partial f}{\partial x} \cdot \frac{\partial g}{\partial y}$ $\quad x \otimes y - y \otimes x \neq 0$

but $\mu(x \otimes y - y \otimes x) = xy - yx = 0$, so μ: not injective and m is not a flat R-mod

F2000

6. Let R be the ring $\mathbb{Q}[X]/\left(X^7-1\right)$, where $\left(X^7-1\right)$ is the ideal generated by X^7-1 in $\mathbb{Q}[X]$. Give an example of a finitely generated projective R–module which is not R–free. (We remind you that an R-module is called projective if it is a direct summand of a free R–module.)

$\mathbb{Q}[x]/(x^7-1) \cong \mathbb{Q}[x]/(x-1) \oplus \mathbb{Q}[x]/(x^6+x^5+\cdots+1)$ as R-modules, so $\mathbb{Q}[x]/(x-1)$ is projective. But it is not free, because $\dim_{\mathbb{Q}} R^{\oplus n} = 7n$ (or ∞) whereas $\dim_{\mathbb{Q}} \mathbb{Q}[x]/(x-1) = 1$.

Basic commutative algebra

S2017 (1) Let A be a commutative ring, and define the *nilradical* $\sqrt{0}$ to be the set of nilpotent elements in A. Show that $\sqrt{0}$ is equal to the intersection of all prime ideals in A. Show that if A is reduced, then A can be embedded into a product of fields.

- $\bigcap_{p:\text{prime}} p = \sqrt{0}$ $\quad$ ($\supset$): obvious
  ($\subset$): take any $f \notin \sqrt{0}$, then $A_f \neq 0$, so $\exists\, m \subset A_f$ maximal.
  $A \xrightarrow{i} A_f$. Since $i(f)$ is invertible,
  $i(f) \notin m$, so $f \notin i^{-1}(m)$: prime ideal

- The projections $A \xrightarrow[\pi_p]{} A/p$ induce $A \xrightarrow{\varphi} \prod_{p:\text{prime}} A/p$ whose Kernel $= \bigcap p = \sqrt{0} = 0$ ($\Updownarrow$ A: reduced)
  So A admits an embedding

$$A \hookrightarrow \prod_p A/p \hookrightarrow \prod_p \mathrm{Frac}(A/p).$$

F2004 **2.** Let $\mathfrak{N}$ be the set of all nilpotent elements in a ring R. Assume first that R is commutative.
(a) Show that $\mathfrak{N}$ is an ideal in R, and $R/\mathfrak{N}$ contains no non-zero nilpotent elements.
(b) Show that $\mathfrak{N}$ is the intersection of all the prime ideals of R.
(c) Give an example with R **non**-commutative where $\mathfrak{N}$ is not an ideal in R. $\leftarrow M_2(\mathbb{R})$. $\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}0&0\\1&0\end{pmatrix}=\begin{pmatrix}1&0\\0&0\end{pmatrix}$

- $x^n = y^m = 0 \Rightarrow (x+y)^{n+m} = 0$
- $\bar{x} \in R/\mathfrak{N}$, $\bar{x}^n = 0$
  $\Leftrightarrow x^n \in \mathfrak{N} \Leftrightarrow \exists m\ x^{nm} = 0$
  $\Leftrightarrow \bar{x} = 0$

S2014
S2016 4. Proof that a finite dimensional associative algebra over a field is a division algebra if and only if it has no zero divisors.

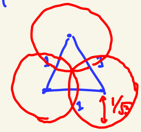
(The same proof as "finite alg/a field is a field $\Leftrightarrow$ int dom")

A/k assoc. alg, $\dim A < \infty$. Take $a \in A \setminus \{0\}$, then $\{1, a, a^2, \cdots\}$ is not linearly indep. $\rightsquigarrow \exists\, c_i \in k$, $\sum_{i=0}^{n} c_i a^i = 0$. We may assume n: minimum
Then $c_0 \neq 0$, because if $c_0 = 0$, $\left(\sum_{i=1}^{n} c_i a^{i-1}\right) \cdot a = 0$, and by assumption $\sum_{i=1}^{n} c_i a^{i-1}$, which contradicts the minimality of n.
$\rightsquigarrow c_0^{-1}\left(\sum_{i=1}^{n} c_i a^{i-1}\right)$ is the two-sided inverse of a. $\blacksquare$

S2009 **2.** Consider $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ where ω is a non-trivial cube root of 1. Show that $\mathbb{Z}[\omega]$ is an Euclidean domain.

$\mathbb{Z}[\omega] \xrightarrow{1-1} \mathbb{R}_{\geq 0}$ image is well-ordered (finitely many pts in a bounded disk)

Take $\beta \in \mathbb{Z}[\omega] \setminus 0$. Then $\exists q \in \mathbb{Z}[\omega]$, $\alpha = q\beta + r$, $|r| < |\beta|$ ($\Updownarrow$ $|r/\beta| < 1$) $\Leftrightarrow \exists\, q \in \mathbb{Z}[\omega]$, $\left|q - \frac{\alpha}{\beta}\right| < 1$
$\alpha \in \mathbb{Z}[\omega]$.
This is true because for any $z \in \mathbb{C}$, the distance to the set $\mathbb{Z}[\omega]$ is $\leq 1/\sqrt{3}$.



F2006

3. Let A be a principal integral domain and K be its field of fractions. Assume that R is a ring such that $A \subset R \subset K$. Show that R is also a principal integral domain.

R is a localization of A : set $S=\{a\in A \mid a\in R^\times\}$, then S is multiplicative, so $\exists$ ring hom $f: S^{-1}A \longrightarrow R$.

- f is injective since both are subrings of K
- f is surjective because if $r=\frac{q}{p}\in R$, $p,q\in A$ coprime (Used A: UFD. for A: PID, This is equivalent to $(p)+(q)=(1)$)

To prove $r\in \mathrm{Im} f$, it is enough to show $p\in S$, i.e. $\frac{1}{p}\in R$. This is true because from this $\exists\, a, b\in A$ $pa+qb=1$, so $\frac{1}{p}=a+b\cdot\frac{q}{p}\in R$.

Now we only need to show $S^{-1}A$ ($\cong R$) is a PID.

Note that (in general) any ideal $\mathfrak{a}\subset S^{-1}A$ is generated by $i(i^{-1}(\mathfrak{a}))$ for $A \xrightarrow{i} S^{-1}A$.

Since i is an inclusion and a generates $i^{-1}(\mathfrak{a})$ as an A-mod, $A\cap\mathfrak{a}=(a)$ $\exists a\in A$ in our case

So a generates $\mathfrak{a}$ as an $S^{-1}A$-module.

F2001

2. Let S denote the ring $\mathbb{Z}[X]/X^2\mathbb{Z}[X]$, where X is a variable.
(a) Show that S is a free $\mathbb{Z}$–module and find a $\mathbb{Z}$–basis for S. $1, X$
(b) Which elements of S are units (i.e. invertible with respect to multiplication) ?
(c) List all the ideals of S.
(d) Find all the nontrivial ring morphisms defined on S and taking values in the ring of Gaussian integers $\mathbb{Z}[i]$.

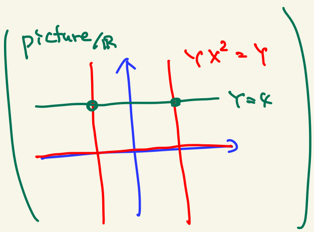
(b) ring hom preserves units ⇝ by $\mathbb{Z}[X]/(X^2)\longrightarrow \mathbb{Z}$, $X\longmapsto 0$ the image of $\left(\mathbb{Z}[X]/(X^2)\right)^\times$ is in $\mathbb{Z}^\times=\{\pm1\}$

Conversely $\pm1+aX$ is invertible;
$(\pm1+aX)(\pm1-aX)=1 \mod X^2$

(c) ideals of S $\longleftrightarrow$ ideals of $\mathbb{Z}[x]$ containing (x^2). Consider the $\mathbb{Z}$-submod $\mathbb{Z}\cap\mathfrak{a}=(n)$ and $\mathbb{Z}x\cap\mathfrak{a}=(mx)$.
Since $x\cdot(\mathbb{Z}\cap\mathfrak{a})\subset\mathbb{Z}x\cap\mathfrak{a}$, $m\mid n$. Conversely $I_{m,n}=n\mathbb{Z}+mx\mathbb{Z}+(x^2)$ is an ideal for any $m\mid n$.

(d) $S=\mathbb{Z}[X]/(X^2)\xrightarrow{f}\mathbb{Z}[i]$ $f(X)^2=f(X^2)=0$ and $\mathbb{Z}[i]$ is reduced ⇝ $f(X)=0$

So the only ring hom is $\mathbb{Z}[X]/(X^2)\twoheadrightarrow\mathbb{Z}\hookrightarrow\mathbb{Z}[i]$.



S2001

6. Let R be the ring $\mathbb{Z}[X,Y]/\left(YX^2-Y\right)$, where X and Y are two algebraically independent variables, and $\left(YX^2-Y\right)$ is the ideal generated by YX^2-Y in $\mathbb{Z}[X,Y]$.
(a) Show that the ideal I generated by $Y-4$ in R is not prime.
(b) Provide the complete list of prime ideals in R containing the ideal I described in question (a).
(c) Which of the ideals found in (b) are maximal ?

(a) $R/I\cong\mathbb{Z}[X,Y]/(YX^2-Y,\,Y-4)\cong\mathbb{Z}[X,Y]/(4X^2-4,\,Y-4)\xrightarrow{\cong}\mathbb{Z}[X]/4(X-1)(X+1)$
$Y\longmapsto 4$

(b) prime ideal of $\mathbb{Z}[X]$: (0), $(f(x))$ for f irred
(p), $(p, f(x))$ ← maximal

Nakayama's lemma

M: fin. gen A-mod $\mathfrak{a}$: ideal s.t. $\mathfrak{a} \overset{\forall}{\subset} \mathfrak{m}$ maximal

① $\mathfrak{a}M = M \; (\Leftrightarrow M \otimes A/\mathfrak{a} = 0) \Rightarrow M = 0$

② $N \subset M, \; M = \mathfrak{a}M + N \Rightarrow M = N$ (apply ① for $\mathfrak{a}(M/N) = (\mathfrak{a}M + N)/N \subset M/N$)

When $(A, \mathfrak{m})$ local, $k := A/\mathfrak{m} \rightsquigarrow M/\mathfrak{m}M = M \otimes_A k$: k-vect sp, fin dim'l.

③
$$\begin{array}{ccc} M & \longrightarrow & M/\mathfrak{m}M \cong k^n \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ x_i & \longmapsto & e_i \end{array} \Rightarrow x_1, \dots, x_n \text{ generates } M.$$

F2017

(3) In this problem all rings are commutative.

(a) Let R be a local ring with maximal ideal $\mathfrak{m}$, let N and M be finitely generated R-modules, and let $f\colon N \to M$ be an R-linear map. Show that f is surjective if and only if the induced map $N/\mathfrak{m}N \to M/\mathfrak{m}M$ is.

(b) Recall that a module M over a ring R is *projective* if the functor $\mathrm{Hom}_R(M, -)$ is exact. Show that if R is local and M is finitely generated projective, then M is free.

(a) $N \xrightarrow{f} M \to \underset{\text{cok}}{L} \to 0 \Rightarrow N \otimes_R k \to M \otimes_R k \to L \otimes_R k \to 0$

f: surj $\Leftrightarrow L = 0 \underset{\text{Nakayama}}{\Leftrightarrow} L \otimes_R k = 0 \Leftrightarrow f \otimes_R k : N/\mathfrak{m}N \to M/\mathfrak{m}M$: surj

(b) Take minimal number of generators $x_1, \dots, x_n$ of M.

Then
$$\begin{array}{ccc} R^n & \overset{\varphi}{\twoheadrightarrow} & M \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ e_i & \longmapsto & x_i \end{array}$$
: surj, and since M: projective

we have a split exact sequence

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r] \arrow[d] & R^n \arrow[r, "\cong"] \arrow[d] & M \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & N/\mathfrak{m}N \arrow[r] & k^n \arrow[r] & M/\mathfrak{m}M \arrow[r] & 0 \end{tikzcd}$$

$\otimes k = R/\mathfrak{m}$

split exact

by ①

$0 \cong N$, $N/\mathfrak{m}N \cong 0$

$M/\mathfrak{m}M \cong k^n$

$\dim M/\mathfrak{m}M = n$ by ③.

$\square$

F2010 **4.** Let A be a commutative Noetherian local ring with maximal ideal $\mathfrak{m}$. Assume $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ for some $n > 0$. Show that A is Artinian.

Noetherian $\Rightarrow \mathfrak{m}^n$: fin. gen.

$\mathfrak{m}^n = \mathfrak{m}^{n+1} \xrightarrow{\text{Nakayama}} \mathfrak{m}^n = 0$, so $A \cong A/\mathfrak{m}^n$. Note that A is artinian iff the length of A as an A-mod is finite.

Consider $A/\mathfrak{m}^n \supset \mathfrak{m}/\mathfrak{m}^n \supset \cdots \supset \mathfrak{m}^{n-1}/\mathfrak{m}^n \supset 0$.

$\quad\quad\quad\quad\;\; M_0 \quad\quad\;\; M_1 \quad\quad\quad\quad M_{n-1} \quad\;\; M_n$

annihilated by $\mathfrak{m} \Rightarrow k = A/\mathfrak{m}$-vect. sp

Since $\operatorname{length}_A M_0 = \sum_{i=0}^{n-1} \operatorname{length}_A M_i/M_{i+1} = \sum_{i=0}^{n-1} \operatorname{length}_A \mathfrak{m}^i/\mathfrak{m}^{i+1} = \sum_{i=0}^{n-1} \dim_k \mathfrak{m}^i/\mathfrak{m}^{i+1} < \infty$

A: noeth. $\Rightarrow \mathfrak{m}^i$: fin. gen ideal $\Rightarrow \mathfrak{m}^i/\mathfrak{m}^{i+1} = \mathfrak{m}^i \otimes_A k$: fin. dim vect sp. $\square$

F2009 **5.** Let A, B be two Noetherian local rings with maxima ideals m_A, m_B, respectively. Let $f : A \to B$ be a ring homomorphism such that $f^{-1}(m_B) = m_A$. Assume that:

1. $A/m_A \to B/m_B$ is an isomorphism. $\leftarrow$ Let $k \cong A/m_A \cong B/m_B$
2. $m_A \to m_B/m_B^2$ is surjective.
3. B is a finitely generated A-module (via f).

Show that f is surjective.

Noetherian $\Rightarrow m_A \subset A$, $m_B \subset B$ fin gen ideals

f: surjective $\Leftrightarrow$ B is generated by $1 \in B$ as an A-module. $\overset{\text{Nakayama}}{\Longleftrightarrow}$ $B \otimes_A k \cong B/m_A B$ is a 1-dim vector space $/k$.

$\Leftrightarrow m_A B \xhookrightarrow{g} m_B$ is an Isom of B-module

$$\begin{tikzcd}
m_A \arrow[r, hook] \arrow[d] & A \arrow[r] \arrow[d, "f"] & A/m_A \cong k \arrow[d] \arrow[dd, bend left, "\shortparallel"] \\
m_A B \arrow[r, hook] \arrow[d, hook, "g"'] & B \arrow[r] \arrow[d, "\shortparallel"] & B/m_A B \overset{?}{\cong} k \arrow[d] \\
m_B \arrow[r, hook] & B \arrow[r] & B/m_B \cong k
\end{tikzcd}$$

It suffices to show $\operatorname{cok} g = 0$, or by Nakayama, $(\operatorname{cok} g) \otimes_B k \cong 0$.

$(\operatorname{cok} g) \otimes_B B/m_B \cong \operatorname{cok}(m_A B \otimes_B B/m_B \xrightarrow{g \otimes \mathrm{id}} m_B \otimes_B B/m_B)$

$$\begin{tikzcd}
 & m_A B \otimes_B B/m_B \arrow[r, "g\otimes\mathrm{id}"] & m_B \otimes_B B/m_B \arrow[d, phantom, "\cong"] \\
m_A B := \mathrm{Im}(m_A \otimes B \to B) \arrow[ur, bend left] & m_A \otimes_A B \otimes_B B/m_B \arrow[u] \arrow[d, phantom, "\cong"] & m_B/m_B^2 \\
 & m_A \otimes_A A/m_A & \\
 & m_A \arrow[u, two heads] \arrow[uur, bend right] &
\end{tikzcd}$$

$g \otimes \mathrm{id}$ factors the canonical map $m_A \to m_B/m_B^2$, which is surjective by assumption 2.

$\rightsquigarrow g \otimes \mathrm{id}$: surj, i.e. $(\operatorname{cok} g) \otimes_B k = 0$ $\square$

Integrality

F2015

6. Let K be a finite algebraic extension of $\mathbb{Q}$.

   (a) Give the definition of an integral element of K.

   (b) Show that the set of integral elements in K form a sub-ring of K.

   (c) <u>Determine</u> the ring of integers in each of the following two fields *No credit for memorized answers*: (1) $\mathbb{Q}(\sqrt{13})$, and (2) $\mathbb{Q}(\sqrt[3]{2})$.

(a) $x \in K$ integral $\iff \exists f(T) \in \mathbb{Z}[T]$ monic, $f(x) = 0$

(b) $x \in K$ integral $\overset{①}{\Rightarrow}$ $\mathbb{Z}[x]$: finite $\mathbb{Z}$-algebra $\overset{②}{\Rightarrow}$ $\exists A$: finite $\mathbb{Z}$-alg s.t. $x \in A \subset K$

$\overset{③}{\Rightarrow}$ $\exists$ faithful $\mathbb{Z}[x]$-module M which is fin. gen. as a A-module $\overset{④}{\Rightarrow}$ x : integral

① : easy ② Take $A = \mathbb{Z}[x]$ ③ Take $M = A$

④ The action of x on M defines $f : M \to M$. Then $\exists P(T) \in \mathbb{Z}[T]$ monic s.t. $P(f) = 0$, i.e. $P(x) \curvearrowright_{A[x]} M$ $= 0$.

Take a surjection $A^n \xrightarrow{\pi} M$.
Using freeness we can lift f to $\tilde{f}$

$$\begin{tikzcd} A^n \arrow[r, dashed, "\tilde{f}"] \arrow[d, "\pi"'] & A^n \arrow[d] \\ M \arrow[r, "f"'] & M \end{tikzcd}$$

Apply Cayley-Hamilton to see that we can take P to be the characteristic polynomial of $\tilde{f}$

Now
$x, y \in K$ integral
$\Rightarrow \mathbb{Z}[x, y] = \mathbb{Z}[x][y]$: finite $\mathbb{Z}$-algebra,
$\rightsquigarrow x \pm y, xy$: integral by the third characterization of integrality.

(c) In general, if A : normal domain, $K = \mathrm{Frac}\, A$, L/K finite ext, B = int cl. of A,
then $\forall x \in L$ [$x \in B \iff$ the monic minimal polynomial of $x_{/K}$ have coeff. in A.]

(1) $\alpha = x + y\sqrt{13}$, $x, y \in \mathbb{Q}$ $\rightsquigarrow (\alpha - x)^2 = 13y^2 \iff \alpha^2 - 2x\alpha + (x^2 - 13y^2) = 0$.

so α : integral$_{/\mathbb{Z}}$ $\iff 2x \in \mathbb{Z}$, $x^2 - 13y^2 \in \mathbb{Z} \iff x = \frac{n}{2}, y = \frac{m}{2}$, $n, m \in \mathbb{Z}$, $2 \mid n - m$

So the ring of integer is $\mathbb{Z}\left[\frac{1+\sqrt{13}}{2}\right]$

(2) The answer is $\mathbb{Z}[\sqrt[3]{2}]$, but it's not easy. → https://math.stackexchange.com/questions/99913/easy-way-to-show-that-mathbbz-sqrt32-is-the-ring-of-integers-of-mat

F2009

2. Consider $\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$. Determine the integral closure of $\mathbb{Z}$ in $\mathbb{Q}[\sqrt{5}]$.

$\rightsquigarrow \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, same as above.

S2012

5. (a) Give the definition of a Dedekind domain. 1-dim'l, noetherian, normal domain

   (b) Give an example of a Dedekind domain that is not a principal ideal domain. Verify from the definition that it *is* a Dedekind domain, and also that it isn't a principal ideal domain.

Dedekind ←
- $\mathbb{Z}[\sqrt{5}]$ is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{5})$, so it's normal
- Noetherian because $\mathbb{Z}[\sqrt{5}] \cong \mathbb{Z}[x]/(x^2+5)$, $\mathbb{Z}[x]$ noetherian (by Hilbert basis thm)
- Since any integral extension preserves the Krull dim (and $\dim \mathbb{Z} = 1$), $\dim \mathbb{Z}[\sqrt{-5}] = 1$.

Not an PID : $\mathfrak{a} = (2, 1+\sqrt{5})$ If $\mathfrak{a} = (a)$ for some $a \in \mathbb{Z}[\sqrt{5}]$, then $\exists b, c \in \mathbb{Z}[\sqrt{5}]$ s.t. $2 = ab$, $(1+\sqrt{5}) = ac$

So $4 = 2 \cdot 2 = ab\bar{a}\bar{b} = |a|^2|b|^2$, $6 = (1+\sqrt{5})(1-\sqrt{5}) = ac\bar{a}\bar{c} = |a|^2|c|^2$ ($|a|^2, |b|^2, |c|^2 \in \mathbb{Z}$).

and we must have $|a|^2 = 1$ or 2. The only possibility (up to unit) is $a = 1$. This cannot happen because

if $a = 1$ we have $(a\bar{a}) = (2, 1+\sqrt{-5})(2, 1-\sqrt{5}) = (2)$, where $(a\bar{a}) = (1)$, which is not true.

S2005 **5.** Let A be an integral domain and let K be its field of fractions. Let A' be the integral closure of A in K. Let $P \subset A$ be a prime ideal and let $S = A - P$. (Note that $A_P = S^{-1}A$ is contained in K.) Show that A_P is integrally closed in K if and only if $(A'/A) \otimes_A A_P = 0$.

$0 \to A \to A' \to A'/A \to 0$

$0 \to A_P \to A'_P \to (A'/A)\otimes A_P \to 0$ $\big) \otimes A_P$, exact, so $(A'/A) \underset{A}{\otimes} A_P = 0 \iff A_P = (A')_P$.

Therefore it suffices to prove that A'_P is the integral closure of A_P in K.

- Take $\frac{x}{s} \in A'_P$, $x \in A'$, $s \notin P$. Then $\exists a_1, \dots, a_n \in A$ s.t. $x^n + a_1 x^{n-1} + \dots + a_n = 0$

  dividing by s^n, we get $\left(\frac{x}{s}\right)^n + \left(\frac{a_1}{s}\right)\left(\frac{x}{s}\right)^{n-1} + \dots + \left(\frac{a_n}{s^n}\right) = 0$, which is A_P-coeff. monic.

  So A'_P is contained in the integral closure of A_P.

- Conversely, take any integral element $x \in K$ over A_P.

  This means that $\exists \frac{a_1}{s_1}, \dots, \frac{a_n}{s_n} \in A_P$ s.t. $x^n + \frac{a_1}{s_1}x^{n-1} + \dots + \frac{a_n}{s_n} = 0$.

  multiplying by $(s_1 \cdots s_n)^n$ we get $(s_1 \cdots s_n x)^n + a'_1 (s_1 \cdots s_n x)^{n-1} + \dots + a'_n = 0$, so we have $s_1 \cdots s_n x \in A'$, and $x \in A'_P$. ☒

F2013 2. Let a be an integral algebraic number such that its norm is 1 for any imbedding into $\mathbb{C}$, the field of complex numbers. Prove that a is a root of unity.

Consider the minimal polynomial $f(x) \in \mathbb{Z}[x]$ of α.

Since all embedding of a into $\mathbb{C}$ is of norm 1, (i.e. all $\mathbb{Z}[x]/(f(x)) \longrightarrow \mathbb{C}$ lands in the unit circle)

over $\mathbb{C}$ it decomposes as

$$f(x) = \prod_{i=1}^{d} (x - \alpha_i) \quad \begin{pmatrix} d = \deg d, \\ |\alpha_i| = 1 \end{pmatrix}$$

Any polynomial of the form $\prod_{i=1}^{d}(x - \beta_i)$, $|\beta_i| = 1$, the absolute value of the coefficient of x^k is bounded by $\binom{d}{k}$, so there exists only finitely many such polynomials.

Now considering $f_m(x) = \prod_{i=1}^{d}(x - \alpha_i^m)$, which again satisfies $|\alpha_i^m| = 1$, we see $f_k = f_{mk}$ $\exists k, m$ (e.g. consider $f_p, f_{p^2}, \dots$)

So $\alpha_1^k = (\sigma \alpha_1^k)^m$ $\exists \sigma \in \mathrm{Gal}_{\mathbb{Q}}(f)$, and because $\exists N$ $\sigma^N = \mathrm{id}$, $\alpha_1^k = \sigma^N((\alpha_1^k)^{m^N})$

$= \alpha_1^{k \cdot m^N}$, so α_1 is a root of unity. ☒

F2004 **4.** Let $\lambda_1, \dots, \lambda_n$ be roots of unity, with $n \geq 2$. Assume that $\frac{1}{n}\sum_{i=1}^{n} \lambda_i$ is integral over $\mathbb{Z}$. Show that either $\sum_{i=1}^{n} \lambda_i = 0$ or $\lambda_1 = \lambda_2 = \dots = \lambda_n$.

The proof for the above problem works even if $|\alpha_i| = 1$ is replaced by $|\alpha_i| \leq 1$ up to here

we instead get $\alpha = 0$ or α: root of unity.

Now set $\alpha = \frac{1}{n}\sum_{i=1}^{n} \lambda_i$, then $|\alpha| \leq \frac{1}{n}\sum|\lambda_i| = 1$. so is its conjugates (since $\alpha \in \mathbb{Q}(\zeta_N)$ $\exists N$, conjugates of α are still an average of roots of unity)

Therefore we have α or $|\alpha| = 1$, in the latter case the equality holds in the triangle ineq. so $\lambda_1 = \dots = \lambda_n$. ☒

Ring theory random problems

S2010 **2.** Let R be a ring such that $r^3 = r$ for all $r \in R$. Show that R is commutative. (Hint: First show that r^2 is central for all $r \in R$.)

$\forall a, b \quad ab = 0 \Rightarrow ba = bababa = 0$.

For any $s \in R$ we have $sr^2 = sr \cdot r = sr \cdot r^3 = sr^4$, so $sr^2(1-r^2) = 0$

$\rightsquigarrow (1-r^2)sr^2 = 0 \rightsquigarrow sr^2 = r^2sr^2$.

Similarly we get $r^2sr^2 = r^2s$, so $sr^2 = r^2s$, i.e., r^2 is central.

Now $(r+r^2)^2 = r^2 + 2r^3 + r^4 = 2r + 2r^2 = 2(r^2+r)$

So $(r^2+r) = (r^2+r)^3 = \underbrace{2(r^2+r)^2}_{\text{central}}$: central, and $r = (r^2+r) - r^2$ is central as well.

S2006 **2.** Let R be a ring with identity 1. Let $x, y \in R$ such that $xy = 1$.

(1). Assume R has no zero-divisor. Show that $yx = 1$. $\quad x(yx-1) = 0 \Rightarrow yx = 1$ (or $0 = 1$)

(2). Assume R is finite. Show that $yx = 1$.

$$\begin{tikzcd} R \arrow[r, "y\cdot(-)", "\text{inj}"'] \arrow[rr, bend right, "\mathrm{id}_R"'] & R \arrow[r, "x\cdot(-)", "\text{surj}"'] & R \end{tikzcd}$$

finite $\Rightarrow$ both bij $\quad zx(yx-1) = 0$.

$\rightsquigarrow \exists z$ s.t. $zx = 1$

Tensor products over fields (everything is free ⇒ no flatness problem)

S2018

> (3) Let K/k be a finite separable field extension, and let L/k be any field extension. Show that $K \otimes_k L$ is a product of fields.

(This step is unnecessary but) finite separable ext ⇒ simple, i.e. $K = k(\alpha) = k[x]/(f(x))$, $\exists \alpha \in K$, f: min. poly of α.

So $K \otimes_k L \cong k[x]/(f(x)) \otimes_k L \cong L[x]/(f(x))$

$\underset{\text{CRT}}{\cong} \prod_i \underbrace{L[x]/(f_i(x))}_{\text{fields}}$

$f(x) = f_1(x) f_2(x) \cdots f_n(x)$: irred factors in L.
f: separable ⇒ f_i relatively prime

Similar argument ⇝ L/k Separable ⟺ $L \otimes_k \bar{k} \cong \bar{k}^{[L:k]}$
L/k Galois ⟺ $L \otimes_k L \cong L^{[L:k]}$

F2019

> 3. Let F, L be extensions of a field K. Suppose that F/K is finite. Show that there exists an extension E/K such that there are monomorphisms of F into E and of L into E which are identical on K.

$$\begin{tikzcd} & \exists E & \\ F \arrow[ur] & & L \arrow[ul] \\ & K \arrow[ul, dash, "\text{fin}"] \arrow[ur, dash] & \end{tikzcd}$$

Consider the ring $F \otimes_k L$. This is nonzero because as K-modules $F \otimes_k L \cong K^n \otimes_k L \cong L^n$.

So $\exists\, m \subset F \otimes_k L$: maximal ideal.

Then the following diagram commutes and f, g are injective (because ring hom between fields)

$$\begin{tikzcd} K \arrow[r, hook] \arrow[d, hook] & F \arrow[d] \arrow[ddr, "g"] & \\ L \arrow[r] \arrow[drr, bend right, "f"'] & F \otimes_k L \arrow[dr] & \\ & & E = F \otimes_k L/m \end{tikzcd}$$

F2009

> **4.** Let E and F be finite field extensions of a field k such that $E \cap F = k$, and that E and F are both contained in a larger field L. Assume that E is Galois over k. Show that $E \otimes_k F \cong EF$.

$$\begin{tikzcd} & L & \\ & E \otimes_k F \arrow[u] & \\ E \arrow[uur] \arrow[ur] & & F \arrow[uul, dash] \arrow[ul] \\ & k \arrow[ul, dash, "\text{fin. Gal}"] \arrow[ur, dash, "\text{finite}"'] & \end{tikzcd}$$

Since EF is by definition the image of $E \otimes_k F$ in L,
It suffices to prove that $E \otimes_k F$ is a field.
Since E : finite Galois, $\exists \alpha \in E$ s.t. $E = k(\alpha) \cong k[x]/(f(x))$
where f : monic min poly of α, E is the minimal decomposition field of f.
So $E \otimes_k F \cong F[x]/(f(x))$. We need to prove that f is irreducible in $F[x]$.
If $f(x) = g(x) h(x)$ for $g(x), h(x) \in F[x]$ (monic, $\deg \geq 1$),
then since E contains all the roots of f in $\bar{L}$, we also have
$g(x), h(x) \in E[x]$, so $g(x), h(x) \in E[x] \cap F[x] = k[x]$.
This contradicts to the fact that f is irred. in $k[x]$. ☑

S2008 **5.** Let k be a field of characteristic zero. Assume that E and F are algebraic extensions of k and both contained in a larger field L. Show that the k-algebra $E \otimes_k F$ has no nonzero nilpotent elements.

$$x = \sum_{i=1}^{n} e_i \otimes f_i \rightsquigarrow \begin{array}{l} \exists E' \subset E \\ \exists F' \in F \end{array} \quad \text{s.t. } x \in E' \otimes F'.$$

$$\begin{tikzcd}[column sep=small] & L \arrow[dl, dash] \arrow[dr, dash] & \\ E \arrow[d, dash] & & F \arrow[d, dash] \\ E' \arrow[dr, dash, "\text{finite}"'] & & F' \arrow[dl, dash, "\text{finite}"] \\ & k & \end{tikzcd}$$

E'/k : finite separable ext

$\rightsquigarrow E' \cong k[x]/(f(x))$ $f(x)$ separable polynomial

$\rightsquigarrow E' \otimes_k F' \simeq F'[x]/(f(x)) \underset{CRT}{\cong} \prod_{i=1}^{k} F'[x]/(f_i(x))$: product of fields ($\Rightarrow$ reduced)

$f = f_1 \cdots f_r$ coprime irred factors & separable

$\boxed{\checkmark}$

S2004 **5.** Show that there is a $\mathbb{C}$-algebra isomorphism between $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ and $\mathbb{C} \times \mathbb{C}$.

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{R}[x]/(x^2+1) \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C}[x]/(x^2+1) \cong \mathbb{C}[x]/(x+\sqrt{-1})(x-\sqrt{-1}) \underset{CRT}{\cong} \mathbb{C} \times \mathbb{C}$$

F2005 **5.** Let $\mathbb{C}$ and $\mathbb{R}$ be complex and real number fields. Let $\mathbb{C}(x)$ and $\mathbb{C}(y)$ be function fields of one variable. Consider $\mathbb{C}(x) \otimes_{\mathbb{R}} \mathbb{C}(y)$ and $\mathbb{C}(x) \otimes_{\mathbb{C}} \mathbb{C}(y)$.

(1). Determine if they are integral domains.

(2). Determine if they are fields.

- $\mathbb{C} \times \mathbb{C} \cong \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \subset \mathbb{C}(x) \otimes_{\mathbb{R}} \mathbb{C}(y)$ so both (1)(2) are No.

- $\mathbb{C}(x) \otimes_{\mathbb{C}} \mathbb{C}(y) \longrightarrow \mathbb{C}(x,y)$ injective $\mathbb{C}$-alg hom

  $f(x) \otimes g(y) \longmapsto f(x)g(y)$

  ($\because$) if $\sum_{i=1}^{n} \frac{f_i(x)}{s_i(x)} \otimes \frac{g_i(y)}{t_i(y)} \mapsto 0$ (f_i, g_i, s_i, t_i polynomials).

  $= \frac{1}{s(x)} \otimes \frac{1}{t(y)} \underline{\sum_{i=1}^{n} \tilde{f}_i(x) \otimes \tilde{g}_i(y)} \longmapsto 0.$

  Using $\mathbb{C}[x] \otimes_{\mathbb{C}} \mathbb{C}[y] \xrightarrow{\cong} \mathbb{C}[x,y]$

  $\sum \tilde{f}_i(x) \otimes \tilde{g}_i(y) \longmapsto 0$ it has to be 0.

  So $\mathbb{C}(x) \otimes_{\mathbb{C}} \mathbb{C}(y)$ can be identified with the subring of $\mathbb{C}(x,y)$ of those element that can be written in the form $\frac{\sum f_i(x) g_i(y)}{s(x)t(y)}$.

$\rightsquigarrow$ it is a int dom but not a field (e.g. $1-xy$ has no inverse)

F2003 4. Verify the isomorphism of algebras over a field K:

$$\mathbb{M}_n(K) \otimes_K \mathbb{M}_m(K) \simeq \mathbb{M}_{mn}(K).$$

[Note: $\mathbb{M}_n(K)$ denotes the algebra of $n \times n$ matrices over K.]

$\mathbb{M}_n(K) \otimes_K S \cong \mathbb{M}_n(S)$ in general, so $\mathbb{M}_n(K) \otimes_K \mathbb{M}_m(K) \cong \mathbb{M}_n(\mathbb{M}_m(K)) \cong \mathbb{M}_{nm}(K)$

multiplication of matrices can be computed by blocks

Irreducibility of polynomials

$f \in \mathbb{Z}[X]$ monic

Gauss' lemma : f : irred $/\mathbb{Q}$ $\Longleftrightarrow$ f : irred $/\mathbb{Z}$ (or more generally $/R$: UFD and $K = \mathrm{Frac}(R)$)

Eisenstein criterion : $f(x) = X^n + \underbrace{a_1 X^{n-1} + \cdots + a_{n-1}X + a_n}_{\in p} \in R[X]$, $a_n \notin p^2$, $p \subset R$ prime

(proof : $R[X] \longrightarrow R/p[X]$: int dom, $f(x) \longmapsto X^n$; $g(x) \cdot h(x) \longmapsto X^k \cdot X^\ell$ $\rightsquigarrow$ constant term of $g(x)h(x) \in p^2$)

mod p reduction : If f (monic) mod $p \in \mathbb{F}_p[X]$ is irreducible, then $f \in \mathbb{Z}[T]$ is irred.

(proof: $\mathbb{Z}[T] \twoheadrightarrow \mathbb{F}_p[X]$, $f = gh \rightsquigarrow \bar{f} = \bar{g}\bar{h}$, $\deg \bar{f} = \deg f$, $\deg \bar{g} = \deg g$, $\deg \bar{h} = \deg h$)

S2018 3. Let R be the ring $\mathbf{Z}[\zeta_p]$, where p is a prime number and ζ_p denotes a primitive pth root of unity in $\mathbf{C}$. Prove that if an integer $n \in \mathbf{Z}$ is divisible by $1-\zeta_p$ in R, then p divides n.

When $p = 2$, $\zeta_p = -1$ and $1-\zeta_p \mid n \Leftrightarrow 2 \mid n$ is obvious. Assume p: odd.

$\alpha = 1-\zeta_p \Leftrightarrow \zeta_p = 1-\alpha \Rightarrow 1 = (1-\alpha)^p$, so $\underbrace{\frac{(\alpha-1)^p + 1}{\alpha}}_{1+(\alpha-1)^p} = \alpha^{p-1} - p\alpha^{p-2} + \binom{p}{2}\alpha^{p-3} - \cdots + \underbrace{\binom{p}{p-1}}_{=p} \cdot \alpha^0 = 0$.

This is the minimal polynomial of α by the Eisenstein's criterion

If $\alpha \mid n$ in R, then $\forall \sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, $\sigma\alpha \mid n$.

$\Rightarrow p = \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})} \sigma\alpha \mid n^{\#\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})} \Rightarrow p \mid n$. ☒

const term of the char poly = norm

F2008 **2.** Show that the polynomial $x^5 - 5x^4 - 6x - 2$ is irreducible in $\mathbb{Q}[x]$

irreducible mod 5.

no linear factor, so possible factorization is

$x^5 - x - 2 = (x^2 + ax + b)(x^3 - ax^2 + (a^2-b)x - (a^3 - 2ab))$ to match coeff's of $x^5, \cdots, x^2$.

but $(a^2-b)b - a^2(a^2-2b) = -1$, $ab(a^2-2b) = -2$

$\Rightarrow (a, b) = (-1, 4), (2, -1), (2, 3)$

F2003 3. Obtain a factorization into irreducible factors in $\mathbb{Z}[x]$ of the polynomial $x^{10} - 1$.

$X^{10} - 1 = (X^5+1)(X^5-1) = (X-1)(X+1)(X^4 - X^3 + X^2 - X + 1)(X^4 + X^3 + X^2 + X + 1)$

irreducible mod 2

S2004

3. Let k be a field with characteristic 0. Let $m \geq 2$ be an integer. Show that $f(x, y) = x^m + y^m + 1$ is irreducible in $k[x, y]$.

take an irreducible factor $p(y)$ of y^m+1 and let $P = (p(y)) \subset k[x,y]$

$\Downarrow$

$(p(y)) \subset k[y]$ prime

$\gcd\left(\frac{d}{dy}(y^m+1),\ y^m+1\right) = \gcd\left(\underset{k^\times}{\underset{\cap}{m}} y^{m-1},\ y^m+1\right) = 1 \quad \Rightarrow y^m+1 \notin P^2$

by Eisenstein criterion (mod P) f is irred.

There are cases that mod p reduction never works:

S2017

S2007

(2) Write down the minimal polynomial for $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$ and prove that it is reducible over $\mathbb{F}_p$ for every prime number p.

$\alpha = \sqrt{2}+\sqrt{3} \Rightarrow (\alpha-\sqrt{3})^2 = 2 \Leftrightarrow \alpha^2+1 = 2\sqrt{3}\alpha \Rightarrow \alpha^4+2\alpha^2+1 = 12\alpha^2 \Leftrightarrow \alpha^4-10\alpha^2+1=0.$

It can be factored into degree 2 polynomial if $\sqrt{2}$ or $\sqrt{3}$ or $\sqrt{6}$ exists. If $\left(\frac{2}{p}\right)=-1, \left(\frac{3}{p}\right)=-1, \left(\frac{6}{p}\right)=-1$

then $\left(\frac{2\cdot3\cdot6}{p}\right)=\left(\frac{36}{p}\right)=-1$

but $\left(\frac{36}{p}\right) = \begin{cases} 0 & p=2,3 \\ 1 & p\neq 2,3 \end{cases}$

S2015

4. Prove that the polynomial x^4+1 is not irreducible over any field of positive characteristic.

- $x^4 \pm 2x^2+1 \mp 2x^2 = (x^2+1-\sqrt{\pm2}\,x)(x^2+1+\sqrt{\pm2}\,x)$
- $x^4+1 = x^4-(-1) = (x^2-\sqrt{-1})(x^2+\sqrt{-1})$

so if any of $\sqrt{-1}, \sqrt{\pm2}$ exists in $\mathbb{F}_p$, x^4+1 can be factored. Now $(-1)(+2)(-2)=4$ is a quad. residue. So by the same argument as ↗ so is one of $-1, \pm2$

F2010

2. (a) Find the complete factorization of the polynomial $f(x) = x^6 - 17x^4 + 80x^2 - 100$ in $\mathbb{Z}[x]$. $= (x^2-2)(x^2-5)(x^2-10)$

(b) For which prime numbers p does $f(x)$ have a root in $\mathbb{Z}/p\mathbb{Z}$ (i.e, $f(x)$ has a root modulo p)? Explain your answer. $\forall p$

by the same argument

Galois theory (non-Computational)

S2009

3. Consider the field $K = \mathbb{Q}(\sqrt{a})$ where $a \in \mathbb{Z}$, $a < 0$. Show that K cannot be embedded in a cyclic extension whose degree over $\mathbb{Q}$ is divisible by 4.

Assume $\exists$ field ext $L/K/\mathbb{Q}$ such that $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/4n\mathbb{Z}$

$$\begin{array}{cc} (\mathbb{C} & \\ \;\mid) & \\ L & 1 \\ \mid & \mid \\ K & 2\mathbb{Z}/4n\mathbb{Z} \\ \mid 2 & \mid \\ \mathbb{Q} & \mathbb{Z}/4n\mathbb{Z} \end{array}$$

We can embed L into $\mathbb{C}$, so fix one embedding and consider L as a subfield of $\mathbb{C}$.
Since $[K:\mathbb{Q}] = 2$, K is fixed by an index 2 subgroup of $\mathrm{Gal}(L/\mathbb{Q})$, so it has to correspond to $2\mathbb{Z}/4n\mathbb{Z}$.
Since $K \not\subset \mathbb{R}$, we have $L \not\subset \mathbb{R}$ as well, so the complex conjugation defines an element $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ of order 2. $\mathbb{Z}/4n\mathbb{Z}$ has only one order 2 element, namely $[2n]$, so $[2n] = \tau \in \mathrm{Gal}(L/\mathbb{Q})$, therefore $\tau \in 2\mathbb{Z}/4n\mathbb{Z} = \mathrm{Gal}(L/K)$.
This is a contradiction, since $\tau(\sqrt{a}) \neq \sqrt{a}$, so $K \not\subset L^{\tau}$.

F2000

4. Let G be a finite group. Show that there exists a Galois field extension K/k whose Galois group is isomorphic to G.

Take $G \hookrightarrow S_n$ (e.g. $n = |G|$, permutation defined by left multiplication)

Note that $\forall K$, $L := K(X_1, \cdots, X_n)$

$$\begin{array}{c} L := K(X_1,\cdots,X_n) \\ \mid \\ K(s_1,\cdots,s_n) \end{array}$$

$\left(s_i : \begin{array}{c} i\text{th} \\ \text{elementary} \\ \text{sym poly of} \\ X_1,\cdots,X_n \end{array} \right)$

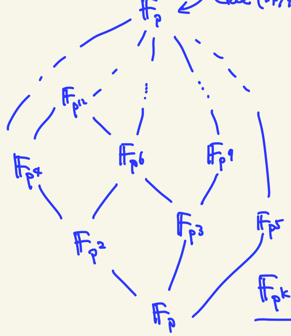
Galois with $\mathrm{Gal} = S_n$.

$$\begin{array}{c} \{e\} \\ \mid \\ G \\ \mid \\ S_n \end{array} \qquad \begin{array}{c} L \\ \mid \\ L^G \end{array}$$

Take the fixed subfield, then it is Galois, $\mathrm{Gal}(L/L^G) \cong G$

Finite fields

$\overline{\mathbb{F}_p} \circlearrowleft \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \cong \hat{\mathbb{Z}} \ (= \varprojlim \mathbb{Z}/n\mathbb{Z})$



$\mathbb{F}_{p^k} \subset \mathbb{F}_{p^n} \iff k \mid n$

$\forall p,\ \forall n\ \ \exists!$ field $\mathbb{F}_{p^n}$ with p^n elements (upto isom)

$=$ the splitting field of $T^{p^n} - T \in \mathbb{F}_p[T]$

Fix $\overline{\mathbb{F}_p}$. $\rightsquigarrow \mathbb{F}_q = \left\{ \text{fixed pts of } \mathrm{Frob}_q : \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p},\ x \mapsto x^q \right\}$

- $\mathbb{F}_{q^m}/\mathbb{F}_q$ Galois, $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) = \langle \mathrm{Frob}_q \rangle \cong \mathbb{Z}/m\mathbb{Z}$
- $\mathbb{F}_q^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}$

F2016

3. Let F be a finite field of order 2^n. Here $n > 0$. Determine all values of n such that the polynomial $x^2 - x + 1$ is irreducible in $F[x]$.

$X^2 - X + 1$ is irreducible in $\mathbb{F}_2[X]$, and $\mathbb{F}_4 \cong \mathbb{F}_2[X]/(X^2-X+1) \rightsquigarrow X^2 - X + 1$ splits in $\mathbb{F}_4$

So if we fix $\overline{\mathbb{F}_2}$, the two roots of $x^2 - x + 1$ are in $\mathbb{F}_4 \setminus \mathbb{F}_2$.

$X^2 - X + 1$ is irreducible $\in \mathbb{F}_{2^n}[X] \iff \mathbb{F}_4 \not\subset \mathbb{F}_{2^n} \iff 4 \nmid 2^n \iff n$: odd.

F2015

5. Let L be a finite field ($\mathbb{F}_q$). Let a and b be elements of $L^\times$ (the multiplicative group of L) and $c \in L$. Show that there exist x and y in L such that $ax^2 + by^2 = c$.

Let $n = \#\left((\mathbb{F}_q^\times)^2\right) + 1$, i.e. the number of square element of L.

$n = \begin{cases} q & \text{if } q: \text{even} \\ \frac{q+1}{2} & \text{if } q: \text{odd}, \end{cases}$ so $2n > \# L$ in both cases.

Now since $a, b \in L^\times$, we have $\#\{ax^2 \mid x \in L\} = \#\{c - by^2 \mid y \in L\} = n$.
By pigeonhole principle, $\{ax^2 \mid x \in L\} \cap \{c - by^2 \mid y \in L\} \neq \phi$, so $ax^2 + by^2 = c$ has a solution.

F2013

6. Let p be a prime and let F be a field of characteristic p.
   (a) Prove that the map $\varphi : F \to F, \varphi(a) = a^p$ is a field homomorphism. easy
   (b) F is said to be *perfect* if the above homomorphism φ is an automorphism. Prove that every finite field is perfect. field hom between finite field are bijective.
   (c) If x is an indeterminate and F is any field of characteristic p, prove that the field $F(x)$ is not perfect.

$f(x), g(x) \in F[x] \rightsquigarrow \varphi\left(\frac{f(x)}{g(x)}\right) = \frac{f(x^p)}{g(x^p)} \neq x \in F(x)$ because

$p \mid \deg f(x^p)$, $p \nmid \deg g(x^p) + 1$

F2017 (5) Let K/k be an extension of finite fields with $\#k = q$, let $\Phi\colon x \mapsto x^q$ denote the qth power Frobenius map on K, and let $G := \mathrm{Gal}(K/k)$.

(a) Compute the minimal polynomial of Φ as a k-linear endomorphism of K.

(b) Use (a) to prove the *normal basis theorem* in the case of the extension K/k: there exists $x \in K$ such that the set $\{\sigma x \mid \sigma \in G\}$ is a k-basis for K.[1] (According to taste, it may be helpful to note that this is equivalent to the statement that $K \simeq k[G]$ as $k[G]$-modules.)

(a) Let $K \cong \mathbb{F}_{q^n}$. Since $\mathbb{F}_{q^n} = \{x \in \overline{\mathbb{F}_q} \mid \Phi^n(x) = x\}$, $\Phi^n - 1$ is divided by the min. poly $f(\Phi)$.
Suppose $\deg f \leq n-1$. Then any $x \in \mathbb{F}_{q^n}$ is the root of the polynomial $f(\Phi)(x) - X$.
However, the degree of $\Phi(f)(x) - X$ is at most q^{n-1}, which is impossible.
So $f(T) = T^n - 1$ is the minimal polynomial of Φ.

(b) By (a), $\mathbb{F}_{q^n}$ is a faithful $\mathbb{F}_q[X]/(X^n-1)$-module where X acts on $\mathbb{F}_q$ by Φ.
Since $\mathbb{F}_q[X]$ is a PID, by the structure thm of fin gen modules / PID (and by the fact that its annihilator is (X^n-1))

$$\mathbb{F}_{q^n} \cong \mathbb{F}_q[X]/(X^n-1) \oplus \mathbb{F}_q[X]/f_1(x) \oplus \cdots \oplus \mathbb{F}_q[X]/f_k(x), \quad f_k(x) \mid \cdots \mid f_1(x) \mid (X^n-1).$$

Since $\dim_{\mathbb{F}_q} \mathbb{F}_{q^n} = n$, $\dim_{\mathbb{F}_q} \mathbb{F}_q[X]/(X^n-1) = n$, we have $\mathbb{F}_{q^n} \cong \mathbb{F}_q[X]/(X^n-1) \left(\cong \mathbb{F}_q[\mathbb{Z}/n\mathbb{Z}]\right)$ $\boxed{}$

(This proof works for all cyclic ext)

F2010 **5.** Let $\mathbb{F}_q$ be a finite field with $q = p^n$ elements. Here p is a prime number. Let $\varphi : \mathbb{F}_q \to \mathbb{F}_q$ be given by $\varphi(x) = x^p$.

(a) Show that φ is a linear transformation on $\mathbb{F}_q$ (as vector space over $\mathbb{F}_p$), then determine its minimal polynomial. $f(x) = x^n - 1$

(b) Supposed that φ is diagonalizable over $\mathbb{F}_p$. Show that n divides $p-1$.

(b) φ diagonalizable $\Leftrightarrow$ $X^n - 1$ splits into distinct linear factors in $\mathbb{F}_p[X]$
$\Leftrightarrow$ $\mathbb{F}_p^\times \cong \mathbb{Z}/p-1$ has n elements of order dividing n $\Leftrightarrow$ $n \mid p-1$

$\#$ of elements of order $d = \begin{cases} \varphi(d) & d \mid p-1 \\ 0 & d \nmid p-1 \end{cases}$

S2011 2. Let p be a prime, F a finite field with p elements and K a finite extension of F. Denote by $F^\times$ and $K^\times$ the multiplicative groups of nonzero elements of fields F and K, respectively. Prove that the norm homomorphism $N : K^\times \to F^\times$ is surjective.

Recall Norm map of a field ext L/k is defined by $x \in L \rightsquigarrow N_{L/k}(x) = \left(\det \text{ of } \begin{array}{c} L \to L \\ y \mapsto xy \end{array} \text{ as a } k\text{-linear map}\right)$

$= \prod_{\sigma \in \mathrm{Hom}_k(L, \overline{k})} (\sigma x)^{[L:k]_i} \in K$ — 1 if separable

$\mathrm{Gal}(L/k) = \mathrm{Aut}_k(L)$ if L/k normal

$K = \mathbb{F}_q$, $q = p^n$ $\rightsquigarrow$ $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \langle \varphi \rangle$ $\varphi : x \mapsto x^p$.

$F = \mathbb{F}_p$

$$N_{K/F}(x) = \prod_{\sigma \in \langle\varphi\rangle} \sigma x = x \cdot x^p \cdot x^{p^2} \cdot \ldots \cdot x^{p^{n-1}} = x^{\frac{p^n-1}{p-1}}$$

Take x to be the primitive root of $\mathbb{F}_q$ (i.e. the generator of $\mathbb{F}_q^\times$)
then $x^{\frac{p^n-1}{p-1}} \in \mathbb{F}_p^\times$ has order $p-1$, so it generates $\mathbb{F}_p^\times$. $\boxed{}$

Note (linear independence of characters)

$\left(\begin{array}{l}\forall G: \text{monoid} \\ \forall L: \text{field}\end{array}\right)$. $\chi_1, \dots, \chi_n : G \to (L, *)$: distinct monoid hom
Then $\chi_1, \dots, \chi_n$: linearly indep $/L$

☺ Induction on n : $n=1$ case $\chi_1(1) = 1$ ✓

$n>1$ Take $(\lambda_1, \dots, \lambda_n) \neq (0, \dots, 0)$, want to prove $\sum \lambda_i \chi_i \neq 0$.

If $\lambda_i = 0$ for some i, then we are done by induction hypothesis.

If $\sum_i \lambda_i \chi_i = 0$ (we may assume $\lambda_n = -1$), then $\chi_n = \sum_{i=1}^{n-1} \lambda_i \chi_i$.

$$\chi_n(g)\chi_n(h) = \sum_{i=1}^{n-1} \lambda_i \chi_i(g) \chi_n(h)$$

$$-)\ = \chi_n(gh) = \sum_{i=1}^{n-1} \lambda_i \chi_i(g) \chi_i(h)$$

$$0 = \underbrace{\sum_{i=1}^{n-1} \lambda_i (\chi_n(h) - \chi_i(h))}_{\overset{\shortparallel}{0} \text{ by induction.}} \chi_i(g) \quad \forall g \in G \quad \rightsquigarrow \chi_n = \chi_i \ (\forall i). \text{ Contradiction}$$

F2008 **3.** Let k be a finite field and K be a finite extension of k. Let $\mathfrak{Tr} = Tr_k^K$ be the trace function from K to k. Determine the image of $\mathfrak{Tr}$ and prove your answer.

Since k is perfect, K/k is separable, so $\mathrm{Tr}_{K/k} \neq 0$ (If $\mathrm{Hom}_k(K, \bar{k}) = \{\phi_1, \dots, \phi_n\}$, K/k separable then $\mathrm{Tr}_{K/k}(\alpha) = \phi_1(\alpha) + \dots + \phi_n(\alpha) \neq 0$ by linear independence of characters)

$\mathrm{Tr}_{K/k} : K \to k$, nonzero k-linear $\rightsquigarrow$ surjective.

Artin-Schreier ext

S2014 3. Let L/K be a Galois extension of degree p with $\operatorname{char} K = p$. Show that $L = K(\theta)$, where θ is a root of $x^p - x - a$, $a \in K$, and, conversely, any such extension is Galois of degree 1 or p.] ✱

S2015 1. Let K be a field of characteristic $p > 0$. Prove that a polynomial $f(x) = x^p - x - a \in K[x]$ either irreducible, or is a product of linear factors. Find this factorization if f has a root $x_0 \in K$.

Fermat's little thm: $k^p = k$

Let $f_a(x) = x^p - x - a$. Note that $\forall k \in \mathbb{F}_p$, $f_a(x+k) = (x+k)^p - (x+k) - a \overset{\downarrow}{=} f_a(x)$

Therefore f_a is separable, and $K(\theta) = K[x]/(f_a(x))$ is the minimal splitting field of f_a.

$\left(\text{if } f_a(x_0) = 0, \text{ then } f_a(x) = \prod_{k \in \mathbb{F}_p} (x - x_0 - k)\right)$. $\Downarrow$ $K(\theta)$: Galois

If $\theta \in K$, then $[K(\theta) : K] = 1$ and $[K(\theta) : K] = p$ otherwise.

side rmk: $\mathrm{Gal}(K(\theta)/K) \cong \mathbb{Z}/p\mathbb{Z} \subset S_p$ because $\theta \mapsto \theta + k$ forces $\theta + i \mapsto \theta + k + i$.

Now we prove ✱ part : fix $\mathrm{Gal}(L/K) = \langle\sigma\rangle \cong \mathbb{Z}/p\mathbb{Z}$.

If we can find $\theta \in L$ s.t. $\sigma(\theta) = \theta + 1$, then $\sigma(\theta^p - \theta) = \sigma(\theta)^p - \sigma(\theta) = \theta^p - \theta$, so $a := \theta^p - \theta \in K$ and $K(\theta) = L$ (because $\theta \notin K$) is the splitting field of $x^p - x - a$.

To find such θ, note that by the linear independence of characters, $\{\sigma^k : L \to L \mid 0 \le k \le p-1\}$ is lin. indep. (L^-)

so $T^p - 1 = (T-1)^p$ is the minimal polynomial of $\sigma : L \to L$.

↳ Jordan normal form w.r.t. a K-basis $e_1, \dots, e_p$ is

$$\sigma = \underbrace{\begin{pmatrix} 1 & 1 & & 0 \\ & 1 & \ddots & \\ & & \ddots & 1 \\ 0 & & & 1 \end{pmatrix}}_{p}$$

$\sigma(e_1) = e_1 \rightsquigarrow e_1 \in K$, may assume $e_1 = 1$

$\sigma(e_2) = e_1 + e_2$, so let $\theta = e_2$ and we are done.

Cyclotomic extensions

$K(\mu_n)$: splitting field of $X^n - 1$ Galois$/K$ if $n \in K^\times$

$\rightsquigarrow \exists \chi : \mathrm{Gal}(K(\mu_n)/K) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ injective in general, isom when $K = \mathbb{Q}$ (because of the irreducibility of cyclotomic polynomials)

$\sigma \longmapsto i$ s.t. $\sigma(\zeta_n) = \zeta_n^i$

If we take ζ_n: a primitive nth root of unity, $K(\mu_n) = K(\zeta_n)$

S2002 5. **Let $\zeta = e^{\frac{2\pi i}{5}}$ and $K = \mathbf{Q}(\zeta)$ the field generated by ζ over the field of rational numbers. Prove that K contains $\sqrt{5}$.**

Let $\alpha = \zeta + \underset{\zeta^4}{\underset{\|}{\zeta^{-1}}}$, then $\alpha^2 = \zeta^2 + \underset{\zeta^3}{\underset{\|}{\zeta^{-2}}} + 2$. By $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0$, we have $\alpha^2 + \alpha - 1 = 0$

Since the discriminant of $X^2 + X - 1$ is 5, we have $\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\alpha) \subset K$.

S2008 **2.** Let ξ be a primitive 9-th root of unity. Find the minimal polynomial of $\xi + \xi^{-1}$ over $\mathbb{Q}$.

Since $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \simeq (\mathbb{Z}/9\mathbb{Z})^\times = \{\pm 1, \pm 2, \pm 4\}$ and the orbit of $\xi + \xi^{-1}$ by the Galois action is $\{\xi + \xi^{-1}, \xi^2 + \xi^{-2}, \xi^4 + \xi^{-4}\}$

$\xi \mapsto \xi^n \longleftrightarrow n$

The minimal polynomial of $\xi + \xi^{-1}$ is $(X - (\xi + \xi^{-1}))(X - (\xi^2 + \xi^{-2}))(X - (\xi^4 + \xi^{-4})) = X^3 - 3X + 1$.

F2007 1. Let G be a cyclic group of order 12. Construct a Galois extension K over $\mathbf{Q}$ so that the Galois group is isomorphic to G.

$\mathrm{Gal}(\mathbb{Q}(\zeta_{13})/\mathbb{Q}) \cong (\mathbb{Z}/13\mathbb{Z})^\times \cong \mathbb{Z}/12\mathbb{Z}$

F2011 3. Let G be a cyclic group of order 100. Let $K = \mathbb{Q}$, the field of rational numbers, or $K = F_p$, the finite field with p elements, p being a prime number. For each such K, construct a Galois extension L/K whose Galois group $Gal(L/K)$ is isomorphic to G. *Explain your construction in detail.*

$\mathrm{Gal}(\mathbb{Q}(\zeta_{101})/\mathbb{Q}) \simeq (\mathbb{Z}/101\mathbb{Z})^\times \cong \mathbb{Z}/100\mathbb{Z}$

$\mathrm{Gal}(\mathbb{F}_{p^{100}}/\mathbb{F}_p) \cong \mathbb{Z}/100\mathbb{Z}$

Inseparable field extensions

$f(x)$ is separable $\iff \gcd(f(x), f'(x)) = 1$.

When $f(x)$: irreducible, $f(x)$ is inseparable iff $f'(x) = 0$. (only happens for positive characteristic)

S2003 2. Let K be a field. A polynomial $f(x) \in K[x]$ is called *separable* if, in any field extension, it has distinct roots. Prove that:

(a) if K has characteristic 0, then each irreducible polynomial in $K[x]$ is separable; and

(b) if K has characteristic $p \neq 0$, then an irreducible polynomial $f(x) \in K[x]$ is separable if and only if has no form $g(x^p)$ where $g(x) \in K[x]$.

Give an example of an inseparable irreducible polynomial.

Irreducible $f(x) = \sum_{i=1}^{n} a_i x^i$ is inseparable iff $f'(x) = \sum_{i=1}^{n} i a_i x^i = 0 \iff \forall i\ p \mid i$ or $a_i = 0 \iff \exists g \in K[X]\ f(x) = g(x^p)$.

$K = \mathbb{F}_p(t) \rightsquigarrow X^p - t$ is irreducible (Eisenstein at $t \in \mathbb{F}_p[t]$ (prime)) and inseparable.

S2001 4. Let p be a prime number, $\mathbb{F}_p$ the prime field of p elements, X and Y algebraically independent variables over $\mathbb{F}_p$, $K = \mathbb{F}_p(X, Y)$, and $F = \mathbb{F}_p(X^p - X, Y^p - X)$ $= \mathbb{F}_p(X^p - X, Y^p)$

(a) Show that $[K : F] = p^2$ and the separability and inseparability degrees of K/F are both equal to p.

(b) Show that there exists a field E, such that $F \subseteq E \subseteq K$, which is a purely inseparable extension of F of degree p.

$E = F[t]/(t^p - Y^p) = \mathbb{F}_p(X^p - X, Y)$ is purely inseparable $/F$ of deg $= p$.

(a) $\underbrace{K / \mathbb{F}_p(X, Y^p)}_{\text{insep}} \underbrace{/ F}_{\text{sep}: t^p - t - X^p - X \overset{f'(t)}{\rightsquigarrow} -1}$ each of deg p. (so $\mathbb{F}_p(X, Y^p)$ is the separable closure of F)

F2003

F2000 2. Let k be a field of characteristic p and let t, u be algebraically independent over k. Prove the following:

a) $k(t, u)$ has degree p^2 over $k(t^p, u^p)$.

b) There exist infinitely many fields between $k(t, u)$ and $k(t^p, u^p)$.

a) $k(t, u^p) = k(t^p, u^p)[X]/(X^p - t^p)$, $k(t, u) = k(t, u^p)[Y]/(Y^p - u^p)$.

$\uparrow$ irred as above

$[k(t, u) : k(t, u^p)] \cdot [k(t, u^p) : k(t^p, u^p)] = p \cdot p = p^2$

b) Take $f(t^p) \in k(t^p)$ and consider $K_f := k(t^p, u^p)(f(t^p)u + t) \rightsquigarrow k(t^p, u^p) \subsetneq K_f \subsetneq k(t, u)$

We show that if $f \neq g$, then $K_f \neq K_g \subset k(t, u)$.

Suppose $K_f = K_g$ for $f \neq g$. Then $u = \dfrac{(f(t^p)u + t) - (g(t^p)u + t)}{f(t^p) - g(t^p)} \in K_f$, so $t = (f(t^p)u + t) - f(t^p) \cdot u \in K_f$.

$\rightsquigarrow k(t, u) = K_f$. Contradiction.

Galois group of a polynomial

$f \in K[X] \rightsquigarrow$ Galois group of f over K (write $G = \mathrm{Gal}_K(f)$ today) $:= \mathrm{Gal}(\underbrace{E/K}_{\text{normal}})$, E = min splitting field of f; if f: sep $\Rightarrow E/K$ Galois

$\sigma \in \mathrm{Gal}(E/K)$ permutes the roots $\{u_1, \dots, u_d\}$ ($d = \deg f$) since $\sigma(f(x)) = f(\sigma(x))$ [σ fixes (coef of f) $\in K$]

$u_1, \dots, u_d$ generates E/K

$\rightsquigarrow \mathrm{Gal}_K(f) \hookrightarrow S_d$.

If f: irred. sep. this is transitive

($\rightsquigarrow d \mid |G|$ by the orbit-stabilizer)

$g = \prod_{u_i \in (\text{orbit of } u_1)} (X - u_i)$ fixed by G

$\hookrightarrow$ orbit decomp of $G \curvearrowright \{u_1, \dots, u_d\} \Rightarrow$ factorization of f in K

char $K \neq 2$, f: sep of deg d $\in K[X]$,

$f = \prod (X - u_i)/_E \rightsquigarrow \Delta := \prod_{i<j} (u_i - u_j)$, $D := \Delta^2$: discriminant ($D = 0 \iff f$: inseparable)

$$\begin{array}{ccc} K(u_1, \dots, u_d) & & 1 \\ | & & | \\ K(\Delta) & & G \cap A_d \\ | & \begin{array}{c}2:1 \\ \text{or} \\ 1:1\end{array} & | \\ D \in K & & G \end{array}$$

property of Δ: $\rightsquigarrow D \in K$ always

For $\sigma \in G < S_d$: $\sigma \cdot \Delta = (\mathrm{sgn}\,\sigma) \cdot \Delta$

$\Delta \in K$ (i.e. G-invariant) $\iff G < A_d$

$D(T^n + aT + b) = (-1)^{\frac{n(n-1)}{2}} \left((1-n)^{n-1} a^n + n^n b^{n-1} \right)$

($\rightsquigarrow$ if $d = 3$ irred. (char $k \neq 2$) then $\mathrm{Gal}_k(f) = \begin{cases} A_3 & \text{if } \Delta \in k \\ S_3 & \text{if } \Delta \notin k \end{cases}$)

If f: irred$/_{\mathbb{Q}}$ with two nonreal roots $r_1, r_2 \rightsquigarrow \mathrm{Gal}_{\mathbb{Q}}(f) \ni$ transposition given by the cplx conj of $E \hookrightarrow \mathbb{C}$

$\hookrightarrow$ if moreover $\deg f = p$: prime, then $\exists$ order p elements $=$ p-cycle $\rightarrow$ generate S_p

Thm (Dedekind)

$f \in \mathbb{Z}[X]$ monic (deg $= d$), irreducible, $p \nmid D(f)$ (i.e. $f \bmod p$: sep),

$f \bmod p = f_1 f_2 \cdots f_k$ in $\mathbb{F}_p[X]$ with $d_i = \deg f_i$ ($d = d_1 + \cdots + d_k$)

$\rightsquigarrow \exists\, \sigma \in \mathrm{Gal}_{\mathbb{Q}}(f)$ ($\subset S_d$) s.t. the cycle type of $\sigma = (d_1, \dots, d_k)$

- For random polynomials ($\Leftarrow$ large Galois group) $\leftarrow$ find many elements, generate A_n or S_n

  fact (should be proved for each special cases)

  - $n \geq 2$. transitive subgroup of S_n that contains a transposition and a p-cycle for $\exists p > \frac{n}{2}$ is S_n.
  - $n \geq 3$ ——— " ——— a 3-cycle and a p-cycle for $\exists p > \frac{n}{2}$ is A_n or S_n.

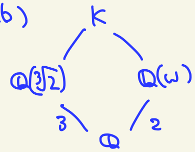
- For "organized" polynomials ($\Leftarrow$ small Galois group)
  write down the splitting field explicitly, break down into simple extensions and compute the degree, then write down an automorphism using generators, generate the group.

S2001 2. Let K be the splitting field of $f(X) = X^3 - 2$ over $\mathbb{Q}$.
(a) Determine an explicit set of generators for K over $\mathbb{Q}$.
(b) Show that the Galois group $G(K/\mathbb{Q})$ of K over $\mathbb{Q}$ is isomorphic to the symmetric group S_3.
(c) Provide the complete list of intermediate fields k, $\mathbb{Q} \subseteq k \subseteq K$, satisfying $[k:\mathbb{Q}] = 3$.
(d) Which of the fields determined in (c) are normal extensions of $\mathbb{Q}$?

(a) roots of $f(x)$ in $\mathbb{C}$: $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$ (ω: an order 3 element $\in \mathbb{C}^*$)

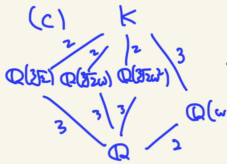
$\rightsquigarrow K \cong \mathbb{Q}(\sqrt[3]{2}, \omega)$

(b)



Since $\#\mathrm{Gal}(K/\mathbb{Q}) = [K:\mathbb{Q}]$ and $\mathrm{Gal}(K/\mathbb{Q}) < S_3$, it suffices to see $[K:\mathbb{Q}] = 6$.
now $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$ and $[\mathbb{Q}(\omega):\mathbb{Q}] = 2$ both divides $[K:\mathbb{Q}]$, so it must be 6.

(c)



S_3 permutes $\{\overset{1}{\sqrt[3]{2}}, \overset{2}{\sqrt[3]{2}\omega}, \overset{3}{\sqrt[3]{2}\omega^2}\}$, and by (b) any perm. can be realized as a field automorphism.

(23): $\sqrt[3]{2} \mapsto \sqrt[3]{2}$, $\omega \leftrightarrow \omega^2$ $\rightsquigarrow$ fixed subfield $\mathbb{Q}(\sqrt[3]{2})$

(12): $\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega \mapsto \sqrt[3]{2}$ ($\Leftrightarrow \omega \mapsto \omega^2$) $\rightsquigarrow$ fixed field $\mathbb{Q}(\sqrt[3]{2}\omega^2)$

(13): $\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2$, $\sqrt[3]{2}\omega^2 \mapsto \sqrt[3]{2}$ ($\Leftrightarrow \omega \mapsto \omega^2$) $\rightsquigarrow$ fixed field $\mathbb{Q}(\sqrt[3]{2}\omega)$

(d) None (all three are conjugate of each other)

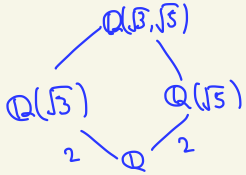
F2001 **4.** Let $K := \mathbb{Q}(\sqrt{3} + \sqrt{5})$.
(a) Show that K is the splitting field of $X^4 - 6X^2 + 4$.
(b) Find the structure of the Galois group of $K/\mathbb{Q}$.
(c) List all the fields k, satisfying $\mathbb{Q} \subseteq k \subseteq K$.

(a) $(\sqrt{3}+\sqrt{5})^2 = 8 + 2\sqrt{15} \rightsquigarrow \sqrt{15} \in K$, $\sqrt{15}\cdot(\sqrt{3}+\sqrt{5}) = 3\sqrt{5} + 5\sqrt{3} \rightsquigarrow \sqrt{5}, \sqrt{3} \in K$, so $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$.

$(X^2-3)^2 - 5 = 0 \iff X^2 - 3 = \pm\sqrt{5} \iff X = \pm\sqrt{3\pm\sqrt{5}} = \pm\frac{1}{\sqrt{2}}(1\pm\sqrt{5})$ ... ?

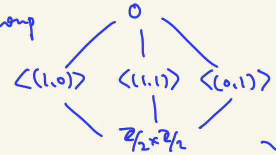
the splitting field is $K(\sqrt{2}, \sqrt{5})$

(b)

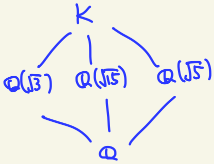


$\rightsquigarrow$ by the translation theorem $\mathbb{Z}/2 \times \mathbb{Z}/2$.

(c) subgroup



$\rightsquigarrow$

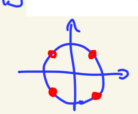


$\mathrm{Gal}(\mathbb{Q}(\sqrt{3},\sqrt{5})/\mathbb{Q}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$

$\sqrt{3} \leftrightarrow -\sqrt{3}$, $\sqrt{5}$ fixed; $\sqrt{5} \leftrightarrow -\sqrt{5}$, $\sqrt{3}$ fixed

$\rightsquigarrow (1,1)$: $\sqrt{15}$ fixed, $\sqrt{3} \mapsto -\sqrt{3}$, $\sqrt{5} \mapsto -\sqrt{5}$,

F2013 5. Compute the Galois group of $f(x) = x^4 + 1$ over $\mathbb{Q}$.

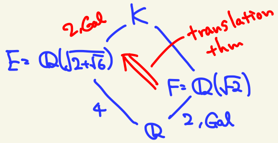


roots $\frac{\pm 1 \pm \sqrt{-1}}{\sqrt{2}}$. Splitting field $\mathbb{Q}(\sqrt{-1}, \sqrt{2}) \rightsquigarrow \mathrm{Gal}_{\mathbb{Q}}(f) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$.

F2016 4. (1). Determine the Galois group of x^4-4x^2-2 over $\mathbb{Q}$.

(2). Let G be a group of order 8 such that G is the Galois group of a polynomial of degree 4 over $\mathbb{Q}$. Show that G is isomorphic to the Galois group in part (1).

(1) roots are $\pm\sqrt{2\pm\sqrt{6}}$. Let $K=\mathbb{Q}(\sqrt{2+\sqrt6},\sqrt{2-\sqrt6})$, then $\sqrt{-2}=\sqrt{2+\sqrt6}\sqrt{2-\sqrt6}\in K$.



Since x^4-4x^2-2 is 2-Eisenstein, so irreducible. $[\underbrace{\mathbb{Q}(\sqrt{2+\sqrt6})}_{E}:\mathbb{Q}]=4$.

$F:=\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$ is Galois of degree 2, and $EF=K$, $E\cap F=\mathbb{Q}$.

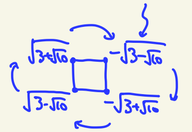
By translation thm $[K:E]=2$, Galois, so $[K:\mathbb{Q}]=8$. By (2) all subgroup of order 8 of S_4 is D_8, so $\mathrm{Gal}(K/\mathbb{Q})\cong D_8$.

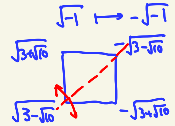
(2) G is a Sylow 2-subgroup of S_4. By Sylow's theorem, they are all conjugate to each other, so in particular isomorphic to D_8.

S2008 **3.** Let K be the splitting field of the polynomial X^4-6X^2-1 over $\mathbb{Q}$.
(a). Compute $\mathrm{Gal}(K/\mathbb{Q})$.
(b). Determine all intermediate fields that are Galois over $\mathbb{Q}$.

roots are $\pm\sqrt{3\pm\sqrt{10}}$, so $K=\mathbb{Q}(\sqrt{3+\sqrt{10}},\sqrt{3-\sqrt{10}})=\mathbb{Q}(\sqrt{3+\sqrt{10}},\sqrt{-1})$. By the same argument as above $\mathrm{Gal}(K/\mathbb{Q})\cong D_8$

Now define $\sigma:\sqrt{3+\sqrt{10}}\mapsto-\sqrt{3-\sqrt{10}}$, $\sqrt{-1}\mapsto-\sqrt{-1}$ $\qquad$ $\tau:\sqrt{3+\sqrt{10}}\mapsto-\sqrt{3+\sqrt{10}}$, $\sqrt{-1}\mapsto-\sqrt{-1}$





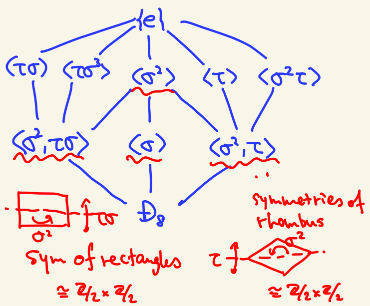
These hom are well-def by the universality of adjoining roots

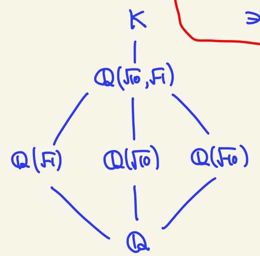
$$\begin{tikzcd} \mathbb{Q}[X,Y] \arrow[r] \arrow[d] & \mathbb{Q}[X,Y] \arrow[d] \\ \mathbb{Q}[X,Y]/(X^4-6X^2-1,Y^2+1) \arrow[r, dashed] & \mathbb{Q}[X,Y]/(X^4-6X^2-1,Y^2+1) \end{tikzcd}$$

$K\cong\left(\mathbb{Q}[X]/(X^4-6X^2-1)\right)[Y]/(Y^2+1)\cong\mathbb{Q}[X,Y]/(X^4-6X^2-1,Y^2+1)$

$\sqrt{3+\sqrt{10}},\sqrt{-1}\leftarrow\!\shortmid X,Y$

by the pictures $\langle\sigma,\tau\rangle\subset S_4$ satisfy the relations for D_8.





Only need to compute the fixed fields of normal subgroups (the ones with ~~)

σ^2 fixes $\sqrt{-1}$, $\sqrt{10}$, $\sqrt{-10}$ (spans 4 dim $/\mathbb{Q}$)

σ fixes $\sqrt{3+\sqrt{10}}\cdot(-\sqrt{3+\sqrt{10}})=-3-\sqrt{10}$

$\rightsquigarrow\sigma$ fixes $\sqrt{10}$.

$\tau\sigma$ fixes $\sqrt{-1}$, τ fixes $\sqrt{-10}$.

S2010 **3.** Compute Galois groups of the following polynomials.
(a). $x^3+t^2x-t^3$ over k, where $k=\mathbb{C}(t)$ is the field of rational functions in one variable over complex numbers $\mathbb{C}$.
(b). x^4-14x^2+9 over $\mathbb{Q}$. roots $\pm\sqrt2\pm\sqrt5$, Splitting field $\mathbb{Q}(\sqrt2,\sqrt5)$, $\mathrm{Gal}(f)\cong\mathbb{Z}/2\times\mathbb{Z}/2$

(a) Let $\underbrace{a_1,a_2,a_3}_{\in\mathbb{C}}$ be the roots of a^3-a-1. These are distinct because $(a^3-a-1,\underbrace{3a^2-1}_{\text{differential}})=1$

We have $x^3+t^2x-t^3=(x-a_1t)(x-a_2t)(x-a_3t)\in k[x]$, i.e. the polynomial already splits $/k$.

(because $a^3-a-1=0\Rightarrow(at)^3-t^2\cdot(at)-t^3=0$) $\qquad$ So $\mathrm{Gal}(x^3-t^2x-t^3)=\{e\}$.

S2013 6. Let K be the splitting field of x^6-5 over $\mathbb{Q}$.

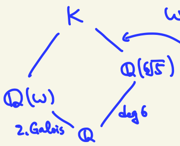
(a) Prove that x^6-5 is irreducible over $\mathbb{Q}$.

(b) Compute the Galois group of K over $\mathbb{Q}$.

(c) Describe an intermediate field F such that F is not $\mathbb{Q}$ or K and $F/\mathbb{Q}$ is Galois.

(a) $(x+5)^6-5$ is Eisenstein at 5, so irreducible.

(b) $K=\mathbb{Q}(\sqrt[6]{5},\zeta_6)$, $\zeta_6 = \omega+1$, $\omega^2+\omega+1=0$



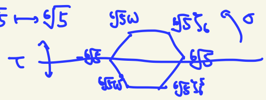
$\rightsquigarrow [K:\mathbb{Q}]=12$

Consider

$\sigma: \sqrt[6]{5} \mapsto \zeta_6\sqrt[6]{5}$, $\omega \mapsto \omega$

$\tau: \omega \mapsto \omega^2$ $(\Leftrightarrow \zeta_6 \mapsto \zeta_6^5)$

cpx conj $\sqrt[6]{5} \mapsto \sqrt[6]{5}$



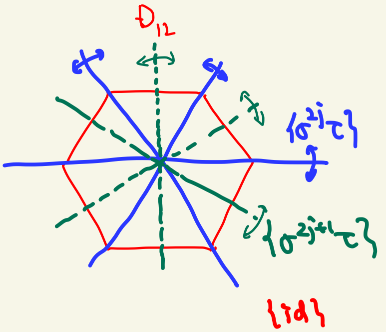
$\rightsquigarrow \mathrm{Gal}(K/\mathbb{Q}) = D_{12}$

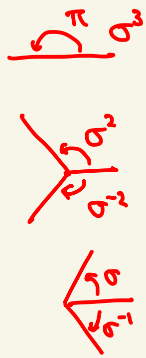
σ fixes ω

σ^2 fixes $\sqrt{5}$ $(\sqrt{5}=\sqrt[6]{5}^3 \mapsto (\omega\sqrt[6]{5})^3=\sqrt{5})$

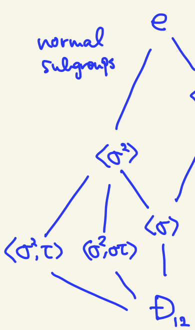
σ^3 fixes $\sqrt[3]{5}$

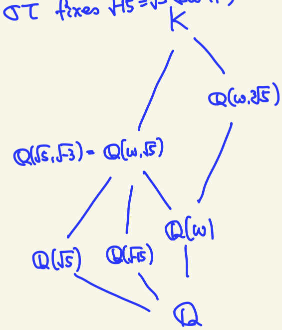
$\sigma\tau$ fixes $\sqrt{15}=\sqrt{5}(2\omega+1)$





normal subgroups



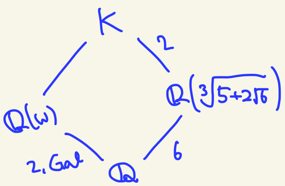


S2016 3. Determine the Galois group of x^6-10x^3+1 over $\mathbb{Q}$.

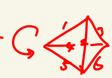
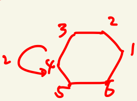
Irreducible: $(x-1)^6-10(x-1)^3+1 = x^6-6x^5+15x^4-30x^3+45x^2-36x+12$: Eisenstein at 3.

roots $\omega^i\sqrt[3]{5\pm2\sqrt{6}}$ $(i=0,1,2)$ $\rightsquigarrow$ splitting field $K=\mathbb{Q}(\sqrt[3]{5+2\sqrt{6}},\omega)$

$[K:\mathbb{Q}]=12$

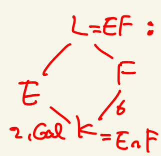


I know Galois gp must be D_{12}, so I only need to do the same thing as before.. $\sigma: \sqrt[3]{5+2\sqrt{6}} \mapsto \omega\sqrt{5-2\sqrt{6}}$ or something like this

fact: transitive subgroup $G<S_6$ of order 12 is either A_4  or D_{12} 

A_4 has no index 2 subgroup, so if

$L=EF$: splitting field of irr deg 6 poly $/K$



$\rightsquigarrow \mathrm{Gal}(L/K)$ must be D_{12}

F2010 **3.** Let $K = \mathbb{Q}(\sqrt[8]{2}, \sqrt{-1})$ and $F = \mathbb{Q}(\sqrt{-2})$. Show that K is Galois over F and determine the Galois group $\mathrm{Gal}(K/F)$.

$X^8 = 2$

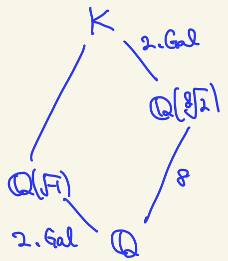
F2015 2. The dihedral group D_{2n} is the group on two generators r and s, with respective orders $o(r) = n$ and $o(s) = 2$, subject to the relation $rsr = s$.

(a) Calculate the order of D_{2n}.

primitive 8th root of 1

(b) Let K be the splitting field of the polynomial $x^8 - 2$. Determine whether the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is dihedral (i.e., isomorphic to D_{2n} for some n). $\leftarrow 2n$

$\mathbb{Q}(\sqrt[8]{2}, \zeta)$ $=$ $K = \mathbb{Q}(\sqrt[8]{2}, \sqrt{-1})$ is the splitting field of $X^8 - 2$. Since X^8-2 is Eisenstein at 2, it is irreducible.



$[K:\mathbb{Q}] = 16$, so if $\mathrm{Gal}(K/\mathbb{Q})$ is dihedral, it must be D_{16}.

Now we define (check well-def)

$\sigma: \sqrt[8]{2} \mapsto \zeta\sqrt[8]{2}$

$\quad \sqrt{-1} \mapsto \sqrt{-1} \quad (\Leftrightarrow \zeta \mapsto \zeta^5)$

$\tau: \sqrt[8]{2} \mapsto \sqrt[8]{2}$

$\quad \sqrt{-1} \mapsto -\sqrt{-1} \quad (\Leftrightarrow \zeta \mapsto \zeta^7)$

$\rightsquigarrow \sigma^8 = 1,\ \tau^2 = 1,\ \sigma\tau = \tau\sigma^3$ (generates distinct 16 elements)

$\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3 \rangle$ Now $(\tau\sigma^i)^2 = \sigma^{4i}$

$\rightsquigarrow \tau\sigma^{2j}$ has order 2

$\tau\sigma^{2j+1}$ has order 4

σ^{2j+1} has order 8

$\sigma^{2 \text{ or } 6}$ has order 4

σ^4 has order 2

id has order 1

$D_{16} = \langle \tau, \sigma \mid \tau^2 = \sigma^8 = 1, \sigma\tau = \tau\sigma^{-1} \rangle$

$\rightsquigarrow \tau\sigma^i$ has order 2

σ^{2j+1} has order 8

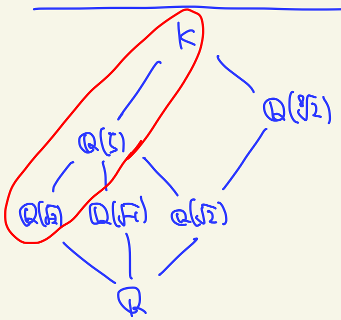
$\sigma^{2 \text{ or } 6}$ has order 4

σ^4 has order 2

id has order 1

#s of order 2 or 4 elements don't match.

$\mathrm{Gal}(K/\mathbb{Q}) \not\cong D_{16}$.



$K/\mathbb{Q}$ Galois

$\Rightarrow K/\mathbb{Q}(\sqrt{-2})$ Galois

$\sqrt{-2}$ is fixed by σ^2 and $\sigma\tau$,

these already generate group of order 8 ($\cong Q_8$ quaternion group)

$\rightsquigarrow \mathrm{Gal}(K/\mathbb{Q}(\sqrt{-2})) \cong Q_8$.

S2019

1. Show that any transitive subgroup of A_5 is isomorphic to one of the following groups: (a) the cyclic group $\mathbb{Z}/5\mathbb{Z}$, (b) the dihedral group D_5, (c) A_5.

2. Let $f(x) = x^5 - 5x + 12$. Verify that $f(x)$ is irreducible in $\mathbb{Q}[x]$ and its discriminant is $d(f) = (2^6 5^3)^2$. If $r_1, \ldots, r_5$ are the roots of f, let

$$P(x) = \prod_{1 \le i < j \le 5} (x - (r_i + r_j)).$$

Show that $P(x)$ is a product of two monic irreducible polynomials in $\mathbb{Q}[x]$:

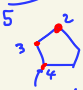
$$P(x) = (x^5 - 5x^3 - 10x^2 + 30x - 36)(x^5 + 5x^3 + 10x^2 + 10x + 4).$$

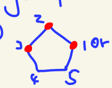
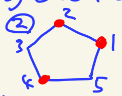
Use this information, Problem 1 and properties of $f_3 \in \mathbb{F}_3[x]$, the reduction of f modulo 3, to show that the the Galois group G_f of f is isomorphic to D_5.

1. $G < A_5 \curvearrowright \{1,2,3,4,5\}$ possible cycle type: id, (123), (12345), $(12)(34)$
transitive $\Rightarrow 5 \mid |G|$ by orbit-stabilizer thm. $\overset{\text{Cauchy}}{\Longrightarrow}$ $\exists$ element of order $5 = 5$ cycle $\in G$
May assume $\underset{x=}{(12345)} \in G$. ($\Rightarrow (13524), (14253), (15432) \in G$)

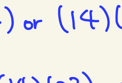
- If G contains a 5-cycle $y \notin \langle x \rangle$, then $x^{1-y(1)} \cdot y \neq id$ fixes 1, so G also contains an element of cycle type (123) or $(12)(34)$
- If G contains a 3-cycle $s = (s_1 s_2 s_3)$.

Considering $x^k s x^{-k} = ((s_1+k)\ (s_2+k)\ (s_3+k))$, we may assume that $\{s_1, s_2, s_3\} = \{1,2,3\}$ or $\{1,3,4\}$
mod 5



(because any triangle spanned by 3 vertices of a regular pentagon is, up to rotation, ①  or ② 

In the first case, $\langle s, xsx^{-1} \rangle$ acts transitively on $\{1,2,3,4\}$
In the second case, $\langle s, x^2 s x^{-2} \rangle$ —— " ——

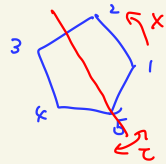


Therefore $|\langle s, x \rangle|$ must divide 4, as well as 3 and 5, so $\langle s, x \rangle = A_5$.

- If G contains an order 2 element $\tau = (ab)(cd)$
again by rotation we may assume $\{a,b,c,d\} = \{1,2,3,4\}$,
i.e. $\tau = (12)(34)$ or $(13)(24)$ or $(14)(23)$. Since $((12)(34)) \cdot x = (245)$, $((13)(24)) \cdot x^2 = (345)$, these generate A_5.

On the other hand, $(14)(23)$ and (12345) generates D_{10}.

2. $f(x-2) = (x-2)^5 - 5(x-2) + 12 = x^5 - 10x^4 + 40x^3 - 80x^2 + 75x - 20$ $+10$



is irreducible/$\mathbb{Q}$ by Eisenstein ($p = 5$)

We need to compute $d(f) = \prod_{i<j}(r_i - r_j)^2$

Note that

$$f'(x) = \sum_{cyc} (x-r_1)(x-r_2)(x-r_3)(x-r_4)$$

$$\rightsquigarrow f'(r_1)f'(r_2)f'(r_3)f'(r_4)f'(r_5) = \prod_{i\neq j}(r_i - r_j) \overset{(-1)^{10}=1}{=} d(f).$$

$$f'(x) = 5(x^4 - 1)$$

$$f(x) = x(x^4-1) - 4x + 12 \iff x^4 - 1 = \frac{f(x) + 4x - 12}{x}$$

So $d(f) = 5^5 \prod_{i=1}^{5}(r_i^4 - 1) = 5^5 4^5 \prod_{i=1}^{5}\left(1 \underbrace{- \frac{3}{r_i}}_{= -3t_i}\right)$. $t_i = \frac{1}{r_i}$ are the roots of $12x^5 - 5x^4 + 1$

$\rightsquigarrow t_1 + \cdots + t_5 = \frac{5}{12}$

$t_1 t_2 \cdots t_5 = -\frac{1}{12}$

0 for other degrees

$$= 5^5 4^5 \left(1 - 3\cdot\frac{5}{12} + 3^5 \cdot \frac{1}{12}\right)_{=20}$$

$$= 5^6 4^6.$$

Since this is a perfect square, $\mathrm{Gal}_{\mathbb{Q}}(f) \subset A_5$.

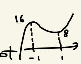
$x^4 + 1 = \underbrace{x^4 + 1 - 2x^2}_{(x^2-1)^2} - x^2$

Now consider the mod-3 reduction $f_3 = x^5 - 2x = x(x^4+1) = x(x^2 - x - 1)(x^2 + x - 1)$

irreducible

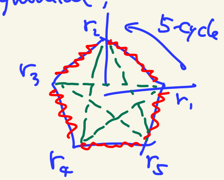
$3 \nmid d(f) \rightsquigarrow$ separable/$\mathbb{F}_3$ $\exists$ element of cycle type $(12)(34)$,

also follows from that $\exists$ only one real root



so $\mathrm{Gal}_{\mathbb{Q}}(f)$ is either D_{10} or A_5 by Problem 1.

If $P(x)$ admits degree 5 factors as in the problem, there cannot be a 3-cycle in the Galois group, since the orbit of (123) acting on $\{r_i + r_j \mid 1 \le i < j \le 5\}$ are $\{r_1+r_2, r_2+r_3, r_3+r_1\}$, $\{r_1+r_4, r_2+r_4, r_3+r_4\}$, $\{r_1+r_5, r_2+r_5, r_3+r_4\}$, $\{r_4+r_5\}$, and elements in the same orbit must have the same minimal polynomial, but there is no way to distribute $3+3+3+1$ into $5+5$.



So it remains to prove $P(x) = \prod_{cyc}(x - (r_1 + r_2)) \cdot \prod_{cyc}(x - (r_1 + r_3))$

both in $\mathbb{Q}[x]$.

- $P(2x) = \prod_{i<j}((x - r_i) + (x - r_j))$ is a symmetric polynomial in $(x - r_i)$.
- Can compute fundamental symmetric polynomials from $f'(x), f''(x), f'''(x), f''''(x)$.

$\rightsquigarrow$ can be done in principle. I've heard of a way to do this more efficiently but I can't remember

F2019 Question 6. Determine the Galois group over $\mathbb{Q}$ of the polynomial

$$f(x) = X^6 + 22X^5 - 9X^4 + 12X^3 - 37X^2 - 29X - 15.$$

$d(f)$
$13 \times 1231 \times 5892691967359$

We prove that $\mathrm{Gal}_{\mathbb{Q}}(f) = S_6$.

mod 2 $f(X) = X^6 + X^4 + X^2 + X + 1$ irreducible ($\Rightarrow f(x)$: irred$/\mathbb{Q}$) $\rightsquigarrow \exists$ 6-cycle $X \in G$

$f'(X) = 1 \rightsquigarrow$ separable

$X, X+1, X^2+1, X^2+X+1$, $X^3+1, X^3+X+1, X^3+X^2+1, X^3+X^2+X+1$ does not divide f

mod 3 $f(X) = X(X^5 + X^4 + 2X + 1)$: irred (no linear factor, no factor of the form $(X^2 + aX \pm 1)$ $\rightsquigarrow \exists$ 5-cycle $Y \in G$

$a \in \{0, \pm 1\}$

mod 5 $f(x) = X^6 + 2X^5 + X^4 + 2X^3 - 2X^2 + X \rightsquigarrow \exists$ 2-cycle $Z \in G$

$= X(X+1)(X+2)(X+4)(X^2+2)$

($\rightsquigarrow$ separable)

We may assume that $Y = (1\,2\,3\,4\,5)$.

Replacing Z by $X^k Z X^{-k}$ if necessary, we may also assume that Z does not involve 6.

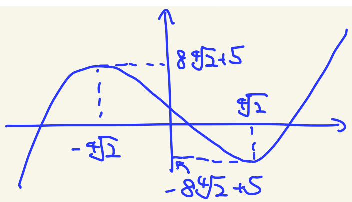
Then since any p-cycle and a 2-cycle generates S_p if p : prime.

$\langle Y, Z \rangle = S_5$ acting on $\{1, 2, 3, 4, 5\}$.

Now we see $G \supset \langle X, Y, Z \rangle = S_6$ because for any $\sigma \in S_6$, $\exists k$ $X^k \cdot \sigma(6) = 6$, so $X^k \cdot \sigma \in \langle Y, Z \rangle$, i.e. $\sigma \in \langle X, Y, Z \rangle$. $\boxtimes$

F2017 (4) Compute the Galois group of $x^5 - 10x + 5$ over $\mathbb{Q}$.

graph



irred$/\mathbb{Q}$ (Eisenstein $p=5$), 3 real roots

$\rightsquigarrow S_5$

F2004 **3.** Let $f(x) = x^5 - 9x + 3$. Determine the Galois group of f over $\mathbb{Q}$. 3-Eisenstein, 3 real roots

F2006 **2.** Let f be a polynomial in $\mathbb{Q}[x]$. Let E be a splitting field of f over $\mathbb{Q}$. For the following cases, determine whether E is solvable by radicals.

Yes (1). $f(x) = x^4 - 4x + 2$. Any subgp of S_4 is solvable

No (2). $f(x) = x^5 - 4x + 2$. $\mathrm{Gal} = S_5$ (irred mod 3, 3 real roots) : not solvable

S2011 3. Determine the Galois group [up to isomorphism] of the splitting field of each of the following polynomials over $\mathbb{Q}$:

(a) $f(x) = x^4 - 9x^3 + 9x + 4$,

(b) $g(x) = x^5 - 6x^2 + 2$. 2-Eisenstein, 3 real roots $\rightsquigarrow S_5$

(a) S_4. mod 2 $\rightsquigarrow X(X^3 + X^2 + 1)$ separable $\rightsquigarrow \exists$ 3-cycle

mod 3 $\rightsquigarrow (X^2 + X + 2)(X^2 + 2X + 2)$ $\rightsquigarrow \exists (12)(34)$ type

mod 5 $\rightsquigarrow (X+1)(X+4)(X^2 + X + 1)$ $\rightsquigarrow \exists$ 2-cycle

(mod 13 $\rightsquigarrow$ irred, $\exists$ 4-cycle)

$\exists$ 3-cycle + transitive

$\Rightarrow$ at least 12 elements,

Contains a 2-cycle $\Rightarrow$ not A_4, so $\underline{S_4}$

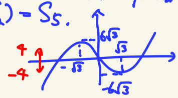
F2014

1. (a) Let S_n be the symmetric group (permutation group) on n objects. Prove that if $\sigma \in S_n$ is an n-cycle and $\tau \in S_n$ is a transposition (i.e., a 2-cycle), then σ and τ generate S_n.

(b) Let $f_a(x)$ be the polynomial $x^5 - 5x^3 + a$. Determine an integer a with $-4 \le a \le 4$ for which f_a is irreducible over $\mathbb{Q}$, and the Galois group of [the splitting field of] f_a over $\mathbb{Q}$ is S_5. Then explain why the equation $f_a(x) = 0$ is not solvable in radicals.

(a) Suppose $\tau = (a\ b)$. $\exists k$ s.t. $\sigma^k(a) = b$, so relabeling if necessary we may assume $\tau = (1\,2)$, $\sigma = (1\,2 \cdots n)$. Now $\sigma^i \tau \sigma^{-i} = (1+i\ \ 2+i)$ for $i \le n-2$, so any $(i\ \ i+1) \in \langle \tau, \sigma \rangle$, and these generate S_n.

(b) By drawing the graph of $x^5 - 5x^3$, we see that $x^5 - 5x^3 + a$ admits three real roots (without multiplicity) so as soon as $f_a(x)$ is irreducible separable, it has two imaginary roots and $\mathrm{Gal}_{\mathbb{Q}}(f_a) = S_5$.



- $x^5 - 5x^3 \pm 4$ have a root $\pm 1 \in \mathbb{Q}$
- $x^5 - 5x^3 + 0$ have a root $0 \in \mathbb{Q}$
- $x^5 + x^3 + 1$: irred $\in \mathbb{F}_2[x]$ (check!), so $x^5 - 5x^3 - a$ for $a = -3, -1, 1, 3$ are irred.
- $(x \pm 2)^5 - 5(x \pm 2) \mp 2$ is 5-Eisenstein, so $x^5 - 5x^3 \pm 2$ are irreducible.

Separability: $f_a'(x) = 5x^4 - 15x^2 = 5x^2(x^2 - 3)$. By the graph, f_a for $|a| \le 4$ cannot have a root $\pm\sqrt{3}$

$f_a(0) = 0$ only for $a = 0$, which is already eliminated.

So f_a for $a = -3, -2, -1, 1, 2, 3$ are the irreducibles with $\mathrm{Gal}(f_a) = S_5$.

$f_a = 0$ is not solvable by radicals for these a's because S_5 is not solvable (contains simple subgp A_5).

F2009

3. Determine the Galois group of $\overset{f(x)}{x^4 - 4x^2 + 7x - 3}$ over $\mathbb{Q}$.

mod 2 $\quad x^4 + x + 1$ separable & irreducible $/\mathbb{F}_2$ ($\Rightarrow f(x)$ irred $/\mathbb{Q}$).

$\rightsquigarrow \mathrm{Gal}_{\mathbb{Q}}(f)$ have a 4-cycle in it.

mod 3 $\quad x^4 + 2x^2 + x = x\underbrace{(x^3 + 2x + 1)}_{\text{irred, separable}} \rightsquigarrow \mathrm{Gal}_{\mathbb{Q}}(f) \ni \exists$ 3-cycle.

So $\mathrm{Gal}_{\mathbb{Q}}(f) \cong S_4$

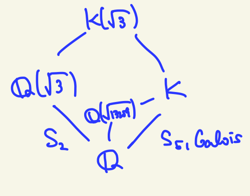
So the order of $\mathrm{Gal}(f)$ has to divide 12 but it cannot be A_4 because A_4 doesn't contain a 4-cycle.

S2012 3. In this problem, G denotes the group $S_5 \times C_2$, where S_5 is the symmetric group on five letters and C_2 is the cyclic group of order 2.

(a) Determine all normal subgroups of G.

(b) Give an example of a polynomial with rational coefficients whose Galois group is G, deducing that from basic principles.

(b) Let $f(x) = x^5 - 4x - 2$ (Eisenstein at 2, has 3 real roots) and K be the splitting field.



discriminant $\Delta = 256 \cdot (-4)^5 + 3125 \cdot (-2)^4 = 2^4 \cdot 13259$

Since the only quadratic extension of $\mathbb{Q}$ contained in K is $\mathbb{Q}(\sqrt{\Delta})$ (fixed field of A_5),

We see $\sqrt{3} \notin K$, so $\mathbb{Q}(\sqrt{3}) \cap K = \mathbb{Q}$.

Now by translation theorem, $Gal(K(\sqrt{3})/\mathbb{Q}) \cong S_2 \times S_5$,

This is the splitting field of $(x^5 - 4x - 2)(x^2 - 3)$.

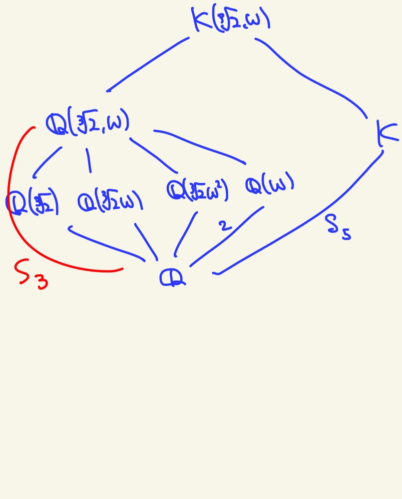
F2015 4. Let $H = S_3 \times S_5$.

(a) Determine all normal subgroups of H. *Make sure you have them all!* What would be different if H were replaced by $S_2 \times S_5$?

(b) Describe, <u>in full detail</u>, the construction of a polynomial with rational coefficients, whose Galois group is isomorphic to H.

(b) We consider the splitting field K of $x^5 - 4x - 2$ again.

$H < S_5$, $|H| = 40$
$\rightsquigarrow$ contains Sylow 5 & Sylow 2
$\rightsquigarrow$ contains 5-cycle & transposition
$\rightsquigarrow$ generate S_5. contradiction



- Since $\mathbb{Q}(\omega) \neq \mathbb{Q}(\sqrt{13259})$, $\mathbb{Q}(\omega) \not\subset K$.
- Since S_5 does not contain index 3 subgroup, $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}\omega), \mathbb{Q}(\sqrt[3]{2}\omega^2) \not\subset K$

So $\mathbb{Q}(\sqrt[3]{2}, \omega) \cap K = \mathbb{Q}$ and by translation theorem

$Gal(K(\sqrt[3]{2}, \omega)/\mathbb{Q}) \cong S_5 \times S_3$, which is the Galois group of $(x^3 - 2)(x^5 - 4x - 2)$

Field theory random problems

S2016

2. Let $F \subset K$ be an algebraic extension of fields. Let $F \subset R \subset K$ where R is a F-subspace of K with the property such that $\forall a \in R$, $a^k \in R$ for all $k \geq 2$.

   (1). Assume that $char(F) \neq 2$. Show that R is a subfield of K.

   (2). Give an example such that R may not be a field if $char(F) = 2$.

(1) Take $x, y \in R$. $xy = \frac{1}{2}((x+y)^2 - x^2 - y^2) \in R$.

Since K/F algebraic. $\exists$minimal polynomial $x^n + a_1 x^{n-1} + \cdots + \underset{\neq 0}{a_n} = 0$ so $\underbrace{-\frac{1}{a_n}(x^{n-1} + \cdots + a_{n-1})}_{\in R} \cdot x = 1$

(2) $F = \mathbb{F}_2(X^2, Y^2) \subset \underbrace{\mathrm{Span}_F(1, X, Y)}_{= R} \subset \mathbb{F}_2(X, Y) = K$.

$[K:F] = 4$, $\dim_F R = 3$, so R cannot be an intermediate field.

R is closed under taking powers: Let $a + bX + cY \in R$, $a, b, c \in F$.

Then $(a + bX + cY)^n = \sum_{i+j+k=n} \binom{n}{i,j,k} a^i (bX)^j (cY)^k$ each term belongs to $\begin{cases} F & \text{if } (j,k) \equiv (0,0) \bmod 2 \\ F \cdot X & \text{if } \equiv (1,0) \\ F \cdot Y & \text{if } \equiv (0,1) \\ F \cdot XY & \text{if } \equiv (1,1) \end{cases}$

So it suffices to prove $2 \mid \binom{n}{i,j,k}$ if j, k : odd.

$\binom{n}{i,j,k}$ can be divided $\left(\sum_{l=1}^{\infty} \left\lfloor \frac{n}{2^l} \right\rfloor - \left\lfloor \frac{i}{2^l} \right\rfloor - \left\lfloor \frac{j}{2^l} \right\rfloor - \left\lfloor \frac{k}{2^l} \right\rfloor \right)$ times by 2

This is nonzero because $\left\lfloor \frac{n}{2} \right\rfloor - \left\lfloor \frac{i}{2} \right\rfloor - \left\lfloor \frac{j}{2} \right\rfloor - \left\lfloor \frac{k}{2} \right\rfloor \geq \left\lfloor \frac{\overset{= j+k}{n-i}}{2} \right\rfloor - \left\lfloor \frac{j}{2} \right\rfloor - \left\lfloor \frac{k}{2} \right\rfloor \underset{\substack{\uparrow \\ j,k \text{ odd},\ j+k \text{ even}.}}{=} 1$

S2013

4. Prove that the group of automorphisms $\underset{\ni f}{\mathrm{Aut}_{\mathbb{Q}}(\mathbb{R})}$ of the field $\mathbb{R}$ that fix $\mathbb{Q}$ pointwise is trivial (Hint: Prove that every such automorphism is continuous).

$x_1 \geq x_2 \Rightarrow \exists y \in \mathbb{R} \quad y^2 = x_1 - x_2 \Rightarrow \exists y \in \mathbb{R} \quad f(y)^2 = f(x_1) - f(x_2) \Rightarrow f(x_1) \geq f(x_2)$.

Therefore f is monotonous.

$$\begin{tikzcd} \mathbb{Q} \arrow[r, hook] \arrow[d] & \mathbb{R} \\ \mathbb{R} \arrow[ur, dashed, "\exists! \text{ monotonous extension}"'] & \end{tikzcd} \quad = \mathrm{id}_{\mathbb{R}}$$

F2018 Question 5. Let t be transcendental over $\mathbb{Q}$. Set $K = \mathbb{Q}(t)$, $K_1 = \mathbb{Q}(t^2)$ and $K_2 = \mathbb{Q}(t^2 - t)$.
Show that K is algebraic over K_1 and over K_2 and that K is not algebraic over $K_1 \cap K_2$.

$$\begin{tikzcd} & \mathbb{Q}(t) = K \arrow[dl, dash] \arrow[dr, dash] & \\ K_1 = \mathbb{Q}(t^2) \arrow[dr, dash] & & \mathbb{Q}(t^2 - t) = K_2 \arrow[dl, dash] \\ & K_1 \cap K_2 \arrow[d, dash] & \\ & \mathbb{Q} & \end{tikzcd}$$

t : algebraic$/K_1, K_2$ because it is a root of $(T^2 - t^2) \in K_1[T]$, $(T^2 - T - (t^2 - t)) \in K_2[T]$.

Consider $\varphi_1, \varphi_2 \in \mathrm{Aut}_{\mathbb{Q}}(K)$ defined by

$\varphi_1(t) = -t$, $\varphi_2(t) = 1 - t$

These satisfy $\varphi_1^2 = \varphi_2^2 = \mathrm{id}$, $K_1 \subset K^{\varphi_1}$ ← fixed pt, $K_2 \subset K^{\varphi_2}$.

$\rightsquigarrow K_1 \cap K_2 \subset K^{\langle \varphi_1, \varphi_2 \rangle}$

Now note that $\varphi_1 \circ \varphi_2 : t \mapsto t + 1$.

For any rational fcn $f(t) \in \mathbb{Q}(t)^{\times}$, either $\lim_{t \to \infty} f(t)$ or $\lim_{t \to \infty} \frac{1}{f(t)}$ exists,

So 1-periodicity implies that $f(t)$ is constant. so $K_1 \cap K_2 = \mathbb{Q}$.

$K/\mathbb{Q}$ is transcendental.

S2006

4. Let k be a field. Let p be a prime number. Let $a \in k$. Show that the polynomial $\overset{f(x)=}{x^p - a}$ either has a root in k or is irreducible in $k[x]$.

Take a splitting field E of $x^p - a$. $x^p - a = (x - r_1) \cdots (x - r_p)$ in $E[x]$.

If f is reducible $/k$, then $x^p - a = g(x) h(x)$ we may assume $g(x) = (x - r_1) \cdots (x - r_k)$ $k < p$

$r = r_1 \cdots r_k \in k$, $r_i^p = a$ $\rightsquigarrow r^p = a^k$. $\exists l.\ kl \equiv 1\ (p) \rightsquigarrow \left(r^l \cdot a^{-\frac{kl-1}{p}} \right)^p = a$.

Problems not included in the notes (for my time reason)

edit: I solved some.

F2005

1. Let K be a finite field with q elements. Let $n > 0$ be a positive integer. Compute the sum

$$\sum_{x \in K} x^n.$$

2. Let K be the splitting field (in $\mathbb{C}$) of the polynomial $x^4 - 3x^2 + 5$ over $\mathbb{Q}$.
(1). Determine $\mathrm{Gal}(K/\mathbb{Q})$. dihedral of order 8
(2). Find all intermediate fields $\mathbb{Q} \subset E \subset K$ such that E is Galois over $\mathbb{Q}$.

3. Let $k \subset E$ be an algebraic extension of fields of characteristic zero. Assume that every non-constant polynomial $f(x) \in k[x]$ has a root in E. Show that E is algebraically closed.

Let $g(x) \in E[x]$ nonconst.
Let $L = (K \text{ adjoined with all coeffs of } g(x))$
E/k alg $\Rightarrow$ L/k $\overset{\text{fin}}{\text{alg}}$, $g(x) \in L[x]$
$[L[x]/(g(x)) : k] = \deg g \cdot [L:k] < \infty$
$\overset{\parallel}{F} \rightsquigarrow \underset{\text{char } 0}{F/k} : \text{fin sep ext.} \underset{\text{simple ext thm}}{\Rightarrow} F \cong k[y]/(f(y))$.
by assumption $L[x]/(g(x)) \xrightarrow{\cong} k[y]/(f(y)) \xrightarrow{\exists} E$
$x \longmapsto$ root of $g(x)$

4. Let R be a commutative ring. Let I be a finitely generated ideal. Assume that $I^2 = I$. Show that I is a direct summand of R.

S2005

2. Let $\mathbb{F}_p$ be the field with p elements, where p is a prime number. Let $f_{n,p}(x) = x^{p^n} - x + 1$, and suppose that $f_{n,p}(x)$ is irreducible in $\mathbb{F}_p[x]$. Let α be a root of $f_{n,p}(x)$.
(a) Show that $\mathbb{F}_{p^n} \subset \mathbb{F}_p(\alpha)$ and $[\mathbb{F}_p(\alpha) : \mathbb{F}_{p^n}] = p$.
(b) Determine all pairs (n, p) for which $f_{n,p}(x)$ is irreducible.

3. Let ξ be a primitive p^n-th root of unity. Here p is prime and $n > 0$. Let $f(x)$ be the minimal polynomial of ξ over $\mathbb{Q}$, and let m be its degree.
(a) Determine $f(x)$.
(b) Let $\alpha_1, \ldots, \alpha_m$ be all the roots of $f(x)$. Define the *discriminant* of ξ as:

$$D(\xi) = [\det(\alpha_i^{j-1})_{ij}]^2, \quad i, j = 1, \ldots m.$$

Show that $D(\xi) = (-1)^{\frac{m(m-1)}{2}} N_{\mathbb{Q}}^{\mathbb{Q}(\xi)}(f'(\xi))$.
(c) Take $n = 2$. Compute $D(\xi)$ in this case.

S2004

2. Let $K \subset \mathbb{C}$ be the splitting field of $f(x) = x^6 + 3$ over $\mathbb{Q}$. Let α be a root of $f(x)$ in K.
(a) Show that $K = \mathbb{Q}(\alpha)$.
(b) Determine the Galois group $\mathrm{Gal}(K/\mathbb{Q})$. C_6 ($\subset S_6$, deg 6 ext, transitive)

S2004

4. Let k be a field. Consider the integral domain $R = k[x, y]/(x^2 - y^2 + y^3)$.
(a) Show that R is not a unique factorization domain.
(b) Let F be the field of fractions of R. Find $t \in F$ such that $F = k(t)$.
(c) Determine the integral closure of R in F.

F2000

2. (a) Let p be a prime number. Show that $f(X) = X^p - pX - 1$ is irreducible in $\mathbb{Q}[X]$. (Hint: use Eisenstein's criterion of irreducibility for the image of $f(X)$ via a ring automorphism of $\mathbb{Q}[X]$.)
(b) Let R be the ring $\mathbb{Z}[X]/(X^4 - 3X^2 - X)$, where $(X^4 - 3X^2 - X)$ is the ideal generated by $X^4 - 3X^2 - X$ in $\mathbb{Z}[X]$. Find all the prime ideals of R containing $\hat{3}$ (the image of $3 \in \mathbb{Z}[X]$ via the canonical surjection $\mathbb{Z}[X] \longrightarrow R$.)

$$f(X+1) = (X+1)^p - pX - 1 = X^p + pX^{p-1} + \dots + \binom{p}{2}X^2$$

$\rightsquigarrow$ Eisenstein mod p

Let $3 \in \mathfrak{p} \in R$ prime.
$R/\mathfrak{p}$ is a quotient of $R/(3)$ which is int dom.

$$R/(3) \cong \mathbb{F}_3[X]/(X^4 - X) = \mathbb{F}_3[X]/X(X-1)^3$$

$$\xrightarrow[(\text{mod } X,\, \text{mod } (X-1)^3)]{\text{CRT}\ \cong} \mathbb{F}_3 \times \frac{\mathbb{F}_3[X]}{(X-1)^3} \twoheadrightarrow R/\mathfrak{p} \leftarrow \text{reduced}$$

$\frac{\mathbb{F}_3[X]}{(X-1)^3} \xrightarrow{\text{mod}(X-1)} \mathbb{F}_3 \times \mathbb{F}_3 \to R/\mathfrak{p}$ factors through reduction

mod $(1,0)$ or $(0,1)$

ideal

mod $((1,0),(0,X-1))$ or mod $(0,1)$

CRT

mod $(1-X^3, X-X^3)$ $= (X^3-1, X-1) = (X-1)$; (X^3)

$\rightsquigarrow \mathfrak{p} = (3, X-1)$ or $(3, X^3)$

3. Let K/k be a finite, separable field extension of degree n. Let

$$\rho, \quad \rho' : K \longrightarrow M_n(k)$$

be two morphisms of k–algebras, where $M_n(k)$ is the ring of $n \times n$ matrices with entries in k. Show that there exists an invertible matrix A in $M_n(k)$ such that

$$\rho'(x) = A \cdot \rho(x) \cdot A^{-1}, \text{ for all } x \in K.$$

F2019

1. Let $\mathbb{F}_q$ be a field with $q \neq 9$ elements and a be a generator of the cyclic group $\mathbb{F}_q^*$. Show that $\mathrm{SL}_2(\mathbb{F}_q)$ is generated by

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}.$$

at least this shows that it can't be formal

This is a bad problem (hard)

"Dickson's theorem"