A08Q4

$R = M_2(\mathbb{Q})$

(a) Show all $A \in R$, $A \neq I$, that satisfy $A^3 = I$ are similar.

$A^3 = I \Rightarrow A^3 - I = 0 \Rightarrow A$ satisfies

$x^3 - 1 = (x-1)(x^2+x+1)$

$\uparrow$ $A \neq I$ $\quad$ irr over $\mathbb{Q}$

so $c_A(x) = x^2 + x + 1 = m_A(x)$.

so $A \sim \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \in$ RCF via $B \in M_2(\mathbb{Q})$

(b) Let $n \in \mathbb{Z}^+$ odd. Show $\nexists A \in R$ st $A \neq I$, $A^n = I$ & 1 is an eigenval of A.

Sup so. Then $x^n - 1 \leftarrow$ n^{th} roots of unity

$(x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$

1 eigen value so $x-1 \mid c_A(x)$. $A \neq I$ so other eigen value must be a root of

n odd, n-1 even, so ± 1 not a root. no linear term. So other eigenvalue $\notin \mathbb{R}$.

So $c_A(x) = (x-1)(x-\alpha) = x^2 - (1+\alpha)x + \alpha$

$A \approx \begin{pmatrix} 0 & -\alpha \\ 1 & 1+\alpha \end{pmatrix}$

$\alpha \notin \mathbb{Q}$ but $\uparrow \in R$, so $-\alpha \in \mathbb{Q}$ $\Rightarrow \alpha \in \mathbb{Q} \rightarrow \leftarrow$

$\boxed{A08Q1}$

$$|G| = 2^3 \cdot 5 \cdot 13 \qquad \begin{array}{r} 40 \\ \times\ 13 \\ \hline 120 \\ 400 \\ \hline 520 \end{array}$$

$n_2 \in \{1, 5, 13\}$ $\quad n_5 \in \{1, \cancel{13}, \cancel{2}, \cancel{4}, \cancel{8}, 26, \cancel{52}, \cancel{104}\}$

$n_{13} \in \{1, \cancel{5}, \cancel{2}, \cancel{4}, \cancel{8}, \cancel{10}, \cancel{20}, 40\}$

$$\left.\begin{array}{l} 26 \cdot 4 = 104 \\ 40 \cdot 12 = 480 \end{array}\right\rangle \ 584 \quad \text{too many elements}$$

$\boxed{A08Q3}$

Let p be a prime number in the ring of integers $\mathbb{Z}$. Let A be the set $\{\frac{a}{b} \in \mathbb{Q} : a,b \in \mathbb{Z},\ p \nmid b\}$ where $\mathbb{Q}$ is the field of rational numbers.

(a) Show that A is a subring of $\mathbb{Q}$ & is an integral domain.

$0,1 \in \mathbb{Z}$, $p \nmid 1$, $\frac{0}{1} = 0 \in A$, nonempty

Let $x,y \in A$. $x = \frac{a}{b}$ $y = \frac{a'}{b'}$

$x+y = \frac{ab' + a'b}{bb'} \in A$ $\begin{matrix} p \nmid b \\ p \nmid b' \end{matrix} \Rightarrow p \nmid bb'$

$\frac{a}{b} \in A$ then $\frac{-a}{b} \in A$ since $-a \in \mathbb{Z}$ so $\frac{a}{b} + (\frac{-a}{b}) = 0$ and $\frac{-a}{b} \in A$

$xy = \frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'} \in A$

Subring so ring, comm inherited $\frac{1}{1} \in A$

$\mathbb{Q}$ has no zero divisors (a field) so neither does A. Integral dom ✓

b) Show that for every nonzero $\alpha \in A$, there is a unique unit $u \in A$ and a unique non-neg int e st $\alpha = up^e$.

Let $\alpha \in A$. Then $\alpha = \frac{a}{b}$ $a, b \in \mathbb{Z}$ $p \nmid b$.

$\alpha = \frac{1}{b} \cdot a$ $\mathbb{Z}$ is a UFD

$\Rightarrow a = p^e \, p_1^{e_1} \cdots p_k^{e_k}$

$p \nmid p_i$ so p_i is a unit w/ inverse $\frac{1}{p_i}$

$$\alpha = \underbrace{\left(\frac{1}{b} p_1^{e_1} \cdots p_k^{e_k}\right)}_{\text{unit}} p^e$$

unit w/ inverse $\frac{b}{p_1^{e_1} \cdots p_k^{e_k}} \in A$

(c) Show that A is a Euclidean domain.

A08 Q4

Let $R = M_2(\mathbb{Q})$

a) Show that all $A \in R$, $A \neq I$, that satisfy $A^3 = I$, are similar (via a matrix in R) to each other.

Let $A \in R$ st $A^3 = I$. Then A satisfies the polynomial $x^3 - 1 = (x-1)(x^2+x+1)$. However $A \neq I$ so A does not satisfy $x-1$. Since we don't have zero divizors, A must satisfy x^2+x+1. This polynomial is irreducible since it is degree 2 and the only possible roots by rational roots thm are ± 1 but $1^2+1+1 = 3 \neq 0$ and $(-1)^2 - 1 + 1 = 1 \neq 0$. So x^2+x+1 is the min & char polynomial with RCF $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$. So A is similar via a matrix $B \in R$ to $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$. That is $BAB^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$. Since this holds for all such A, we have any such matrix is sim to the other via a matrix in R. E.g.

$$BAB^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = CA'C^{-1}$$

$$\Rightarrow (C^{-1}B)A(B^{-1}C) = A' \qquad B, C \in R$$

$$\Rightarrow (C^{-1}B)A(C^{-1}B)^{-1} = A' \qquad \text{so } C^{-1}B \in R$$

(R field).

b) Let n be an odd positive integer. Show that there is no $A \in \mathbb{R}$ for which $A \neq I$, $A^n = I$, and 1 is an eigenvalue.

Sup $A \neq I$, $A^n = I$, and 1 is an eigenvalue of A.
Note since $A \in \mathbb{R}$, A has 2 eigenvalues.
The other cannot also be 1 since $A \neq I$.
So let α denote the other. Then the char poly is $\chi_A(x) = (x-1)(x-\alpha) = m_A(x)$

$$= \underline{x^2 - (\alpha+1)x + \alpha}.$$

since $A^n = I$ we have A satisfies $x^n - 1$

$\Rightarrow (x-1)(\underbrace{x^{n-1} + x^{n-2} + \dots + x + 1}_{\text{even degree}})$

$m_A(x) \mid \underline{x^{n-1} + x^{n-2} + \dots + x + 1}$

so $\alpha = \pm 1$.

by rational roots

$\alpha \neq 1$ so $\alpha = -1$ so $\cancel{A} \simeq \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ (JCF)

but $A^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$

this contradicts $A^n = I$ f.s. odd n

by rational roots the only linear factors of $x^{n-1} + \dots + x + 1$ can be ± 1. Can't be 1. If -1 then

$\boxed{A08Q5}$ Let k be a field, and $f \in k[x]$ an irreducible poly. Let α be a root of f in a splitting field of f over k. Sup. that $\alpha+1$ is also a root of f.

(a) Show that k has char p for pos. prime p.

$$f(\alpha) = f(\alpha+1) = 0 \qquad f \text{ deg } n$$

$\exists$ an aut $\sigma \in Gal(K/k)$ st $\sigma(\alpha) = \alpha+1$

$$\sigma(\alpha+1) = \sigma(\alpha) + \sigma(1) = \alpha+1+1 = \alpha+2$$

must have finite order, p st $\sigma^p(\alpha) = \alpha + p = \alpha$

so $p = p \cdot 1 = 0$

if p is composite

then $p = ab$ st $a, b \neq 0$

but then zero divisor in field. $\Rightarrow\!\Leftarrow$

so p is prime.

(b) Let $\beta = \alpha^p - \alpha$. Show ~~that the degree of $k(\alpha)$~~ over $k(\beta)$ is p.

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

$$\alpha = \frac{\beta}{\alpha^{p-1} - 1} = \frac{\alpha^p - \alpha}{\alpha^{p-1} - 1}$$

$$\sigma(\beta) = \beta$$

$$\begin{aligned}
\sigma(\beta) &= \sigma(\alpha^p - \alpha) \\
&= \sigma(\alpha^p) - \sigma(\alpha) \\
&= \sigma(\alpha)^p - \sigma(\alpha) \\
&= (\alpha+1)^p - (\alpha+1) \\
&= \alpha^p + \cancel{1} - \alpha - \cancel{1} \\
&= \alpha^p - \alpha
\end{aligned}$$

$\boxed{\text{J09Q1}}$

$$1 = \frac{1}{|G|} \sum_{g \in G} |\{x \in X \mid g \cdot x = x\}|$$

1. Sup G acts transitively on sets X & Y where $1 < |X| < |Y| = p$, p prime. Show G is not simple.

$|X| = k$

$$|X| = \frac{|G|}{|\mathrm{stab}_G(x)|} \qquad |Y| = \frac{|G|}{|\mathrm{stab}_G(y)|} = p \qquad p \mid |G|$$

$p \geq 3$

$\varphi_X : G \to S_X$ $\qquad$ $\varphi_Y : G \to S_Y$

$\ker \varphi_X \trianglelefteq G$ $\qquad$ $\ker \varphi_Y \trianglelefteq G$

Sup bwoc G is ~~not~~ simple.

$\exists$ hom. $\varphi : G \to S_k$ st ~~sta~~ $\ker \varphi \leq \mathrm{stab}_G(x)$

Note $\ker \varphi \trianglelefteq G$. Since G simple $\ker \varphi = 1$. So by FIT $G/\ker\varphi \cong \varphi(G) \leq S_k$

$|G| = |\varphi(G)| \leq |S_k|$ $\quad k!$

$|G| \mid k!$

$\rightarrow\leftarrow$

$p \mid |G|$ but $k < p$ so $p \nmid k!$

$\boxed{A08Q2}$

$|K_i| \rightarrow |G : C_G(x_i)|$

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : \cancel{K}_i|$$

2.

a) $|[s]| = \dfrac{|G|}{|\mathrm{stab}_{G\times G}(s)|}$ $\quad \{(g,h) \in G\times G \;\; gsh^{-1} = s\}$

$gs = sh$

$|sG||Gs|$

$a = gsh^{-1}$ $\quad \downarrow$ $\quad \{(g,h)$

$$Gs \cap sG = \{a \in S \mid a = gs = sh \text{ f.s } g,h \in G\}$$

$$|sG| = \frac{|G|}{\mathrm{stab}_{G}^{\cancel{R}}(s)} = \frac{|G|}{|\{g \in G \mid sg = s\}|}$$

$$|Gs| = \frac{|G|}{\mathrm{stab}_{G}^{L}(s)} = \frac{|G|}{|\{g \in G \mid gs = s\}|} = \frac{|G|}{|\{g^{-1} \in G \mid s = g s\}|}$$

$s = g^{-1}s$

$$= \frac{|G|}{\mathrm{stab}_G^{R}(s)}$$

b) $$|G| = |Z(G)| + \sum \frac{|G|}{\mathrm{Stab}(x_i)}$$

Burside

~~If $g \in G$ st $sg = s$~~

~~then $g^{-1} \in G$ satisfies~~

~~$s = sg^{-1}$~~

$$t|G| = \sum_{g \in G} \mathrm{Fix}(g)$$

$\mathrm{Fix}(g,h)$

$|G|^2$

$$t|G\times G| = \sum_{g,h \in G} |\{s \in S \mid gsh^{-1} = s\}|$$

$\boxed{\text{A10Q4}}$

Let p be an odd prime, and let $SL(2,p)$ be the group of all 2×2 matrices of det 1 over the field w/ p elements. Show that $SL(2,p)$ has $p+2$ conj. classes.

$\begin{pmatrix} a & 0 \\ & b \end{pmatrix}$ $\begin{pmatrix} a & 0 \\ & a \end{pmatrix}$ $\begin{pmatrix} a & 1 \\ & a \end{pmatrix}$

$ab = 1$

$p \cdot 1$

$aa = 1$

$a = 1$

$a = -1$

$m = x$ p_j

$\chi_A(x) = x^2 + ax + b$

irreducible

$\begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}$

$\det = b = 1$

$1 + a + 1 = 0$

$a \neq -2$

$1 - a + 1 = 0$

$a \neq 2$

$\Rightarrow p-2$

$x^2 + 2a + a^2 \quad a^2 = 1$

$(x-a)^2$

$\downarrow$

$m_A(x) = x - a$

or

$\cancel{m_A(x) = (x-a)^2 = x^2 - 2ax + a^2}$

$\begin{pmatrix} a & 0 \\ \tau & a \end{pmatrix}$

$\det = a^2 = 1$

$a = 1$ or -1

$\underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}}_{2}$

$\cancel{\begin{pmatrix} 0 & -a^2 \\ 1 & 2a \end{pmatrix}}$

$\cancel{\det = a^2}$

$\cancel{a = 1 \text{ or } -1}$

$\cancel{\begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix}}$ $\cancel{\begin{pmatrix} 0 & -1 \\ 1 & -2 \end{pmatrix}}$

$(x-a)(x-b)$

$x^2 - (a+b)x + ab$

$\begin{pmatrix} 0 & -ab \\ 1 & a+b \end{pmatrix}$

$\det = ab = 1$

$p-1$

$\boxed{p+2}$

$\boxed{\text{J09Q4}}$

Let R be a com. ring w/ 1. Let $f: R^n \to R^m$ be an R-module hom. Prove that if f is inj, then $n \leq m$.

pf Sup f is inj. Assume $n > m$ and let $i: R^m \to R^n$ be the inclusion given by $(r_1, \ldots, r_m) \mapsto (r_1, \ldots, r_m, 0, \ldots, 0)$

$i \circ f : R^n \to R^n$

$p_A(x)$ deg n

so

$\boxed{\text{A11 Q4}}$

$100 = 10^2 = 2^2 \cdot 5^2$

to be finite must not have free part so rank $r=0$

$5 \cdot 2,\ 5 \cdot 2$

$5^2 \cdot 2,\ 2$

$5 \cdot 2^2,\ 5$

$5^2 \cdot 2^2$

$\frac{\mathbb{Z}[i]}{(a+bi)} \times \frac{\mathbb{Z}[i]}{(c+di)}$

st $a^2+b^2=10$

st $c^2+d^2=10$

$\frac{\mathbb{Z}[i]}{}$

5

$= (a+bi)(c+di)$

$5 = ac - bd + (ad+bc)i$

$= 0$

$ad = -bc$

A11 Q6

Let $f(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$.

(a) Show that f is irreducible in $\mathbb{Q}[x]$.

deg 3 + Rational roots theorem $\Rightarrow \pm 1$

but $1^3 + 1^2 - 2(1) - 1 = 1 + 1 - 2 - 1 = -1 \neq 0$

$(-1)^3 + (-1)^2 - 2(-1) - 1 = \cancel{-1} + \cancel{1} + 2 - 1 = 1 \neq 0$

so irreducible (no linear factor)

(b) $f(x^2-2) = (x^2-2)^3 + (x^2-2)^2 - 2(x^2-2) - 1$

$= \quad x^4 - 4x^2 + 4 - 2x^2 + 4 - 1$

$x^6 - 4x^4 + 4x^2$
$-2x^4 + 8x^2 - 8$

$x^3 + x^2 - 2x - 1$
$x^3 - 2x + x^2 - 1$
$x(x^2-2) + x^2 - 1$

$= x^6 - 5x^4 + 8x^2 - 4 - 2x^2 + 3$

$= x^6 - 5x^4 + 6x^2 - 1$

$$
\begin{array}{r}
x^3 - x^2 - 2x + 1 \\
x^3 + x^2 - 2x - 1 \;\big)\; x^6 - 5x^4 + 6x^2 - 1 \\
x^6 + x^5 - 2x^4 - x^3 \\
\hline
-x^5 - 3x^4 + x^3 \\
-x^5 - x^4 + 2x^3 + x^2 \\
\hline
-2x^4 - x^3 + 5x^2 \\
-2x^4 - 2x^3 + 4x^2 + 2x \\
\hline
x^3 + x^2 - 2x - 1
\end{array}
$$

(c) $f(x)$ is irreducible & α is a root of $f(x)$
so $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a deg 3 (finite extention) b/c $f(x)$ is deg 3.
So $\mathbb{Q}(\alpha)/\mathbb{Q}$ is algebraic.

$$\alpha^2+\alpha-2$$

$$x^2 \quad (1+\alpha)x \; + (\alpha(1+\alpha)-2)$$

$$x-\alpha \;\overline{\big)\; x^3 \quad x^2 \quad -2x \quad -1}$$

$$x^3 - \alpha x^2$$

$$(1+\alpha)x^2 \quad -2x$$

$$(1+\alpha)x^2 \quad -\alpha(1+\alpha)x$$

$$(\alpha(1+\alpha)-2)x - 1$$

$$-\alpha[\alpha(1+\alpha)-2]$$

$$\alpha[\alpha+\alpha^2-2]-1$$

$$\alpha^3+\alpha^2-2\alpha-1 = 0$$

$$\alpha^2+2\alpha+1$$

$$x = \frac{-1+\alpha \pm \sqrt{(1+\alpha)^2 - 4\alpha^2 - 4\alpha + 8}}{2}$$

$$= \frac{-1+\alpha \pm \sqrt{-3\alpha^2 - 2\alpha + 9}}{2}$$

-27

$-3 \quad 9$

-2

$\boxed{A12Q3}$ Suppose R is a comm ring w/ 1. A proper ideal I in R is said to be a primary ideal if whenever a and b in R satisfy $ab \in I$ and $a \notin I$ then $\exists\, m \in \mathbb{Z}^+$ st $b^m \in I$.

(a) Show that every prime ideal in R is a primary ideal.

Let P be prime ideal in R.

Suppose $ab \in P$ and $a \notin P$. Then since P is a prime ideal we must have $b \in P$. So $1 \in \mathbb{Z}^+$ and $b^1 = b \in P$. So P is a primary ideal.

(b) Let I be a primary ideal & let

$$I' = \{a \in R \mid a^m \in I \text{ f.s. } m \in \mathbb{Z}^+\}$$

Show that I' is a prime ideal containing I.

Note $I \subseteq R$ and for every $a \in I$ we have $a^1 = a \in I$.

So $I \subseteq I'$. BWOC sup neither a nor $b \in I'$!

Let $ab \in I'$. Then $\exists\, m \in \mathbb{Z}^+$ st $(ab)^m \in I$.

R comm $\Rightarrow$ $a^m b^m \in I$.

can't have $a^m \in I$ or $b^m \in I$ or else $a, b \in I'$!

But then since $a^m \notin I$ and I primary we must have $n \in \mathbb{Z}^+$ st $(b^m)^n = b^{mn} \in I$

Since $b \notin I'$ no such mn can exist. $\rightarrow\leftarrow$

So either a or b must be in I'. Thus I' is prime.

[Show its an ideal].

$I' \subseteq R$ I an ideal, $I \subseteq I'$ nonempty

Let $a, b \in I'$ then $a^m \in I$ $b^n \in I$

$(a-b)^{m+n} \in I$

$(ab)^{mn} \in I$

Let $r \in R$ $(ra)^m = r^m \underbrace{a^m}_{\in I} \in I$ since I is an ideal.

(c) Show that if R is a PID then any primary ideal of R is a power of a prime ideal.

Sup R is a PID. Let I be a primary ideal in R. Then $I = (a)$ for some $a \in R$.

Let

$\boxed{A13Q4}$ Let $M \in GL_n(k)$, k alg closed field

(a) Show that $\exists$ S, U st (i) S is diagonalizable (ii) all eigenvalues of $U = 1$ (iii) $M = SU = US$.

$BMB^{-1} = J = SU = US$ S U US

$M = B^{-1} J B = B^{-1} S U B = B^{-1} U S B$

$= \underbrace{B^{-1}SB}_{\text{still diagonalizable}} \underbrace{B^{-1}UB}_{\text{same eigenvalues}} = B^{-1}UBB^{-1}SB$

(b) Sup $M^2 = I$. Sup char $k \neq 2$

M satisfies $x^2 - 1 = 0$

$(x+1)(x-1) = 0$

so possible eigenvalues are ± 1

$1 \neq -1$ (char $k \neq 2$)

so $m_A(x) \mid x^2 - 1$

$m_A(x) = x - 1$

$= x + 1$

or $= (x-1)(x+1)$

in any case no repeated eigenvalues $\Rightarrow$ diagonalizable

if char $k = 2$ then $1 = -1$ and

if $m_A(x) = (x-1)(x+1) = (x+1)^2$

then $m_A(x)$ has repeated eigenvalues so not diagonalizable. (there is a Jordan block like $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ in M.

6. Sup R is an integral domain & M is a nonprincipal ideal of R.

Let $m \in M \setminus \{0\}$ and $r \in R \setminus \{0\}$.
Then $rm \in M$. Sup $\exists\ s \in R \setminus \{0\}$ st

$$s \cdot rm = 0$$
$$sr \cdot m = 0$$
$$rs \cdot m = 0$$
$$r \cdot sm = 0$$

Sup $rm = 0$
then $sm = 0$

$m, n \in M \setminus \{0\}$.

$r \cdot mn = \cancel{rmn = 0 \cdot n = 0}$
$r \cdot nm$

$$rm + sm = 0$$
$$(r+s) \cdot m = 0$$

$$r(sm) = r \cdot 0 = 0$$
$$\underbrace{rs}_{\neq 0} \cdot \underbrace{m}_{\neq 0} = 0 \rightarrow\leftarrow$$

Let $m, n \in M \setminus \{0\}$
then $(-n) \cdot m + (m)(n) = 0$ since $-n, m \in R \setminus \{0\}$
~~so~~ So n, m are lin dep.
So basis is at most one and we showed every element is lin indep so basis is 1.
So M is ~~for~~ free, rank 1.

$\boxed{\text{A13Q5}}$

Let F and E be fields and let D be an intermediate ring st $F \subseteq D \subseteq E$. Show that if $[E:F]$ is finite, then D is a field. Give a counterexample to show that this is not always true if $[E:F]$ is infinite.

$D \subset E \Rightarrow$ commutative

$F \subseteq D \Rightarrow D$ has identity

Now must show every $d \in D$ has an inverse.

Note since $[E:F]$ is finite, F is algebraic

So $d \in D \subset E$ satisfys some monic minimal polynomial

$f(x) \in F[x]$ $\quad f(x) = \sum_{i=0}^{n} a_i x^i$ st $f(d) = 0$

then $\sum_{i=1}^{n} a_i d^i = -a_0$ $\quad$ Note $a_0 \neq 0$ otherwise f is not minimal.

$d \sum_{i=1}^{n} a_i d^{i-1} = -a_0$ $\quad$ $a_0 \in F$, a field

so $a_0^{-1} \in F$

$$d \cdot \underbrace{-a_0^{-1} \sum_{i=1}^{n} a_i d^{i-1}}_{\in D \text{ \& is } d^{-1}} = 1$$

So D is a field.

J14Q6

(a) Fix $n \geq 1$. Let $I = \{1, 2, \dots, n\}$ and let $G \leq S_n$.
Define an equivalence relation on I: for any $a, b \in I$

$$a \sim b \quad \text{iff} \quad a = b \text{ or } (a\ b) \in G$$

First show this is an equiv. relation.
Second note that S_n and whence also G naturally act on I. In addition, if G acts trans. on I, then show that all the equiv classes under $\sim$ have the same number of elements.

Reflexive: suppose $a \sim b$ for $a, b \in I$.
Then $a = b$ or $(a\ b) \in G$.
So $b = a$ or $(b\ a) \in G$.
Thus $b \sim a$.

Symmetric: Let $a \in I$. Note $a = a$. So $a \sim a$.

Trasitive: Let $a, b, c \in I$ & sup $a \sim b$, $b \sim c$.
Then $a = b$ or $(a\ b) \in G$. Also $b = c$ or $(b\ c) \in G$.

If $a = b$ and $b = c$ then $a = c$.
If $a = b$ and $(b\ c) \in G$ then $(a\ c) \in G$.
If $(a\ b) \in G$ and $b = c$ then $(a\ c) \in G$.
If $(a\ b) \in G$ and $(b\ c) \in G$ then
$(b\ c)(a\ b)(b\ c) = (a\ c) \in G$.

So $\sim$ is an equivalence relation.

$\cdot : S_n \times I \to I$ defined by $\sigma \cdot i = \sigma(i)$

So $G \leq S_n$ also acts on I.

Sup G acts transitively on I.

Then for any $a, b \in I$ $\exists$ $\sigma \in G$ st $\sigma \cdot a = b$

If $a = b$ then $\sigma = e$. do must follow a in σ so

If $a \neq b$ then ~~...~~ σ can be written as a product of transpositions st

(a b) is a transposition. Then since

Let $A = \{a_1, \ldots, a_k\}$, & B be some nonempty equivalence class.

Since G transitive $\exists \sigma \in G$ st $\sigma(a_1) = b \in B$. Since

$a_1 \sim a_i$ $\forall_{1 \le i \le k}$ we have $(a_1\ a_i) \in G$. So $\sigma(a_1\ a_i)\sigma^{-1} \in G$

So $(\sigma(a_1)\ \sigma(a_i)) = (b\ \sigma(a_i)) \in G$. So ~~$b \sim \sigma(a_i)$~~ $1 \le i \le k$.

~~Then $|A| \geq |B|$.~~

~~So $|B| \geq |A|$. Do arguement switched.~~ ~~So $|A| = |B|$.~~

(b) Let $f(x) \in \mathbb{Q}[x]$ be irreducible & have prime deg $p \geq 5$.
Suppose that f has exactly $p-2$ real roots & 2 nonreal roots. Then find the Galois gp of f over $\mathbb{Q}$.

$\tau = (b\ b_1)$ st $b_1 \neq \sigma(a_i)$ for any i

$\checkmark$ $\to (b\ b_1) b_1 \neq (b\ b_1)\sigma(a_i)$

then $\tau\sigma(a_1) = b_1$ $b \neq$

$b_1 \in B$ $b_1 \sim b \sim \sigma(a_i)$

If $\sigma(a_i) \in A$ then $B = A$ so $|A| = |B|$

Otherwise $\sigma(a_i) \in B$ so $|B| \geq |A|$. Do arguement again reversed so $|A| = |B|$. Thus $|A| = |B|$.

$\underbrace{n[x]}_{p} = \#$ of roots class eq.

A14Q6

Let $\alpha = \sqrt{4+3\sqrt{2}}$.

(a) Determine the min poly of α.

$\alpha^2 = 4+3\sqrt{2}$

$\alpha^4 = 16+24\sqrt{2}+18 = 34+24\sqrt{2}$

$\alpha^4 - 8\alpha^2 = 2$ $\qquad \alpha^4 - 8\alpha^2 - 2 = 0$

irreducible, Eisenstein $p=2$.
so min poly for α is
$x^4 - 8x^2 - 2$

(b) Show that $L = \mathbb{Q}(\alpha)$ is not galois over $\mathbb{Q}$

$(x^2)^2 - 8(x^2) - 2$ $\qquad x^2 = \dfrac{8 \pm \sqrt{64-4(-2)}}{2}$

$= 4 \pm \frac{1}{2}\sqrt{72}$ $\quad 72 < {9 \atop 8} \quad {3^2 \atop 2^3}$

$= 4 \pm \cancel{\tfrac{1}{2}} \cdot 3 \cdot \cancel{2}\sqrt{2}$

so $\pm\sqrt{4-3\sqrt{2}}$ also roots of f.

L is not galois because L is not the splitting field of f over $\mathbb{Q}$

since $\beta = \sqrt{4-3\sqrt{2}} \notin L$

Sup $\exists g$ st α is a root and g is separable over $\mathbb{Q}$

then $f \mid g$ since f is min poly for α.

so $\sqrt{4-3\sqrt{2}}$ must be a root of g. But

(c) Let M be the galois closure of L over $\mathbb{Q}$. What is the order of the galois group G of M over $\mathbb{Q}$? $\quad M = \mathbb{Q}(\alpha, \beta)$

$\mathbb{Q}(\alpha,\beta)$
| 2
$\mathbb{Q}(\alpha)$
| 4
$\mathbb{Q}$

deg 8

$(x - \sqrt{4-3\sqrt{2}})(x - \sqrt{4+3\sqrt{2}}) = x^2 - (4-3\sqrt{2})$

$\beta^2 = 4 - 3\sqrt{2}$ $\qquad \alpha^2 = 4+3\sqrt{2}$

$x^2 + \alpha^2 - 8$ $\qquad$ min deg? β a root

$$\sqrt{4-3\sqrt{2}} = a + b\sqrt{4+3\sqrt{2}} + \underbrace{c\,(4}_{\text{absorb into } a} + 3\sqrt{2})$$

$$= a + b\sqrt{4+3\sqrt{2}} + c\,\underbrace{3}_{\text{absorb}}\sqrt{2}$$

$$= a + b\sqrt{4+3\sqrt{2}} + c\sqrt{2}$$

$$4-3\sqrt{2} = a^2 + \cancel{ab\sqrt{4+3\sqrt{2}}} + ac\sqrt{2}$$
$$+ \underline{ab\sqrt{4+3\sqrt{2}}} + b^2(4) + 3\sqrt{2})$$
$$+ bc\sqrt{8+6\sqrt{2}}$$
$$+ ac\sqrt{2} + bc\sqrt{8+3\sqrt{2}}$$
$$+2c^2$$

$$4b^2 + a^2 + 2c^2 = 4 \qquad 3b^2 + 2ac = -3$$

$$2ab = 0$$

$$bc = 0$$

$\underline{a=0}$

$4b^2 + 2c^2 = 4$

$bc = 0$

$3b^2 = -3$

$b = i$

$\rightarrow\leftarrow$

$\underline{b=0}$

$a^2 + 2c^2 = 4$

$2ac = -3$

$a = \frac{-3}{2c}$

$\frac{9}{4c^2} + 2c^2 = 4$

$9 + 8c^4 = 16c^2$

$8c^4 - 16c^2 + 9 = 0$

$c^2 = \frac{16 \pm \sqrt{16^2 - 4(8)(9)}}{16}$

$= 1 \pm \frac{1}{16}$

$\ominus$

imaginary

$\rightarrow\leftarrow$

$\begin{array}{r} 16 \\ 16 \\ \hline 96 \\ 160 \\ \hline 256 \end{array} \qquad \begin{array}{r} 72 \\ 4 \\ \hline 288 \end{array}$

J15Q1

a) False

$$\underset{H}{\langle(12)\rangle} \quad \underset{K}{\langle(13)\rangle}$$

$$HK = \{1, (12), (13), \underbrace{(12)(13)}_{(132)}\}$$

$$KH = \{1, (12), (13), \underbrace{(13)(12)}_{(123)}\}$$

not subgps

(b) True.

$$G \xrightarrow[\text{cayley}]{} S_n \xrightarrow[\text{perm matrices}]{} GL_n(\mathbb{C})$$

all rank n so invertible

$\boxed{\text{A18Q1}}$ Sup G is a gp of order $385 = 5 \cdot 77 = 5 \cdot 7 \cdot 11$

(a) Show that G has exactly one Sylow 11-subgp & that it is a normal subgp.

By Syl thm $\exists$ a Syl 11-subgp, $P_{11} \leq G$.
Note also $n_{11} \equiv 1 \pmod{11}$ & $n_{11} \mid 5 \cdot 7 = 35$.

So $n_{11} \in \{1, \cancel{5}, \cancel{7}, \cancel{35}\}$. $\boxed{n_{11} = 1}$.
Note all Syl p-subgps are conj. So $gP_{11}g^{-1} = P_{11}$ $\forall g \in G$.
Thus P_{11} is normal.

(b) Show that G has exactly one Syl 7-subgp & it is contained in the center of G.

$|C_G(P_7)| = G$
$\Rightarrow P_7 \leq Z(G)$

$n_7 \equiv 1 \pmod 7$ $\quad n_7 \mid 5 \cdot 11 = 55$

44
56

$n_7 \in \{1, \cancel{5}, \cancel{11}, \cancel{55}\}$

only 1 P_7 so normal in G. $\quad N_G(H)/C_G(H) \leq \mathrm{Aut}(H)$

$G/C_G(P_7) \leq \mathrm{Aut}(P_7) \cong \mathbb{Z}_6$

$\frac{|G|}{|C_G(P_7)|} = \frac{5 \cdot 7 \cdot 11}{|C_G(P_7)|} \mid 6$ $\quad 7 \nmid 10$

5·11
7
3·5·11
5·7·11

Let $H = G/P_7P_{11}$. ~~Then $|H| = 5 \cdot 11$~~

~~$n_5 \in \{1, 11\}$ $n_{11} \in \{1, 5\}$~~

~~$P_7P_{11} \leq G$~~
~~$|G : P_7P_{11}| = 5$~~
~~smallest prime~~
~~so $P_7P_{11} \trianglelefteq G$.~~

~~It is cyclic $h \in H$~~
~~$h = gP_7P_{11}$ $g \in G/P_7P_{11}$~~
~~$H = \langle h \rangle$~~

~~Let $a, b \in G$ $\bar{a} = g^iP_7P_{11}$ $\quad ab = g^ig^kP_7P_{11}$~~
~~$\bar{b} = g^kP_7P_{11}$ $\quad = g^kg^i$~~
~~$= ba$~~

~~$g^iP_7g^k$~~
~~$g^kP_7g^i$~~

~~$\bar{G}$ is abelian~~

$\boxed{\text{J15Q2}}$ Let $G = H \ltimes U = U \rtimes H$ be a finite grp, for grps H & U. Let p be prime, & let $Syl_p(G)$ denote the set of Syl p-subgps of G.

(a) Show that if $Syl_p(G) \cap Syl_p(U) \neq \emptyset$ then $Syl_p(G) = Syl_p(U)$

Let $Q \in Syl_p(G)$ Let $P \in \cap$

then $\exists g \in G$ st $gQg^{-1} = P \in Syl_p(U)$

$U \trianglelefteq H$ $\quad \varphi : H \to Aut(U)$

so $Q = g^{-1}Pg \in Syl_p(U)$

$\subseteq$
$\supseteq$ clear so $=$

(b) Sup H acts trans on $Syl_p(U) = Syl_p(G)$ & $\gcd(|H|,|U|) = 1$

$(\Rightarrow)$

$Q \in Syl_p(U) = Syl_p(G)$

$$\underset{\substack{\shortparallel \\ n_p}}{Syl_p(H)} \; |[Q]| = |\underset{H}{\cancel{G}} : stab_{\underset{H}{\cancel{G}}}(Q)| = \frac{|\overset{H}{\cancel{G}}|}{|stab_{\underset{H}{\cancel{G}}}(Q)|} = \frac{|\overset{H}{\cancel{G}}|}{|N_{\underset{H}{\cancel{G}}}(Q)|}$$

$|U : N_U(Q)|$

~~$\Rightarrow N_G(Q) = G$~~

~~$\Rightarrow Q \trianglelefteq G$~~

~~$n_Q = 1, \; Q \trianglelefteq U$~~

since $\gcd(|U|,|H|) = 1$

$\Rightarrow |N_U(Q)| = U$

~~$N_H(Q) = H$ (true but not needed)~~

$Q \trianglelefteq U$

$(\Leftarrow)$ easy

sup. $Q \trianglelefteq U$ f.s $Q \in Syl_p(G) = Syl_p(U)$

then $n_p = 1$ in U and $n_p = 1$ in G

so set is of size 1. So H has to act

transitively on $Syl_p(U)$.

$\boxed{\text{J15 Q4}}$

Let F be a field, char 0. $M_n(F)$.
For $n \in \mathbb{Z}^+$, let I be id in $M_n(F)$. Let J be 1 matrix.
Find JCF of $J-I$ & deduce that $J-I$ is invertible $\forall\, n \geq 2$.

$$J - I = \begin{pmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & 1 & \vdots \\ \vdots & 1 & 0 & \ddots \\ & & \ddots & 1 \\ 1 & \cdots & 1 & 0 \end{pmatrix} = A \qquad tr(A) = 0$$

$\lambda = n-1$ is an eigenvalue w/ eigenvector $\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$

$$J^2 = nJ \Rightarrow J^2 - nJ = 0$$

$A + I = J$ so $(A+I)^2 - n(A+I) = 0$

$$(x+1)^2 - n(x+1) = 0$$

$$x^2 + 2x + 1 - nx - n = 0$$

A satisfies $\longrightarrow$ $x^2 + (2-n)x - (n-1) = 0$

$m_A(x)$ is not deg 1 so must be $\uparrow$

$$J^n = n^{n-1} J \Rightarrow J^n - n^{n-1} J = 0$$

$$(A+I)^n - n^{n-1}(A+I) = 0$$

$$det(A) = (1 - n^{n-1})(-1)^n$$

$$tr(A) = \binom{n}{n-1} = n$$

$$\prod 1^a (n-1)^b = \det A$$

$$\sum^a -1 + \sum^b n-1 = 0$$

$$a + b(n-1) = 0 \qquad a+b = n$$

$$a = n-b$$

$$(x+1)(x-n+1) \qquad n-b+b(n-1) = 0$$

$$x^2 - nx + x + x - n + 1 \qquad n-b+bn-b = 0$$

$$x^2 + (2-n)x - n + 1 \qquad b(-2+n) = -n$$

$$b = \frac{-n}{-2+n}$$

$$a = n + \frac{n}{-2+n}$$

$$-a + 2n - 2 = 0$$

$$-a = -2n + 2$$

$a = 2n-2$ then $a+b = 2n > n \rightarrow\!\leftarrow$

so $b = 1$ and $a = n-1$

$$\chi_A(x) = (x+1)^{n-1}(x-n+1)$$

$$JCF = \begin{pmatrix} -1 & 0 & & & \\ & -1 & \ddots & & 0 \\ & & \ddots & 0 & \\ & 0 & & -1 & 0 \\ & & & & n-1 \end{pmatrix}$$

$\det A = (-1)^{n-1}(n-1) \neq 0$ for $n \geq 2$

J15Q6

Suppose F is a field, K is the splitting field of a degree 4 separable polynomial in $F[X]$, and $[K:F]=8$.

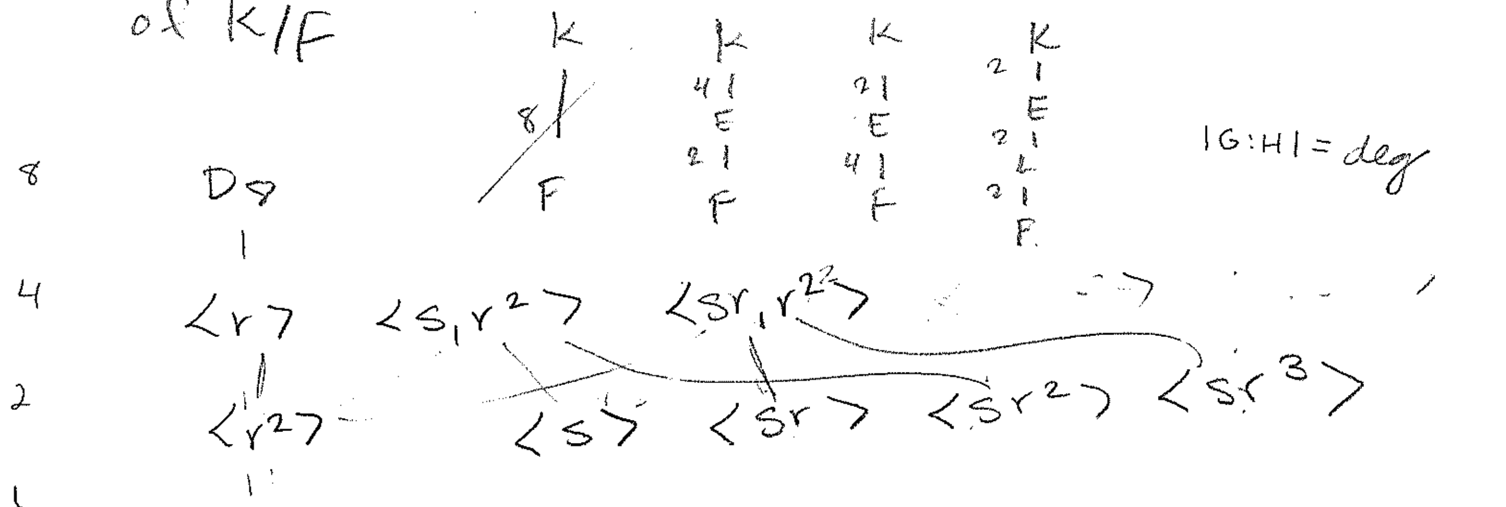
(a) Find $\mathrm{Gal}(K/F)$, up to isomorphism.

K
$8 \mid$
F

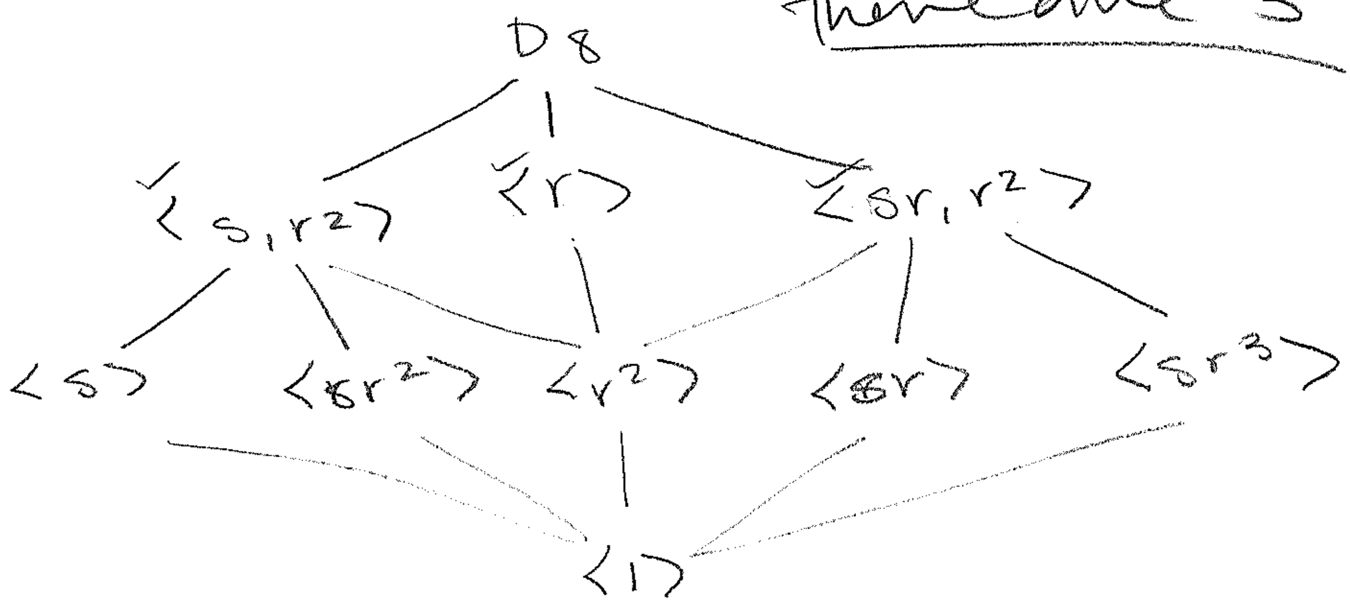
$|\mathrm{Gal}(K/F)| = 8$ & $\leq S_4$ (4 distinct roots)

Must be a transitive $\leq S_4$. So either S_4, D_8, V, or C. So $\cong D_8$.

(b) How many degree 2 subextentions are there of K/F



there are 3



1J15Q3

Let R be the subring of $\mathbb{Q}$ consisting of fractions with odd denominators in reduced form; you may assume w/out proof R is a ring.

(a) Prove that all irr. elements of R, & all prime elements of R are of the form $2u$ f.s. invertible element u of R

R is a ring, $1 \in R$, $R \subseteq \mathbb{Q}$ a field so R has no zero divisors & is commutative. So R is an integral domain.

In an integral domain all prime elements are irreducible. So we need only show this for irreducible elements.

Let $r \in R$ be irreducible. $r = \frac{p}{q}$ f.s. odd q
$(p,q)=1$

If p is odd then r is invertible w/ inverse $\frac{q}{p} \in R$. However, irreducible elements cannot be units. →←

So p must have some ~~factor~~ ~~power~~ factor of 2. Sup $p = 2^k n$, n odd. If $k > 1$ then $p = 2^{k-1} \cdot 2n$, so

$$r = \frac{2^{k-1}}{1} \cdot \frac{2n}{q}$$ Note $\frac{2^{k-1}}{1}, \frac{2n}{q} \in R$ and

neither are units. This also contradicts r being irr. So $k=1$. Thus $r = \frac{2n}{q} = 2u$

~~s.t.~~ $u = \frac{n}{q}$ is a unit w/ inverse $\frac{q}{n}$.

(b) Prove R is Euclidean.

~~Every element in R is a prod. of irreducibles $R \subseteq \mathbb{Q}$ field so UFD~~

~~If $u \in R$ is a unit then $u =$~~

Let $a, b \in R$. If b is a unit then $a = (ab^{-1})b + 0$ ✓

If not then $b = 2^k u$ f.s. $k \in \mathbb{Z}^+$. $a = 2^\ell$ ✗

Then if $k \leq \ell$: $2^\ell v = 2^{\ell-k} 2^k v(v^{-1}u)$ $\ell < k$ $2^k u = 2^{k-\ell} u v^{-1} 2^\ell v$

$\boxed{\text{A08 Q3}}$ p prime. $A = \left\{ \frac{a}{b} \in \mathbb{Q} \mid a, b \in \mathbb{Z},\ p \nmid b \right\}$

(a) Show A is a subring of $\mathbb{Q}$ & is an int dom.

$p \nmid 1$ Clearly $A \subseteq \mathbb{Q}$.

$0 = \frac{0}{1} \in A$, nonempty

Let $x, y \in A$. $x = \frac{a}{b}$ $y = \frac{c}{d}$. Note $-y = \frac{-c}{d} \in A$.

$$\underset{\in A}{x - y} = \frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd} \begin{array}{l} \leftarrow \in \mathbb{Z} \\ \leftarrow p \nmid b,\ p \nmid d \text{ so } p \nmid bd. \end{array}$$

So A subring of $\mathbb{Q}$.

$1 = \frac{1}{1} \in A$. A is comm, since $A \subseteq \mathbb{Q}$, a field.
& A has no zero div
So A is an int dom.

(b) Show that for every nonzero $\alpha \in A$ $\exists$ unique unit $u \in A$ & a unique nonneg int. e st $\alpha = up^e$.

UFD

Let $\alpha \in A$. Then $\alpha = \frac{a}{b}$ $a, b \in \mathbb{Z}$, $p \nmid b$. Since $a \in \mathbb{Z}$ $\exists$ unique $e \in \mathbb{N}$ st
$a = p^e \cdot n$ $p \nmid n$. So $\alpha = \frac{p^e n}{b} = \frac{p^e}{1} \cdot \underbrace{\frac{n}{b}}_{\text{a unit w/ inverse } \frac{b}{n}}$.

(c) Show A is a Euclidean domain.

Let $N : A \to \mathbb{Z}^+ \cup \{0\}$
$N(\alpha) = N(p^e u) = e$
& $N(0) = 0$.

$a = 0$

$a = 0 = 0 \cdot b$

Let $a, b \in A \setminus \{0\}$. $a = p^e u$ $b = p^f v$

wlog $f \le e$ $\quad a = p^e u = p^{e-f} u v^{-1} p^f u$

~~$e < f$~~

Euclidean domain

A15Q1

1. Suppose the conjugacy classes of a finite group G have size at most 4.

Since G is finite let $n \in \mathbb{Z}^+$ be the order of G. By Cayley we have G iso to a subgp of S_n.

Let G act on G by conj. Then by the orbit stabilizer thm we have for $g \in G$

$$\underbrace{|[g]|}_{\text{at most } 4} = \frac{|G|}{|\mathrm{Stab}_G(g)|} = \frac{n}{|\mathrm{Stab}_G(g)|}$$

$$k = \frac{n}{|\mathrm{Stab}_G(g)|} \Rightarrow |\mathrm{Stab}_G(g)| = \frac{n}{k}$$

If $k=1$, then $|\mathrm{Stab}_G(g)| = n \Rightarrow \mathrm{Stab}_G(g) = G$

$C_G(g) = G$

If this holds $\forall g \in G$ the G abelian so solvable. $\Rightarrow g \in Z(G)$

If $k = 2$, then $|\mathrm{Stab}_G(g)| = \frac{n}{2}$. If not then $\downarrow$

$\Rightarrow |G : \mathrm{Stab}_G(g)| = 2 \leftarrow$ smallest prime

$\Rightarrow \mathrm{Stab}_G(g) \trianglelefteq G$ & $G/\mathrm{Stab}_G(g)$ is cyclic so abelian

Note $\mathrm{Stab}_G(g)/\{g\}$ is also cyclic so abelian since index 2.

Sup G has even order. Then $2 \mid n$ cauchy gives an element of order 2. Smallest possible conj class is $n \geq 4$

$\frac{n \cdot (n-1)}{2} \geq \frac{4 \cdot 3}{2} = 6 > 4$. $\Rightarrow \swarrow$ so G not even.

So G solvable w/ series

$1 \trianglelefteq \mathrm{Stab}_G(g) \trianglelefteq G$. $\rightarrow \leftarrow$ otherwise cauchy

If no conj of size 2 then $\nexists$ ~~$\langle a b \rangle \in G$~~ an element of order 2 so G has odd order.

If $k=3$, then $|\mathrm{stab}_G(g)| = \frac{n}{3}$ & $|G:\mathrm{stab}_G(g)| = 3$, smallest prime so normal & $G/\mathrm{stab}_G(g)$ is cyclic so abelian.

So $1 \trianglelefteq \mathrm{stab}_G(g) \trianglelefteq G$ is solvable.

If no such con class size exists then $3 \nmid n$.

So must have $k=4$. However elements in S_n with

Sup G is of even order. Then $2 | n$.
By Cauchy $\exists$ element of order 2.
$G \leq S_n$ must be an element that is the prod of transpositions.

$$\frac{\frac{\binom{n \cdot n-1}{2}\binom{n-2\ n-3}{2} \cdots \binom{2 \cdot 1}{2}}{}}{n/2}$$

If con class size at most 4 then

$|G| = 1$ solv
$|G| = 2$ solv
$|G| = 3$ solv
$|G| \geq 4$?

$$\frac{\frac{(4\cdot \cancel{3})}{\cancel{2}}\frac{(\cancel{2}\cdot 1)}{\cancel{2}}}{\cancel{2}} \quad \frac{\frac{(5\cdot \cancel{4})}{\cancel{2}}\frac{(3\cdot \cancel{2})}{\cancel{2}}}{\cancel{2}} \quad |G| \geq 5$$

$15 > 4 \rightarrow\leftarrow$

smallest can be is $\frac{(5 \cdot \cancel{4}^{2})}{\cancel{2}} = 10 > 4 \rightarrow\leftarrow$

So $|G|$ is odd (so solvable) or 4. $|G| = 4$ then $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_4$

so solvable

A15 Q3

R com $\quad$ max $\Rightarrow$ prime

PID $\quad$ prime $\Rightarrow$ max

3. Suppose R is a PID and S is an integral domain containing no subfield.

Let $\varphi: R \to S$ be a homomorphism. Then $\ker \varphi \subseteq R$ is an ideal of R. Since R is a PID $\ker \varphi = (a)$ for some $a \in R$.

R/P is an integral domain iff P is prime

R/M is a field iff M is maximal.

Note $R/\ker \varphi$ is a subring of S. Since S has no subfields $\ker \varphi$ cannot be maximal. However in a PID we know prime ideals are maximal. That is, in a PID if I is prime then I is maximal. The contrapositive gives not maximal, then not prime. So $\ker \varphi$ is not prime. However in $\ker \varphi$ we have for $k \in \ker \varphi$ $k = ra$ for some $r \in R$. So $a \mid ra$ and $a \mid a$. The only way for $\ker \varphi$ to not be prime then is for $a = 0$. That is $\ker \varphi = (a) = (0) = \{0\}$. Since the kernel of φ is trivial, we have φ is injective.

5. $\boxed{A15Q5}$

Suppose that $f(x) \in \mathbb{Z}[x]$ is a monic irreducible polynomial of degree 4. Suppose there is a complex number α such that both α and α^2 are roots of f.

$$f(x) = (x-\alpha)(x-\bar{\alpha})(x-\alpha^2)(x-\overline{\alpha^2})$$

Note that $\alpha, \alpha^2 \in \mathbb{C} \setminus \mathbb{R}$ since if not then

α ~~or~~ $\alpha^2 \in \mathbb{R}$

$\left(\begin{array}{l} \alpha \in \mathbb{R} \Rightarrow \alpha^2 \in \mathbb{R} \\ \alpha^2 \in \mathbb{R} \Rightarrow \sqrt{\alpha^2} = \alpha \in \mathbb{R} \end{array} \right)$

Note $\alpha \neq \alpha^2$. If so then $\alpha^2 - \alpha = 0$

$\alpha(\alpha - 1) = 0$

$\alpha = 0$ or 1, ~~so real~~

so $\alpha \in \mathbb{Z}$ and so f not irreducible. $\rightarrow\leftarrow$

IA $\alpha, \alpha^2 \in \mathbb{R}$

then $f(x) = (x-\alpha)(x-\alpha^2)(x-\beta)(x-\bar{\beta})$

$\beta \in \mathbb{C} \setminus \mathbb{R}$

FTOA, 4 roots in $\mathbb{C}$, complex conj pairs

---

one real root then 3 non real but conj pairs $\rightarrow\leftarrow$

since if $\beta = \bar{\beta}$ then $\beta \in \mathbb{R}$

three real roots the 1 nonreal again $\rightarrow\leftarrow$

if two real then two nonreal

so $a, b, \beta, \bar{\beta}$

if either α, α^2 are real so is the other

if α^2 non real then α non real

so α nonreal and α^2 must be real

so we have real roots a, α^2 + complex $\alpha, \bar{\alpha}$.

if four real roots then $\exists\, a, b \in \mathbb{R}$, $\alpha, \alpha^2 \in \mathbb{R}$

~~and~~ st $f(x) = (x-a)(x-b)(x-\alpha)(x-\alpha^2)$

no real roots then $\alpha, \beta \in \mathbb{C} \setminus \mathbb{R}$ and come

in complex conj pairs so

$f(x) = (x-\bar{\alpha})(x-\alpha)(x-\bar{\alpha^2})(x-\alpha^2)$

A15Q6

6. Let ζ be a primitive 8^{th} root of unity and let $K = \mathbb{Q}[\zeta]$.

$$\begin{tikzcd} K = \mathbb{Q}[\zeta] \arrow[d, dash, "\varphi(8) = \varphi(2^3) = 2^2(2-1) = 4"] \\ \mathbb{Q} \end{tikzcd}$$

$K/\mathbb{Q}$ is a degree $\varphi(8) = 4$ extention since $K = \mathbb{Q}[\zeta]$ is a cyclotomic field & $\zeta = e^{\frac{2\pi i}{8}}$.

Note $Gal(K|\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z})^{\times} = \{1, 3, 5, 7\}$

Note
$$\left.\begin{array}{l} 3^2 \equiv 9 \equiv 1 \pmod 8 \\ 5^2 \equiv 25 \equiv 1 \pmod 8 \\ 7^2 \equiv 49 \equiv 1 \pmod 8 \end{array}\right\} \text{all have order 2 so}$$

$Gal(K|\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

$1 \mapsto \varphi_1(\zeta) = \zeta$

$3 \mapsto \varphi_3(\zeta) = \zeta^3$

$5 \mapsto \varphi_5(\zeta) = \zeta^5$

$7 \mapsto \varphi_7(\zeta) = \zeta^7$

so

$$\begin{tikzcd} & K \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\zeta^7+\zeta^3) \arrow[dr, dash] & \mathbb{Q}(\zeta+\zeta^5) \arrow[d, dash] & \mathbb{Q}(\zeta+\zeta^7) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}
\qquad
\begin{tikzcd} & \langle 1 \rangle \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\ \langle 3 \rangle \arrow[dr, dash, "2"'] & \langle 5 \rangle \arrow[d, dash, "2"] & \langle 7 \rangle \arrow[dl, dash, "2"] \\ & \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \{1,3,5,7\} & \end{tikzcd}$$

$4 \cdot 3 \equiv 12 \equiv 4$

$4 \cdot 5 \equiv 20 \equiv 4$

$3 \cdot 5 \equiv 15 \equiv 7$

$5 \cdot 7 \equiv 35 \equiv 3$

$3 \cdot 7 \equiv 21 \equiv 5$

$\zeta^a + \zeta^{-a}$ is fixed by φ_a

since $\varphi_a(\zeta + \zeta^a) = \varphi_a(\zeta) + \varphi_a(\zeta^a)^a$

$= \zeta^a + \zeta^{a^2} = \zeta^a + \zeta = \zeta + \zeta^a$

for $a \in \{1, 3, 5, 7\}$

$$\overset{-(\zeta^a+\zeta)}{(x - \zeta^a - \zeta)}\ \overset{-(\zeta^{-a}+\zeta^{-1})}{(x - \zeta^{-a} - \zeta^{-1})}$$

$$= x^2 - \zeta^{-a}x - \zeta^{-1}x - \zeta^a x - \zeta x + (\cancel{\zeta^a\zeta^{-a}} + \zeta^a\zeta^{-1} + \zeta\zeta^{-a} + \cancel{\zeta\zeta^{-1}})$$

$$= x^2 - (\underbrace{\zeta^{-a} + \zeta^a}_{\in \cancel{\mathbb{R}}\,\mathbb{Q}} + \underbrace{\zeta + \zeta^{-1}}_{\in \cancel{\mathbb{R}}\,\mathbb{Q}})x + \underbrace{(\zeta^{a-1} + \overset{(\zeta^{a-1})^{-1}}{\zeta^{1-a}})}_{\in \mathbb{R}}$$

deg 2 poly that $\zeta + \zeta^a$ satisfy in $\mathbb{Q}[x]$. So deg 2 extention.
(can't have deg 1 extention, since $\zeta + \zeta^a \in \mathbb{C} \setminus \mathbb{R}$

So we have

$$\begin{tikzcd}[column sep=small]
 & K \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\zeta+\zeta^3) \arrow[dr, dash, "2"'] & \mathbb{Q}(\zeta+\zeta^5) \arrow[d, dash, "2"] & \mathbb{Q}(\zeta+\zeta^7) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
 & 1 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle e_3 \rangle \arrow[dr, dash] & \langle e_5 \rangle \arrow[d, dash] & \langle e_7 \rangle \arrow[dl, dash] \\
 & \mathbb{Z}_2 \times \mathbb{Z}_2 &
\end{tikzcd}$$

via the Galois correspondence, fixed fields, & degree considerations.

$\boxed{\text{J16 Q3}}$ Prove or disprove:

Every subring of $\mathbb{Q}[x]$ is a UFD.

Let $A = \{ p(x) \in \mathbb{Q}[x] \mid \text{linear term is zero} \}$

Note $0 := \sum_{i=1}^{n} 0x^i \in A$. $q \geq m$

Let $p(x), q(x) \in A$. $p(x) - q(x) = \sum_{i=1}^{n} (p_i - q_i)x^i \in A$.

$\sum_{i=m}^{n} p_i x^i +$

A additive subgp

$i=1$ $p_1 = q_1 = 0$
so $p_1 - q_1 = 0$
so no linear term

$p(x) \cdot q(x) =$ each term's coeff is product & sum of $\mathbb{Q}$ so $\in \mathbb{Q}$
and coeff for x is

$\in A$

$q_0 p_1 + p_0 q_1 = 0$ so no lin term

So A subring of $\mathbb{Q}[x]$.

Note $x \notin A$.

Only way to factor x^2 is $1 \cdot x \cdot \underline{x}$ but $x \notin A$

x^3 $\quad x \cdot x \cdot \underline{x}$

$x^3, x^2 \cdot \underline{x}$

$\deg(p(x)q(x)) = \deg p + \deg q$ so $x^2 = p \cdot q$

$\deg p = 1$, $q = 1$ or $p = 2$, $q = 0$

Observe $x^6 = x^2 x^2 x^2 = x^3 x^3$ $\Leftarrow$ not unique up to a unit

$\deg \neq 1$ so $2, 0$ & $3, 0$ so $\deg 0 \Rightarrow$ unit and $x^2 \mid p(x)$

$\boxed{J13Q3}$

Prove that the subring of $\mathbb{Q}[x]$ consisting of all polynomials w/ integer constant term is not a UFD.

$$A = \left\{ \sum_{i=1}^{n} a_i x^i + c \mid a_i \in \mathbb{Q},\ c \in \mathbb{Z} \right\}$$

Pf

$$\left(\tfrac{1}{2}x + 2\right)\left(2x + 1\right)$$

$$x^2 + 4x + \tfrac{1}{2}x + 2$$

$$x^2 + \tfrac{9}{2}x + 2$$

$$\left(\tfrac{1}{2}x + 1\right)\left(2x + 2\right)$$

$$x^2 + 2x + x + 2$$

$$(ax + b)(cx + d)$$

$$acx^2 + (bc + ad)x + bd$$

$$acx^2 + (2c + 5a)x + 10$$

$$2c + 5a = 0$$

$$c = -\frac{5a}{2}$$

$a = 2$

$c =$

$$x = 2 \cdot \tfrac{1}{2}x$$

$$= 4 \cdot \tfrac{1}{2} \cdot \tfrac{1}{2}x$$

$$= 4 \cdot \tfrac{1}{4}x$$

W16Q5

Find all irr poly of deg 4 in $\mathbb{F}_2[x]$ explicitly.

Must be monic, otherwise $f(x)$ is deg 3.

$f(x) = x^4 + ax^3 + bx^2 + cx + d$

To be irr $d = 1$ otherwise factor an x.

$f(x) = x^4 + ax^3 + bx^2 + cx + 1$

$x^4 + x^3 + x^2 + x + 1$
no lin factor
$\alpha + \gamma = 1$ $\quad \alpha\gamma = 1$
$\Rightarrow \alpha = \gamma = 1$
$\Rightarrow\Leftarrow$
irr
★

$\left[x^4 + x^3 + x^2 + 1 \right.$
1 is a factor
$\left. 1+1+1+1 = 0 \right]$

$\left[x^4 + x^3 + x + 1 \right.$
1 is a factor
$\left. 1+1+1+1=0 \right]$

$\left[x^4 + x^2 + x + 1 \right.$
$\left. 1+1+1+1 = 0 \right]$

$x^4 + x^3 + 1$
no lin factor
$\alpha + \gamma = 1 = 0$ $\Rightarrow\Leftarrow$
irr
★

$\left[x^4 + x^2 + 1 = (x^2+x+1)(x^2+x+1) \right.$
no lin factor
$\alpha\gamma = 1$ $\quad \gamma + \alpha = 0$ ✓
$\left. \Rightarrow \alpha = \gamma = 1 \right]$

$x^4 + x + 1$
no lin factor
$\alpha + \gamma = 1 = 0$ $\Rightarrow\Leftarrow$
irr
★

$\left[x^4 + 1 \right.$
$\left. 1 \text{ is a factor} \right]$

$$(x^2 + \alpha x + \overset{1}{\beta})(x^2 + \gamma x + \overset{1}{\delta})$$
$$= \cancel{x^4} + \cancel{\gamma x^3} + \cancel{\overset{1}{\delta} x^2} + \cancel{\alpha x^3} + \cancel{\alpha\gamma x^2} + \alpha\delta x$$
$$+ \cancel{\overset{1}{\beta} x^2} + \beta\gamma x + \beta\delta$$
$$= x^4 + (\gamma+\alpha)x^3 + 1\alpha\gamma x^2 + (\alpha+\gamma)x + 1$$

$\beta\delta = 1 \Rightarrow \beta = \delta = 1$

$\boxed{\text{J16 Q6}}$

Let p and q be distinct prime numbers & let $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$

(i) Show that the extension $K/\mathbb{Q}$ is Galois deg 4

roots are

$\pm\sqrt{p}$, $\pm\sqrt{q}$

$(x^2 - p)(x^2 - q) \leftarrow$ seperable poly

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\sqrt{p},\sqrt{q}) \arrow[dl, dash] \arrow[dd, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{p}) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\sqrt{q}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Sup $\mathbb{Q}(\sqrt{p}) = \mathbb{Q}(\sqrt{q})$

~~then for $\alpha \in \mathbb{Q}(\sqrt{p})$~~

~~we have~~

$\alpha = \cancel{a + b\sqrt{p} = c + d\sqrt{q}}$

$\cancel{a^2 + 2ab\sqrt{p} + pb^2 = c^2 + 2cd\sqrt{q} + d^2q}$

$\cancel{a + bp = (c + d\sqrt{q})(a - b\sqrt{p})}$

$\cancel{= ac - cb\sqrt{p} + ad\sqrt{q} - bd\sqrt{qp}}$

then $\sqrt{q} \in \mathbb{Q}(\sqrt{p})$. That is,

$\sqrt{q} = a + b\sqrt{p}$, $a, b \neq 0$ so $q = a^2 + 2ab\sqrt{p} + b^2p$

$\Rightarrow \dfrac{q - b^2p - a^2}{2ab} = \sqrt{p}$

if $a = 0$

$q = b^2p$ ~~prime~~ $\rightarrow\leftarrow$

if $b = 0$ $\sqrt{q} \in \mathbb{Q} \rightarrow\leftarrow$

if $a = b = 0$ $\sqrt{q} = 0$

$\Rightarrow \sqrt{p} \in \mathbb{Q} \rightarrow\leftarrow$

$[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2 \neq 1$.

So $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}] = 4$, is Galois

(ii) $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p} + \sqrt{q})$

$\boxed{A16\ Q4}$ Let F be a field & let $A \in M_n(F)$ be a non-invertible $n \times n$ matrix over F

(i) Prove that if 0 is the only eigenvalue of A in F and F is algebraically closed then we have $A^n = 0$.

alg closed, eigenvalue $0 \in F$ ~~so~~
~~JCF has all 0 on diagonal~~

so $\chi_A(x) = \prod_{i=1}^{n}(x-0) = x^n = 0$

thus $A^n = 0$.

$\chi_A(x)$ has all roots in F but 0 is only eigenvalue in F and eigenvalues are roots of $\chi_A(x)$.
So 0 is the only eigenvalue thus

(ii) Find an example of a field F & a noninvertible matrix $A \in M_n(F)$ st 0 is

$\chi_A(x) = x^{n-2}(x^2+1)$ over $\mathbb{Q}$

$m_A(x) = x(x^2+1)$
$= x^3 + x$

$$A = \begin{pmatrix} 0 & & & & \\ & \ddots & & & \\ & & 0 & & \\ & & & 0 & 0 & 0 \\ & & & 1 & 0 & -1 \\ & & & 0 & 1 & 0 \end{pmatrix}$$

A14Q4

(a) Sup that A is a complex $n\times n$ matrix w/ $A^3 = -A$.
Show that A is diagonalizable.

so A satisfies $x^3 + x = 0$

$\Rightarrow x(x^2+1) = 0$

$\Rightarrow x(x-i)(x+i) = 0$

$\lambda \in \{0, i, -i\}$
distinct eigenvalues $\in \mathbb{C}$
so diagonalizable

(b) Sup A is a 2×2 matrix over $\mathbb{Q}$
w/ no non-trivial eigenvectors w/
entries in $\mathbb{Q}$ + $A^3 = -A$.
Show that A is $\simeq$ over $\mathbb{Q}$ to $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

$x^3 + x = 0$

$x(x^2+1) = 0$

$m_A(x) \mid x(x^2+1)$ but $\lambda \neq 0$
so

$m_A(x) \mid x^2+1$
$\hookrightarrow$ irreducible over $\mathbb{Q}$
RRT: ± 1 $1^2+1 = 2 \neq 0$
$(-1)^2+1 = 2 \neq 0$

so RCF is $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

$\boxed{\text{A16Q6}}$

Let $f = x^4 - 3$. Find the degree of the splitting field of f over $\mathbb{Q}$. Describe the Galois group of f, by giving its action on the roots of f explicitly, and identifying it as iso to a known finite group.

$\pm \sqrt[4]{3}$, $\pm i\sqrt[4]{3}$ are the four roots of $f(x)$.

Note f is irreducible by Eisenstein, $p=3$.

so $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 4$ and $[\mathbb{Q}(\sqrt[4]{3}, i) : \mathbb{Q}(\sqrt[4]{3})] = 2$

$\mathbb{Q}(\sqrt[4]{3}) \subseteq \mathbb{R}$ while $i \in \mathbb{C}$ so

since i satisfies the irreducible poly x^2+1

deg 8 extension

clearly $K \subseteq \mathbb{Q}(\sqrt[4]{3}, i)$. Now $\sqrt[4]{3} \in K$ and $i\sqrt[4]{3} \in K$

so $i = i\sqrt[4]{3} \cdot \frac{1}{\sqrt[4]{3}} \in K$

Thus $\mathbb{Q}(\sqrt[4]{3}, i) = K$.

$\sigma_a : \sqrt[4]{3} \longmapsto i^a \sqrt[4]{3} \quad 0 \le a \le 3$

$\tau_b : i \longmapsto (-1)^b i \quad 0 \le b \le 1$

$G = \langle \underset{r}{\sigma_1}, \underset{s}{\tau_1} \rangle$. Note $\sigma_1^4 = 1 = \tau_1^2$ $\quad rs = sr^3$

$|G| = 8$

$\sigma_1 \tau_1 : \sqrt[4]{3} \mapsto i\sqrt[4]{3}$ ✓

$i \mapsto -i$ ✓

$\tau_1 \sigma_1^3 : \sqrt[4]{3} \mapsto i\sqrt[4]{3}$

$i \mapsto -i$

so satisfies relation

thus $G \cong D_8$

A08 Q6 Let K be the splitting field of $f = x^4 + 2x^2 - 2$ over the field of rational numbers $\mathbb{Q}$. Determine the Galois group G of K over $\mathbb{Q}$.

f is irreducible by Eisenstein $p = 2$.

$(x^2)^2 + 2(x^2) + 2$ $\quad x^2 = \frac{-2 \pm \sqrt{4 - 4(2)}}{2}$

$= \frac{-2 \pm \sqrt{-4}}{2}$

$= -1 \pm i$

$2e^{\frac{3\pi i}{4}}$ $\quad 2e^{\frac{5\pi i}{4}}$

$\pm\sqrt{2}\, e^{i\frac{3\pi}{8}}$ $\quad \pm\sqrt{2}\, e^{i\frac{5\pi}{8}}$

4 distinct roots
separable

$K = \mathbb{Q}(\sqrt{3}, \sqrt{2}, i)$
$\subseteq$ clearly
$\supseteq$ since

$\sqrt{2}\left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) - \sqrt{2}\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)$
$= \sqrt{2}\left(\frac{1}{2} + \frac{1}{2} + \frac{\sqrt{3}}{2}i - \frac{\sqrt{3}}{2}i\right)$
$= \sqrt{2} \in K$

$\frac{1}{\sqrt{2}}\left[\sqrt{2}\left(\frac{1}{2} + \frac{\sqrt{3}}{2}\right) + \sqrt{2}\left(-\frac{1}{2} + \frac{\sqrt{-3}}{2}\right)\right]$
$= \frac{1}{\sqrt{2}}\left[\sqrt{2}\left(\frac{1}{2} - \frac{1}{2} + \frac{\sqrt{-3}}{2} + \frac{\sqrt{-3}}{2}\right)\right]$
$= \sqrt{-3} \in K$

deg 4

J17Q2

Sup every maximal subgp of a finite gp G has prime index.

(a) Show G has a normal Syl subgp.

$|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ descending $p_1 > p_i$

Let P be a Sylow p_1-subgp. Then $|P| = p_1^{\alpha_1}$.

If P is maximal it must have prime index.

That is $p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q$ for some prime q.

Since $p_1 > p_i$ we have $p > q$. So q is the smallest prime dividing $|G|$. ~~Thus~~ Since $|G:P| = q$ we have $P \trianglelefteq G$. ~~As a Syl p_1-subgp we know~~

$p_1^{\alpha_1} \mid |M|$

If P is not maximal then $P \subsetneq M$, M maximal

Note M has prime index, i.e. $|G:M| = q$

A12Q2

Show any gp of order $104 = 2^3 \cdot 13$ is Solvable.

$n_2 \equiv 1 \pmod 2$ $\quad$ $n_{13} \equiv 1 \pmod{13}$

$n_2 \mid 13$ $\quad$ $n_{13} \mid 2^3 = 8$

$n_2 \in \{1, 13\}$ $\quad$ $n_{13} \in \{1\}$

$\cancel{13+}$

$P_{13} \trianglelefteq G$ $\quad$ $|G : P_{13}| = 2^3$ $\quad$ $\cancel{4+13+4-4+14} = 56$

$n_{13} = |G : N_G(P_{13})| \cancel{=1}$

$\exists$ $H = \langle g \rangle$ $|g| = 2$ since $2 \mid |G| = 104$

$P_{13}H \leq G$ $\quad$ $|P_{13}H| = 26$ w/ index 4

Q1 $\quad$ $|G| = 120 = 4 \cdot 30 = 4 \cdot 3 \cdot 10 = 2^3 \cdot 3 \cdot 5$

$n_2 \in \{1, 3, 5, 15\}$ $\quad$ $n_3 \in \{\cancel{1, 2, 4, 5, 8, 10},$
$\{1, \cancel{2}, 4, \cancel{8}, 10, 20, 40\}$

$n_5 \in \{1, \cancel{2}, \cancel{4}, \cancel{8}, \cancel{3}, \boxed{6}, \cancel{12}, \cancel{24}\}$

Sup $n_2 = 3$. Let G act on the Sylow 2 subgps by conj. $\varphi : G \to S_3$ $\quad$ $G/\ker\varphi \cong \leq S_3$

$\ker\varphi \neq G$ $\quad$ can't have $\ker\varphi = 1$ otherwise $\to\leftarrow$ lagrange

$\ker\varphi \trianglelefteq G$

$n_5 = 6$ $\quad$ $|G : N_G(P_5)| = 6$

$|N_G(P_5)| = 20$ $\quad$ $G \leq S_6$

But P_5 sylow 5 subgp of S_6

$|S_6 : P_5| =$

$\boxed{\text{J08Q4}}$ ~~Let A be an n×n matrix over $\mathbb{C}$ st $tr(A^k)=0$ $\forall k>0$. Show that $A^n=0$.~~

$\boxed{\text{J17Q4}}$

$$A \approx J \quad \boxed{e^A \approx e^J}$$

$$\begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$$

$$Pe^{A}P^{-1}$$

$$\det(e^A) = I + \frac{1}{2}A^2 + \frac{1}{6}A^3 + \cdots +$$

$$\approx I + \frac{1}{2}J^2 + \frac{1}{3!}J^3 + \cdots +$$

$$\begin{pmatrix} e^{\lambda_1} & & & \\ & e^{\lambda_2} & & \\ & & \ddots & \\ 0 & & & e^{\lambda_n} \end{pmatrix}$$

$$\prod_{i=1}^{n} e^{\lambda_i} = e^{\lambda_1 + \cdots + \lambda_n}$$

$$e^{\lambda_1} \quad = e^{tr(A)}$$

$\boxed{\text{A19 Q4}}$ Let T be a lin trans. def on the vector space of polynomials in x of degree $< n$ over $\mathbb{R}$ by $T(f(x)) = f(x+1)$. Find the $\chi_T(x)$, $m_T(x)$, & JCF of T.

Basis for V is $\{x^i \mid 0 \le i \le n-1\}$

$x^2 \to (x^2+2x+1)(x+1)x^3$

x^3+2x^2+x

$x^2 \quad 2x \quad 1$

x^3+3x^2+3x+1

$$T \longleftrightarrow \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & 3 & 4 & & \vdots \\ & & 1 & 3 & 6 & & \vdots \\ & & & 1 & 4 & \cdots & \vdots \\ & & & & 1 & & \vdots \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}$$

$(x+1)^k = \sum_{i=1}^{k} \binom{k}{i} x^i$

$\cancel{\chi_T(x)} = (T-I)^n$

eigenvalues all 1

so $\chi_T(x) = (x-1)^n = m_T(x)$

since there are $n-1$ diag nonzero

JCF is $\begin{pmatrix} 1 & 1 & & & \\ & \ddots & \ddots & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ & & & & 1 \end{pmatrix}$

J17Q6

(a) Find an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ whose splitting field over $\mathbb{Q}$ has a 12 element Galois group where all Sylow subgps are normal.

$12 = 2^2 \cdot 3$

$\mathbb{Q}(\zeta_n)$
$|$
$\mathbb{Q}$

$|A_4| = 12$

$V_4 \trianglelefteq A_4$

$\mathbb{Z}_{12}$
abelian

e
(12)(34)
(13)(24)
(14)(23)
(123) (132)
(124) (142)
(134) (143)
(234) (243)

$|\mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| \cong |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$ $\quad \varphi(7)=6, \ \varphi(4)=2, \ n = 28$

$\cancel{f(x) = \Phi_{28}(x)}$ $\quad \boxed{n=13}$ $\quad \varphi(13) = 12$

Then $(\mathbb{Z}/13\mathbb{Z})^\times \cong \mathbb{Z}_{12}$ abelian so every subgp is normal.

$\mathbb{Q}(\zeta_{13})$ is the splitting field of the cyclotomic polynomial $\Phi_{13}(x)$ over $\mathbb{Q}$ where $\Phi_{13}(x) = x^{12} + x^{11} + \cdots + x + 1$.

Note it is irreducible.

(b) Give the Sylow subgps up to iso

$\mathbb{Z}_4$ & $\mathbb{Z}_3$

A17Q1

Assume G infinite ~~abelian~~ nonabelian gp whose proper subgps are finite.

Show every proper normal subgp $\subseteq Z(G)$.
Explain why $G/Z(G)$ is infin simple gp whose proper subgps are finite.

Let H be a proper normal subgroup of G, $H \trianglelefteq G$.

N C theorem: $N_G(H)/C_G(H) \cong\leq \mathrm{Aut}(H)$

$G/C_G(H) \cong\leq \mathrm{Aut}(H)$

$|H|$ is finite so $|\mathrm{Aut}(H)|$ is finite. Since $|G| = \infty$ must have $C_G(H) = G$ so $|G/C_G(H)| = 1 \,\big|\, |\mathrm{Aut}(H)|$

so ~~[illegible]~~ $H \leq Z(G)$.

$G/Z(G) \cong\leq \mathrm{Aut}(G)$

$\uparrow$

simple since the normal subgps of G ~~subgps of $Z(G)$ and~~ containing $Z(G)$ are in bij correspondence w/ the normal subgps of $G/Z(G)$ by 4th iso. But all proper normal subgps of G are contained in $Z(G)$. So there are no normal proper subgps in G that contain $Z(G)$ So no proper normal subgps of $G/Z(G)$ so simple. Every proper gp of $G/Z(G)$ is in $\Leftrightarrow$ w/ proper in G and $|\bar{H}| \,\big|\, |H|$, so $\bar{H}$ are all finite. Note G nonabelian so $Z(G) \neq G$ so $Z(G) < G$ so $|G/Z(G)| = \infty$.

$f(x) = x^5 - 80x + 5$

$f(2) = 2^5 - 160 + 5$

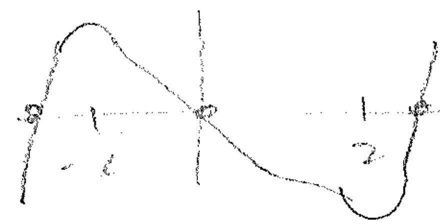
$32 - 160 + 5 = -$

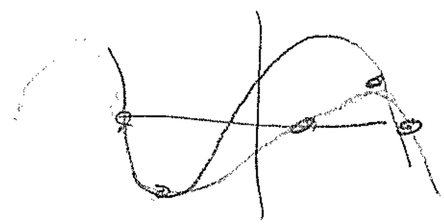
$f(-2) = -32 + 160 + 5 = P$

$f'(x) = 5x^4 - 80$

$= 5(x^4 - 16) = 5(x^2 - 4)(x^2 + 4)$

± 2





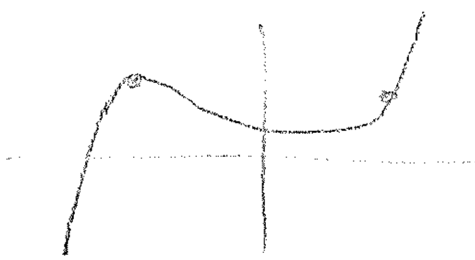
F

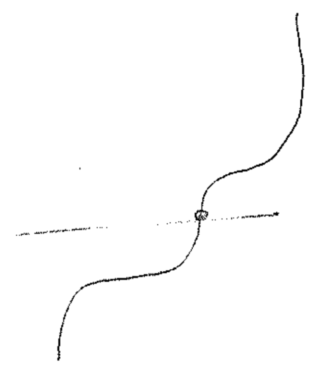
$|$

$k \quad E \quad 5 | K$

$| \; 5$

$\mathbb{Q}$





$\mathbb{Z}_+$ non neg integers

$\mathbb{N}$ $\{1, 2, \ldots, \}$

A17Q6 Let $p \geq 5$ be a prime number and let L be the splitting field of $x^p - 1$ over $\mathbb{Q}$.

(a) Find the explicit generators for Gal(L/K), and explain why your answer is correct. What is the structure of this group?

irreducible (min poly for ζ_p)

$$x^p - 1 = x-1\,(x^{p-1} + \cdots + x + 1)$$

$1 \in \mathbb{Q}$ $\quad \Phi_p(x)$

$p-1$ roots, the powers of ζ_p st primitive

splitting field so $L = \mathbb{Q}(\zeta_p)$ $\quad L/\mathbb{Q}$ is deg $p-1$

$\sigma_a : \zeta_p \mapsto \zeta_p^a$ $\quad$ Gal$(L/K) \cong \mathbb{Z}_{p-1}$

(b) $\quad 1 \leq a \leq p-1$ $\quad = \langle \sigma_2 \rangle$

(b) Use (a) to find the explicit generators for a subfield K of L st $[L:K] = 2$ & explain why your answer is correct.

$$\boxed{\begin{array}{l}\sigma_{-1} : \zeta_p \mapsto \zeta_p^{-1} \\ \text{order } 2 \\ \text{fixes } \zeta_p + \zeta_p^{-1}\end{array}}$$

$$\begin{array}{ccc} L & & 1 \\ | \; 2 & & | \\ K & & H \quad |H| = 2 \\ | & & | \\ \mathbb{Q} & & \mathbb{Z}_{p-1} \end{array} \quad (p-1 \text{ from } \mathbb{Q} \text{ to } L)$$

$\sigma_a(\zeta_p) = \zeta_p^a$

$\sigma_a^2(\zeta_p) = \zeta_p^{2a}$

so $H = \langle \sigma_{\frac{p+1}{2}} \rangle \leq$ Gal$(L/\mathbb{Q})$

order 2

$2 \cdot \frac{p+1}{2}$ $\quad a$

$p+1 = 1$

$\frac{p+1}{2} \cdot$ ~~$2a \equiv 1 \pmod p$~~

$(p+1)a$

pa ~~$+ a \equiv \frac{p-1}{2}$~~

$a = \frac{p-2}{2}$

FTO Galois

J18Q1

Let G be S_5 & let P be a Syl 5-subgp of G.

(i) Show $|N_G(P)| = 20$.

$|S_5| = 5\cdot4\cdot3\cdot2 = 2^3\cdot3\cdot5$

$n_5 \in \{1, \cancel{3}, \cancel{2}, \cancel{4}, \cancel{8}, 6, \cancel{12}, \cancel{24}\}$

but $n_5 \equiv 1 \pmod 5$

Note a Syl 5 subgp can be

$\langle(12345)\rangle = \{1, (12345), (13524), (14253), (15432)\}$

$\neq$

and also $\langle(13245)\rangle = \{1, (13245), (12534), (14352), (15423)\}$

so $n_5 \neq 1$ (if $n_5 = 1$, only 1 sylow 5 subgp.)

so $n_5 = 6$. Thus $|G : N_G(P)| = n_5 = 6$

$\Rightarrow \dfrac{5\cdot3\cdot2^3}{|N_G(P)|} = 6$

$\Rightarrow |N_G(P)| = \dfrac{5\cdot\cancel{3}\cdot2^{\cancel{3}\,2}}{\cancel{6}} = 20$

(b) Clearing the powers of $(12345) \in N_G(P)$.

$(1\,2\,3\,4\,5)$

$\downarrow \sigma \quad \Rightarrow \quad \cancel{\sigma = (25)(34)}$

$\cancel{(15432)}$

$1\,3\,5\,2\,4 \qquad \sigma = (2354)$

$N_G(P) = \langle(2354), (12345)\rangle$

$\boxed{A18Q1}$

$|G| = 385 = 5 \cdot 77 = 5 \cdot 7 \cdot 11$

$n_{11} \equiv 1 \pmod{11}$

a) $n_{11} \in \{\underline{\underline{1}}, \cancel{5}, \cancel{7}, \cancel{35}\}$

unique $\Rightarrow$ normal

$7 \overline{)55}$ 7, 49, 6

b) $n_7 \in \{1, \cancel{5}, \cancel{11}, \cancel{55}\}$ $n_7 \equiv 1 \pmod 7$

$P \trianglelefteq G$

$N_G(P)/C_G(P) \cong\leq \mathbb{Z}_6$

$5 \cdot 7 \cdot 11$ $\dfrac{|G|}{|C_G(P)|} \mid 6$

$C_G(P) = G$

$\Rightarrow P \leq Z(G)$

$\boxed{J18\,Q1}$

Let $G = S_5$, let P be a Sylow 5-subgp

(i) show $|N_G(P)| = 20$.

$|G| = 2^3 \cdot 3 \cdot 5$

$n_5 = |G : N_G(P)|$

$n_5 \equiv 1 \pmod 5$

$n_5 \in \{\underline{1}, \cancel{2}, \cancel{3}, \cancel{4}, \underline{6}, \cancel{8}, \cancel{12}, \cancel{24}\}$

$6 = \dfrac{120}{|N_G(P)|} \Rightarrow |N_G(P)| = 20$

$\dfrac{\cancel{5} \cdot 4 \cdot 3 \cdot 2 \cdot 1}{8}$

$\langle (12345) \rangle =$ 1 2 3 4 5

1 3 5 2 4

1 4 2 5 3

1 5 4 3 2

1

(12) $1 \mapsto 1$, $2 \mapsto 3$, $3 \mapsto 5$, $4 \mapsto 2$, $5 \mapsto 4$ (12) $\underline{(2354)}$

$= (21345) \notin \langle (12345) \rangle$

Not normal $\Rightarrow n_5 = 6 \Rightarrow$

(ii) $\langle (12345), \underline{(2354)} \rangle$

$1 \to 1$
$2 \to 4$
$3 \to 2$
$4 \to 5$
$5 \to 3$

(2453)

$1 \mapsto 1$
$2 \mapsto 3$
$3 \mapsto 5$
$4 \mapsto 2$
$5 \mapsto 4$

(2354)

A18 Q 3 | Let G denote the Galois group of $f(x) = x^5 - 10x + 5$ over the rationals. View G as a subgroup of S_5.

(a) Consider ~~any~~ irreducible polynomial $g(x)$ over $\mathbb{Q}$ of prime degree p. Show that the Galois gp has an element of order p.

$g(x)$ has p roots. $\sigma \in G$ must permute the roots

Let α be a root of $g(x)$. Then $[\mathbb{Q}(\alpha):\mathbb{Q}] = p$ since $g(x)$ is irreducible. Let K be the splitting field then $|G| = [K:\mathbb{Q}]$

$= [K:\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}]$

thus $p \mid |G|$.

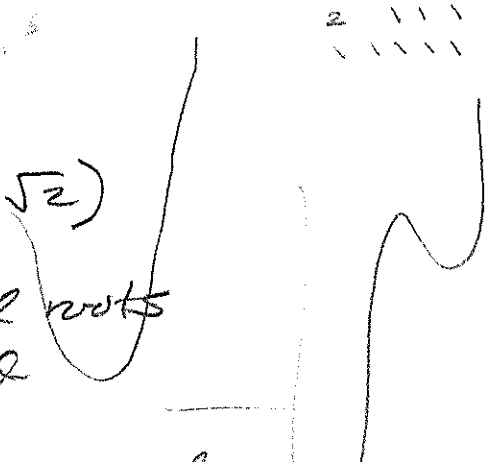
By Cauchy $\exists\ \sigma \in G$ st $|\sigma| = p$.

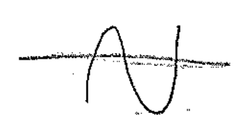
(b) f is irr over $\mathbb{Q}$ of prime deg $p=5$.
so by (a) G contains a $|\sigma| = 5$, in S_5
$\Rightarrow \sigma$ is a 5-cycle

5	5
4 1	4
3 2	6
3 1 1	3
2 2 1	2
2 1 1 1	2
1 1 1 1 1	1

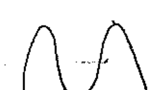
(c) $f'(x) = 5x^4 - 10$
$= 5(x^4 - 2)$
$= 5(x^2 + \sqrt{2})(x^2 - \sqrt{2})$

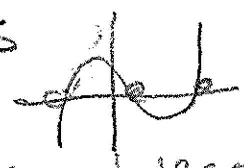
2 imaginary   2 real roots





So almost 3 real roots





so there is at least 2 complex roots to f, conj pairs.
So this gives a 2 cycle in S_5.

d) $\langle (12), (12345) \rangle = S_5$

$G = \langle (a\ b), (a\ b\ \underline{e}\ \underline{c}\ \underline{d}) \rangle$ relabel

the 2-cycle

sup $a = 1$

sup $\sigma = (1\,2\,3\,4\,5)$

then powers of σ give every combo so that

σ^2 1 3

σ^3 1 4

σ^4 1 5

σ 1 2

$\sigma^l = (a\ b\ \_\ \_\ \_)$

f.s. l.

$(a\ b)$ $(c\ a\ \cancel{e}\ b\ d)$

A18Q6

Consider the con classes in $GL_2(\mathbb{F}_5)$

How many such con classes contain matrices whose eigenvalues lie in $\mathbb{F}_5$?

INVERTIBLE

JCF's: $\begin{pmatrix} a & 0 \\ & a \end{pmatrix}$ $\begin{pmatrix} a & 1 \\ & a \end{pmatrix}$ $\begin{pmatrix} a & 0 \\ & b \end{pmatrix}$

$\cancel{5} + \cancel{5} + \cancel{5} \cdot \cancel{4} = 3\cancel{0}$

$4 + 4 + 4 \cdot 3 = 20$

J19Q4 List all con classes of $GL_n(\mathbb{C})$ w/ finitely many elements.

$\boxed{\text{J18 Q4}}$ Let F be a field of arbitrary char. Show that any two elements of order 2 in $SL_2(F)$ are conj. in $GL_2(F)$. Find a necessary & suff condition on F for $SL_2(F)$ to have a unique element of order 2.

Let $A, B \in SL_2(F)$ st $x^2 = 1$

$x^2 - 1 = 0$

$\det A = \det B = 1$

$(x - \lambda_1)(x - \lambda_2) = x^2 - 1$

$\lambda_1 \lambda_2 = 1$

$x^2 - (\lambda_1 + \lambda_2)x + \lambda_1\lambda_2 = x^2 - 1$

$\lambda_1 = \frac{1}{\lambda_2}$

$\lambda_1 \lambda_2 = -1$

and $\lambda_1 + \lambda_2 = 0$

$\lambda_1 = -\frac{1}{\lambda_2}$

$\lambda_1 = -\lambda_2$

$\lambda_1 + \lambda_2 = 0$

$\lambda_2^2 = 1$

$\lambda_1 = -\lambda_2$

$\lambda_2 = \pm 1$

$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$\lambda_2 = 1$, $\lambda_1 = -1$

$\lambda_2 = -1$, $\lambda_1 = 1$

|J19 Q6| Let $[K:F] = 4$ for fields K and F of char $\neq 2$. Show that K is Galois over F w/ $Gal(K/F) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ iff $\exists\ \alpha, \beta \in F$ st $\sqrt{\alpha}, \sqrt{\beta}, \sqrt{\alpha\beta} \notin F$ & $K = F(\sqrt{\alpha}, \sqrt{\beta})$

($\Rightarrow$) Sup. K/F is Galois w/ $Gal(K/F) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$$4\left\{\begin{tikzcd}[column sep=small] & K \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\ E_1 \arrow[dr, dash, "2"'] & E_2 \arrow[d, dash, "2"] & E_3 \arrow[dl, dash, "2"] \\ & F & \end{tikzcd}\right. \qquad \begin{tikzcd}[column sep=small] & \{(0,0)\} \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\ \langle(1,0)\rangle \arrow[dr, dash, "2"'] & \langle(1,1)\rangle \arrow[d, dash, "2"] & \langle(0,1)\rangle \arrow[dl, dash, "2"] \\ & \mathbb{Z}_2 \times \mathbb{Z}_2 & \end{tikzcd}$$

Then ~~wlog~~ E_1 must have $a \in E_1$ st a satisfies a degree 2 monic polynomial in F. That is

$a^2 - \alpha = 0$ for some $\alpha \in F$. Thus $a = \pm\sqrt{\alpha}$.

So $E_1 = F(\sqrt{\alpha})$. ~~Since K/E_1 is degree 2 then there also exists $b \in K$ st b satisfies a deg 2 monic polynomial in E_1. That is $b^2 - \beta = 0$ f.s. $\beta \in E_1$~~ Also, $E_2 \neq E_1$ must have $b \in E_2$ st b satisfies a deg 2 monic poly in F. That is

$b^2 - \beta = 0$ f.s. $\beta \in F$. Thus $b = \pm\sqrt{\beta}$. So $E_2 = F(\sqrt{\beta})$

since $E_1 \neq E_2$, $\sqrt{\beta} \neq \sqrt{\alpha}$. By the diagram, FTOG, we have $K = F(\sqrt{\alpha}, \sqrt{\beta})$. Also $\sqrt{\alpha\beta} \notin F$ since ~~[illegible]~~ $\{1, \sqrt{\alpha}\}$ is a basis for E_1 & $\{1, \sqrt{\beta}\}$ is a basis for E_2, so $\{1, \sqrt{\alpha}, \sqrt{\beta}, \sqrt{\alpha\beta}\}$ is a basis for K. If $\sqrt{\alpha\beta} \in F$ then the basis would be size 3, but $[K:F] = 4$, so it must be $\sqrt{\alpha\beta} \notin F$.

($\Leftarrow$) Sup $\exists\ \alpha, \beta \in F$ st $\sqrt{\alpha}, \sqrt{\beta}, \sqrt{\alpha\beta} \notin F$ & $K = F(\sqrt{\alpha}, \sqrt{\beta})$

$$\begin{tikzcd}
 & K = F(\sqrt{\alpha}, \sqrt{\beta}) \arrow[dl, no head] \arrow[dd, no head, "4"] \arrow[dr, no head] & \\
E_1 \arrow[dr, no head, "2"'] & & E_2 \arrow[dl, no head, "2"] \\
 & F &
\end{tikzcd}$$

$\leftarrow$ has basis $\{1, \sqrt{\alpha}, \sqrt{\beta}, \sqrt{\alpha\beta}\}$
so $[K:F] = 4$.

since $\sqrt{\alpha}, \sqrt{\beta} \notin F$ but $\alpha, \beta \in F$
we have $\sqrt{\alpha}^2 - \alpha = 0$
$\sqrt{\beta}^2 - \beta = 0$

so $E_1 = F(\sqrt{\alpha})$ is a subfield of K and a subextention over F of deg 2 w/ irreducible poly $x^2 - \alpha$.

Sim $E_2 = F(\sqrt{\beta})$ deg 2 over $x^2 - \beta$.

Note $\sqrt{\alpha} \neq \sqrt{\beta}$ since if it were then

$$\sqrt{\alpha\beta} = \sqrt{\alpha}\sqrt{\beta} = \sqrt{\alpha}\sqrt{\alpha} = \sqrt{\alpha^2} = \alpha \in F \rightarrow\leftarrow$$

So $E_1 \not\subseteq E_2$ and $E_2 \not\subseteq E_1$

So $(x^2 - \alpha)(x^2 - \beta)$ is a deg 4 sep poly in F which gives K/F. Finite extention so K/F is Galois.

Galois group

$\sigma: \sqrt{\alpha} \mapsto \sqrt{\alpha}$
$\quad \sqrt{\beta} \mapsto -\sqrt{\beta}$

$\tau: \sqrt{\alpha} \mapsto -\sqrt{\alpha}$
$\quad \sqrt{\beta} \mapsto \sqrt{\beta}$

$\sigma\tau: \sqrt{\alpha} \mapsto -\sqrt{\alpha} \quad = \tau\sigma$
$\quad \sqrt{\beta} \mapsto -\sqrt{\beta}$

$1 \quad \vdots$

all deg 2, commutative
So $\cong \mathbb{Z}_2 \times \mathbb{Z}_2$

J19 Q4

List all conj. classes of $GL_n(\mathbb{C})$ w/ finitely many elements.

$~~\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}~~$

$$\left[\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}\right] \qquad \left[\alpha\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}\right] \quad \alpha \in \mathbb{C}$$

conj classes of size 1

$$\begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$$

$$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \quad \alpha \neq \beta$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{\det(A)}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$\begin{pmatrix} \gamma & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}\frac{1}{\gamma}\begin{pmatrix} 1 & 0 \\ 0 & \gamma \end{pmatrix}$$

$$\begin{pmatrix} \gamma\alpha & \gamma \\ 0 & \alpha \end{pmatrix}\frac{1}{\gamma}\begin{pmatrix} 1 & 0 \\ 0 & \gamma \end{pmatrix}$$

$\gamma \in \mathbb{C}$ so infinitely many

$$\frac{1}{\gamma}\begin{pmatrix} \gamma\alpha & \gamma^2 \\ 0 & \gamma\alpha \end{pmatrix}$$

$$\begin{pmatrix} \alpha & \gamma \\ 0 & \alpha \end{pmatrix} \to (x-\alpha)^2$$

$$C_A(x) = x^2 - 2\alpha x + \alpha^2 = 0$$
$$= (x-\alpha)^2 = m_A(x)$$

$$\begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}\frac{1}{1}\begin{pmatrix} 1 & -\gamma \\ 0 & 1 \end{pmatrix}$$

$\begin{pmatrix} \alpha & 1 \\ & \alpha \end{pmatrix}$ ✓

$$\begin{pmatrix} \alpha & \gamma\beta \\ 0 & \beta \end{pmatrix}\begin{pmatrix} 1 & -\gamma \\ 0 & 1 \end{pmatrix}$$

$\beta - \alpha \neq 0$ since $\alpha \neq \beta$

$$\begin{pmatrix} \alpha & \gamma\beta - \gamma\alpha \\ 0 & \beta \end{pmatrix} \leftarrow \gamma(\beta-\alpha)$$

$\gamma \in \mathbb{C}$ infinitely many

$\boxed{\text{J19Q5}}$

Prove that the cyclotomic polynomial $\Phi_{19}(x)$ is irreducible over the field $\mathbb{Q}(i)$.
(You may assume that $\Phi_n(x)$ is irreducible over $\mathbb{Q}$ $\forall n \geq 1$).

$$\begin{tikzcd} \mathbb{Q}(\zeta_{19}) \arrow[d, dash, "18"'] \\ \mathbb{Q} \end{tikzcd}$$

$\zeta_{19} = e^{\frac{2\pi i}{19}}$

$\zeta_{19}^{a} \neq i = e^{\frac{\pi i}{2}}$ for any a.

$$\begin{tikzcd} \mathbb{Q}(i) \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

$i = \zeta_{4} = e^{\frac{i\pi}{2}} = e^{\frac{2\pi i}{4}}$

$19 \equiv 3 \bmod 4$

$x^4 - 1 = (x^2+1)(x^2-1)$

↑
irreducible RRT

$$\begin{tikzcd} & \mathbb{Q}(\zeta_{19}, i) \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\zeta_{19}) \arrow[dr, dash, "18"'] & & \mathbb{Q}(i) \arrow[dl, dash, "2"] \\ & \mathbb{Q} & \end{tikzcd}$$

$\rightarrow$

primitive
↓

$$\begin{tikzcd} & \mathbb{Q}(\zeta_{19}\zeta_4 = \zeta_{19\cdot 4}) \arrow[dl, dash, "2"'] \arrow[d, dash] \arrow[dr, dash, "(\zeta_{19},\, \zeta_4)\uparrow \; 18"] & \\ \mathbb{Q}(\zeta_{19}) \arrow[dr, dash] & \mathbb{Q} & \mathbb{Q}(\zeta_4) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

$\varphi(19 \cdot 4) = 18 \cdot 2$

since $[\mathbb{Q}(\zeta_{19}, \zeta_4) : \mathbb{Q}(\zeta_4)] = 18$

so ζ_{19} satisfies a deg 18 min poly $f(x)$ over $\mathbb{Q}(i)$. Since $\Phi_{19}(x)$ is min poly over $\mathbb{Q}$ we must have ~~[illegible]~~

$f(x) \mid \Phi_{19}(x)$ but both are monic of deg 18 so $f(x) = \Phi_{19}(x)$.

Thus $\Phi_{19}(x)$ is irreducible over $\mathbb{Q}(i)$.

A19 Q1

Let p, q, r be distinct primes.
Show no gp of size pqr is simple.

wlog $p < q < r$

$n_p \in \{\cancel{1}, \cancel{q}, r, qr\}$

$n_q \in \{\cancel{1}, \cancel{p}, r, pr\}$

$n_r \in \{\cancel{1}, \cancel{p}, \cancel{q}, pq\}$

If $n_p = q$ $\exists$ $\varphi: G \to S_q$

$G/\ker \cong \leq S_q$

$\ker \neq 1 \neq G$

so $\ker \trianglelefteq G$

similarly $n_r = q$

$\ker \trianglelefteq G$

If n_q or $n_r = p$ then

$|G : N_G(Q)|$
$|G : N_G(R)|$ $= p$ smallest prime
so normalizers are normal subgps.

$pq(r-1) + r(q-1) + r(p-1)$

$= pqr \underbrace{-pq + rq}_{q(r-p) > 0} \underbrace{-r + rp - r}_{\underbrace{-2r + rp}_{r(p-2) > 0}}$

> 0 $\quad p \geq 2$

$> pqr$ too many elements!

A17 Q3

Let A be an int. dom. containing a field $\mathbb{F}$ as a subring. This makes A a vector space over $\mathbb{F}$. Show that if A is finite dim over F, then A is a field. Show that A need not be a field if it is not fin dim over $\mathbb{F}$.

Sup A is fin dim over $\mathbb{F}$. Say $[A:\mathbb{F}]=n$

~~Then A has basis $\{1, a_1, \ldots, a_n\}$ $f_i, n \in \mathbb{Z}^+$~~

~~Let $a \in A \setminus \{0\}$. Then~~

~~$a = f_0 \cdot 1 + f_1 a_1 + \cdots + f_n a_n$ st at least one $f_i \neq 0$~~

Then a satisfies some deg n poly w/ coeff in $\mathbb{F}$

$$f_n(a)^n + \cdots + f_1(a) + f_0 = 0$$

$$(f_n(a)^n + \cdots + f_1(a) = -f_0 \quad \exists f_0^{-1} \text{ b/c } \mathbb{F} \text{ field}$$

$$-f_0^{-1} f_n a^n + \cdots + f_0^{-1} f_1 a = 1$$

$$a \underbrace{(-f_0^{-1} f_n a^{n-1} - \cdots - f_0^{-1} f_1)}_{a^{-1}} = 1$$

$\mathbb{F}[x]$ has infinite deg over $\mathbb{F}$ & is not a field since $x \in \mathbb{F}[x]$ does not have an inverse.

A19 Q2

Sup G is finite st $\underset{n}{|G|}$ + $\underset{m}{|Aut(G)|}$ are relatively prime.

(a) Show G is abelian.

$$Inn(G) \cong G/Z(G) \leq Aut(G)$$

$$\Rightarrow \frac{|G|}{|Z(G)|} \Big| |Aut(G)|$$

$(n,m)=1$
$\Rightarrow (\frac{n}{k}, m)=1$
so $\frac{n}{k}=1$

$$\Rightarrow |Z(G)| = |G|$$

$$\Rightarrow G \text{ abelian}$$

b) Possible structure of pf:

(1) WLOG G is a p-group (if each Sylow subgp is cyclic, so is the whole gp)
(2) As an abelian p-gp, G is a product of cyclic gps.
(3) Suppose one of the factors is a cyclic gp of order p^k. Then the automorphism gp has size $p^k - p^{k-1}$ (by counting coprime elements). This is only coprime to the order of G if $k=1$.
(4) Therefore G is elementary abelian w/ say m factors. In this case, the automorphism gp is isomorphic to $GL(m, \mathbb{Z}/p\mathbb{Z})$. This gp has order coprime to G only if $m=1$.

So G is cyclic (and each Sylow subgp is of prime order)

$\boxed{\text{A19Q3}}$

Show that in a UFD every irreducible generates a prime ideal.

Let R be a UFD. Let $r \in R$ be irreducible. Note r is nonzero and not a unit. We will show r is prime. Suppose $r \mid ab$ for some $a, b \in R$. Then $ab = rk$ f.s. $k \in R$.

$$k = v \Sigma k_i^{\kappa_i}$$

$$a = u \Sigma a_i^{\alpha_i} \qquad b = w \Sigma b_i^{\beta_i}$$

Since r is irreducible and $ab = rk$, there must be some a_i or b_i that is associate to r.

WLOG sup $a_1 = u'r$. Then

$$a = u(u'r) \sum_{i=2} a_i^{\alpha_i}$$

so $r \mid a$. Thus, r is prime.

So (r) is a prime ideal by def.

| J20 Q4 |

Let R be subring of $\mathbb{Q}$ consisting of fractions whose denom (in lowest terms) are odd.
You may use that R is Euclidean.
Let M be fin gen, unital R-mod.
Prove if every nonzero element of M satisfies $m+m \neq 0$ then M is a free R-mod

Sup $\exists$ $m \in M \setminus \{0\}$ and $r \in R \setminus \{0\}$

st $rm = 0$ $\therefore r = \frac{p}{q}$ q odd

then $2rm = 0$

$\Rightarrow$

if p even
$p = 2k$
then
$rm = 0$
$\frac{2k}{q} m = 0$
$\underbrace{\frac{k}{q} m}_{\neq 0} + \frac{k}{q} m = 0$ $\rightarrow\leftarrow$

if $\frac{k}{q} m$ is zero then do again till k is odd then

if p odd then r invertible w/ inverse $\frac{q}{p}$

so $rm = 0$
$\Rightarrow \frac{p}{q} m = 0$

$\frac{q}{p} \cdot \frac{p}{q} m = \frac{q}{p} \cdot 0$

$m = 0$ $\rightarrow\leftarrow$

so M is Tor free so $M \cong R^r$ f.s $r \in \mathbb{Z}^+$

J11 Q4

$$\left(\begin{pmatrix} 1 & 1 & \cdots & 1 \\ & \ddots & & \vdots \\ & & \ddots & 1 \\ & & & 1 \end{pmatrix} - I \right)^n$$

$\chi_A(x) = (x-1)^n = m_A(x)$

$\longrightarrow \sum_{i=0}^{n} \binom{n}{i} (-1)^{n-i} x^i$

RCF

$$\begin{pmatrix} 0 & & & & -1 \\ 1 & 0 & & & \vdots \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & \\ & & & 1 & \binom{n}{n-1}(-1)^n \end{pmatrix}$$

JCF

$$\begin{pmatrix} 1 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 1 \end{pmatrix}$$

Sup $I, A, A^2, \ldots, A^{n-1}$ is <u>not</u> lin indep. Then $\exists\, r_i \in F \setminus \{0\}$ st

$r_{n-1} A^{n-1} + \cdots + r_1 A + r_0 I = 0$

$p(x) = \frac{r_{n-1}}{r_{n-1}} x^{n-1} + \cdots + \frac{r_1}{r_{n-1}} x + \frac{r_0}{r_{n-1}}$

~~then~~ is an $n-1$ deg poly ~~that~~ A

satisfies. this must be

$(x-1)\underbrace{(x-1)^{n-1}}$ so r_i are $\binom{n-1}{i}(-1)^{n-1-i}$

$\Rightarrow$ all positive

$\Rightarrow$ can't be $= 0$

so $m_A(x) \mid p(x)$

but $\deg m_A(x)$ is n

and $\deg p(x)$ is $\leq n-1$

$\rightarrow\leftarrow$

$\boxed{J20Q6}$

Let $f(x) = x^5 - 80x + 5$. Find the Galois group of f over $\mathbb{Q}$.

Let K be the splitting field of f over $\mathbb{Q}$.
First, $f(x)$ is irreducible by Eisenstein $p=5$.
So $K/\mathbb{Q}$ is Galois. Since f is deg 5, $G \leq S_5$.

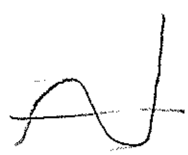
Irreducible over $\mathbb{Q}$ $\Rightarrow$ separable

Note that a degree 5 separable polynomial has 5 distinct roots. ~~Also~~ Since G permutes these roots we have

Since f is deg 5 $\mathbb{Q}(\alpha)$ f.s. α st $f(\alpha)=0$ we have $[\mathbb{Q}(\alpha):\mathbb{Q}]=5$. So $5 \mid |G|$. By Cauchy $\exists\, \sigma \in G$ st $|\sigma|=5$. So σ is a 5-cycle.

$$f'(x) = 5x^4 - 80 = 5(x^4 - 20) = 5(x^2+\sqrt{20})(x^2-\sqrt{20})$$

two real roots

So f looks like  so f has at most 3 real roots. ~~The other two~~ By FTOA all roots live in $\mathbb{C}$. So the other two must be conjugate pairs. So $\exists\, \tau \in G$ that permutes these imaginary conjugate roots. Thus τ is a 2-cycle.

~~the~~ conj

Label the roots $\alpha_1, \alpha_2, \alpha_3, \beta_4, \beta_5$

$\tau = (45)$ $\quad \sigma = (a\ b\ c\ d\ e)$

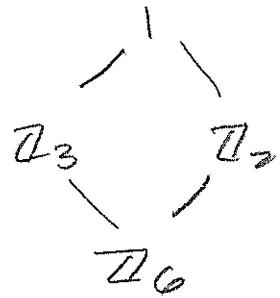
powers of σ give a next to any other element. So

label st $\tau, \sigma^e = (45\_\,\_\,\_)$

thus $G \cong S_5$

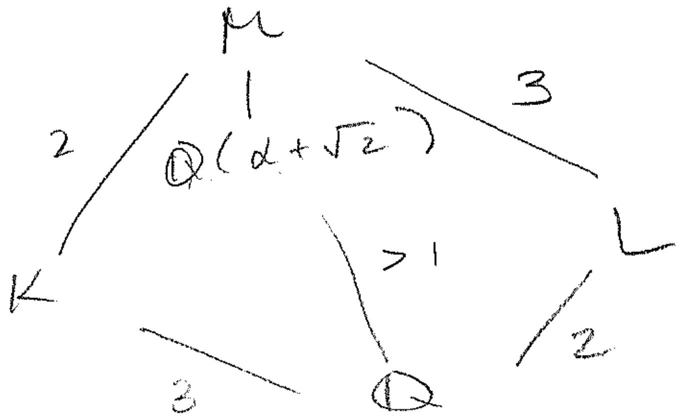
A20Q6

(d) $G \cong \mathbb{Z}_6$



$\alpha + \sqrt{2}$

$\mathbb{Q}(\alpha+\sqrt{2}) \subseteq \mathbb{Q}(\alpha, \sqrt{2})$



$\mathbb{Q}(\alpha+\sqrt{2})$ must be K, L, or M.

Sup $\mathbb{Q}(\alpha+\sqrt{2}) = \cancel{K} = \mathbb{Q}(\alpha)$ then

$\sqrt{2} \in \mathbb{Q}(\alpha)$

$\rightarrow\leftarrow$

sup $= L = \mathbb{Q}(\sqrt{2})$

then $\cancel{\alpha} \in \mathbb{Q}$ $\rightarrow\leftarrow$

So $\mathbb{Q}(\alpha+\sqrt{2}) = M$.

A20Q2

(a) Give an ex of a Syl 2-subgp of S_5 + give iso type

$|S_5| = 5! = 5 \cdot 4 \cdot 3 \cdot 2 = 2^3 \cdot 3 \cdot 5$

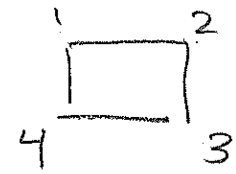
$|D_8| = 8$

$D_8 \cong \langle (13), (1234) \rangle \leq S_5$

So D_8 is a Syl 2-subgp of S_5.

(b) How many does S_5 have?

All must be conjugate.



$n_2 \in \{1, 3, 5, \boxed{15}\}$

$D_8 \cong \{ (12), (13$

$$\frac{5 \cdot \cancel{4} \cdot 3 \cdot 2}{\cancel{4}}$$

D_8 will have 2 four cycles (one + its inverse) there are ↑ 4 cycles so there are 15 diff 4 cycles to label our square

$\cancel{|[D_8]| = \frac{|S_5|}{|\mathrm{Stab}_{S_5}(D_8)|} = \frac{5!}{2} = 5 \cdot 4 \cdot 3}$

(1234)

1 3

3 4 1 2

$\sigma(1) = 1$ or 3.

$\sigma(3) = 3$ or 1

$\sigma(2) = 2$

$\sigma(4) = 4$

$\sigma(2) = 4$

$\sigma(4) = 2$

$\cancel{(13)(24)}$

$\boxed{A20\,Q3}$ Let R be a ring

$\boxed{\text{A20 Q2}}$

(a) Give an example of a Sylow 2-subgp of S_5 & determine its iso type ~~[illegible]~~

$$|S_5| = 5! = 5\cdot 4\cdot 3\cdot 2\cdot 1 = 5\cdot 3\cdot 2^3$$

~~So~~ Let P be a Sylow 2-subgp of S_5.

$|P| = 2^3 = 8$ Note D_8 is a subgp of S_5

$D_8 = \langle (13), (1234)\rangle \le S_5$.

Since all Sylow 2-subgps are conj., P is conj to D_8. Conj ~~[illegible]~~ is an isomorphism.

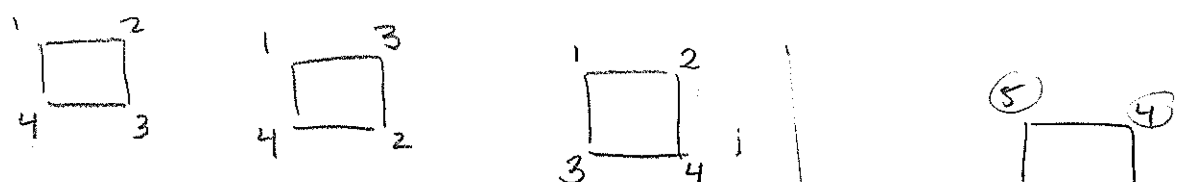
So $P \cong D_8$.

(b) How many Syl 2-subgps does S_5 have? Justify.

$n_2 \equiv 1 \pmod 2$ $\quad n_2 \mid 5\cdot 3$ $\quad$ ~~$n_3 \in \{1, 2, 4, 5, 8$~~

$n_2 \in \{1, 3, 5, 15\}$ $\quad$ ~~$n_3 \in \{$~~

~~Most overlap is 4. So 4·15+4 = 64~~



$\langle (13), (1234)\rangle$ $\quad \langle (12), (1324)\rangle$ $\quad \langle (14), (1243)\rangle$

≥ 3

but any of 1, 2, 3, 4 can be replaced by a 5 so there are $5\cdot 3 = 15$ Syl 2-subgps of S_5 all iso to D_8.

$\boxed{J20\ Q2}$ Let p be odd prime & let G be a gp of order $2p^2$.

(i) Show that G is an internal semidirect prod of Syl subgps.

A20 Q4

Consider $n\times n$ matrices w/ entries in $\mathbb{F}_q$

(a) over $\mathbb{F}_q$ one cannot always compute the JCF of an arbitrary $M \in M_n(\mathbb{F}_q)$. Explain why one can compute it over $\mathbb{F}_q$ when M is upper triangular.

~~det~~ upper tri λ are the diag entries which are in $\mathbb{F}_q$.

(b) sup $n \geq 4$. How many sim classes of $M_n(\mathbb{F}_q)$ contain an upper tri matrix of rank 2?

JCF rank 2

$$\begin{pmatrix} a & 1 & \\ & a & \\ & & \ddots \end{pmatrix} \quad q-1 \qquad = \qquad \begin{pmatrix} a & 0 & \\ & a & \\ & & \ddots \end{pmatrix} \quad q-1$$

$$a \;\Big|\; \begin{pmatrix} 0 & 1 \\ & 0 \end{pmatrix} \quad q-1$$

$$\begin{pmatrix} a & 0 & \\ & b & \\ & & \ddots \end{pmatrix} \quad \cancel{q(q-1)}$$

$$\begin{pmatrix} 0 & 1 & \\ & 0 & 1 \\ & & 0 \end{pmatrix} \quad 1$$

$$\begin{pmatrix} 0 & 1 & & \\ & 0 & & \\ & & 0 & 1 \\ & & & 0 \end{pmatrix} \quad 1$$

$\cancel{q(q-1)+2q}$

$\cancel{q[q-1+2]}$

$(q-1)(q-2)$

$(q-1)(q-2+2)+2$ $\qquad$ $\cancel{q(q+1)}$

$q(q-1)+2+q-1$ $\qquad$ $\boxed{q^2+1}$

$q(q-1)+q+1$ $\qquad$ $q(q-1+1)+1$

$\boxed{\text{A 20 Q6}}$ Consider the field $K = \mathbb{Q}(\alpha)$ where the minimal polynomial of α is $f(x) = x^3 - x^2 - 4x - 1$. Note that $-1/(1+\alpha)$ also satisfies the min poly. Consider also the field $L = \mathbb{Q}(\sqrt{2})$. Define $M = \mathbb{Q}(\alpha, \sqrt{2})$

(a) Prove that K is Galois, and give the iso type of its gp.

f is irreducible by RRT.

$$g = (x-\alpha)\left(x + \frac{1}{1+\alpha}\right) = x^2 + \left(\frac{1}{1+\alpha} - \alpha\right)x - \frac{\alpha}{1+\alpha}$$

$x + \left(\alpha - \frac{1}{1+\alpha} - 1\right)$

$g \,)\, x^3 - x^2 - 4x - 1$

$x^3 \quad \left(\frac{1}{1+\alpha} - \alpha\right)x^2 - \frac{\alpha}{1+\alpha}x$

$\left(\alpha - \frac{1}{1+\alpha} - 1\right)x^2 + \left(\frac{\alpha}{1+\alpha} - 4\right)x - 1$

$x \quad - \frac{\alpha^2}{1+\alpha} + \frac{\alpha}{(1+\alpha)^2} \pm \frac{\alpha}{1+\alpha}$

$\left(-\frac{1}{(1+\alpha)^2} + \frac{\alpha - 1}{1+\alpha} + \alpha - \alpha^2 - 4\right)x + \frac{\alpha^2}{1+\alpha} - \frac{\alpha}{(1+\alpha)^2} - \frac{\alpha}{1+\alpha} - 1$

$\frac{\alpha}{1+\alpha} - \alpha^2$

$-\frac{1}{(1+\alpha)^2} + \frac{\alpha}{1+\alpha}$

$-\frac{1}{1+\alpha} + \alpha$

$$(x-\alpha)\left(x + \frac{1}{1+\alpha}\right)(x - \beta) = f(x)$$

$\frac{\alpha}{1+\alpha}\beta = -1$

$\beta = -\frac{1+\alpha}{\alpha}$

so $K = \mathbb{Q}(\alpha)$.
So $K/\mathbb{Q}$ is Galois
deg 3 so $G \cong \mathbb{Z}_3$

(b) $[L : \mathbb{Q}] = 2$
$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$
$\Big\}$ relatively prime so can't be subfields
so $L \cap K = \mathbb{Q}$

(c) $\mathbb{Q}(\alpha, \sqrt{2})$ is splitting field of

$f(x)\cdot(x^2-2)$

irr so sep.. over $\mathbb{Q}$ w/ no shared roots

so $M/\mathbb{Q}$ Galois w/ $|G| = 6$

$$\begin{array}{cccc} K & 1 & L & 1 \\ | & | & | & | \\ \mathbb{Q} & \mathbb{Z}_3 & \mathbb{Q} & \mathbb{Z}_2 \end{array}$$

$$\begin{tikzcd} & M \arrow[dl, dash, "2"'] \arrow[dr, dash, "3"] & \\ K \arrow[dr, dash, "3"'] & & L \arrow[dl, dash, "2"] \\ & \mathbb{Q} & \end{tikzcd} \qquad \begin{tikzcd} & 1 \arrow[dl, dash] \arrow[dr, dash] & \\ H_1 \arrow[dr, dash] & & H_2 \arrow[dl, dash] \\ & G & \end{tikzcd}$$

$H_1 H_2 = G$ since both normal

$G \cong \mathbb{Z}_3 \times \mathbb{Z}_2$

$G/H_1 \cong \mathbb{Z}_3$

$G/H_2 \cong \mathbb{Z}_2$

$\sqrt{2} \mapsto \pm\sqrt{2}$

$G \cong \mathbb{Z}_3 \times \mathbb{Z}_2$

a	a	a	b	a	b	a	c	a	c
b	b	b	a	b	c	b	a	b	b
c	c	c	c	c	a	c	b	c	a

$\boxed{N21\,Q2}$

Let G be a gp. ~~Denote $Z(G)$~~

(a) Show that if $G/Z(G)$ is cyclic then G is abelian

Sup $G/Z(G)$ is cyclic. Let $a, b \in G$.

$\therefore \; = \langle gZ(G) \rangle$

Then $a = g^k z$ f.s. $z \in Z(G)$ & $k \in \mathbb{Z}^+$

$b = g^l z'$

$$ab = g^k z(g^l z') = g^k g^l z' z$$
$$= g^l g^k z' z$$
$$= g^l z' g^k z$$
$$= ba$$

(b) Show if $Aut(G)$ is cyclic then G is abelian.

$G/Z(G) \cong \leq Aut(G)$

If $Aut(G)$ is cyclic every subgp is cyclic. So $G/Z(G)$ is cyclic. So by part (a), G is abelian.

(c) Show if G is abelian & $|G|>2$, then G has an aut of order 2.

$\varphi: G \to G$ $\quad \varphi(a) = a^{-1}$ has order 2

if $a^2 \neq 1$ $\forall a \in G$.

If $a^2 = 1$ $\forall a \in G$ then $G \cong \mathbb{Z}_2^m$ $\quad m>1$
& G finite (if infinite $m=\infty$) $\quad \uparrow$ since $|G|>2$

$= \langle a_1 \rangle \times \cdots \times \langle a_m \rangle$

$\varphi: G \to G$

$a_1 \longmapsto a_2$
$a_2 \longmapsto a_1$ $\quad \leftarrow$ order 2
$a_i \longmapsto a_i, 2<i\leq m$

(d) Deduce that no grp of size >2 has a cyclic aut grp of odd order.

By part (c)
if G is abelian then $\text{Aut}(G)$ has an element of order 2 so $2 \mid |\text{Aut}(G)|$. So $|\text{Aut}(G)|$ can't be odd.

If G nonabelian, sup $\text{Aut}(G)$ is cyclic of odd order.

By part (b) then G is abelian. $\rightarrow\leftarrow$

J21Q5

Let F be a finite field of odd char. Find the number of elements of F that are squares of elements of F.

$F \cong \mathbb{F}_{p^n}$ for some odd p.

$\forall\ x \in F$

In $\mathbb{F}_p$ $\quad x = a^2 \qquad a^p = a \qquad a^{\varphi(p)} = 1$

F is a finite field so $F^\times$ is cyclic. of order $p^n - 1$

$\cancel{\varphi(p^n) = p^{n-1}(p-1)}$

$F^\times = \langle a \rangle$

then every even power of a is a square of an element of F.

Thus there are $\frac{p^n - 1}{2} + 1$

many plus 1 since $0 = 0^2$.

$$\frac{p^n - 1 + 2}{2} = \frac{p^n + 1}{2}$$

J21Q6

Let $f(x) = x^4 - 2 \in \mathbb{Q}[x]$ and let $\alpha \in \mathbb{C}$ st $f(\alpha) = 0$.
Let $K = \mathbb{Q}(\alpha)$

(a) Show that $f(x)$ is irr over $\mathbb{Q}$ & the extension $K/\mathbb{Q}$ is not normal.

~~$f(x)$ is irreducible over $\mathbb{Q}$ by eisenstein $p=2$~~ ok

$K/\mathbb{Q}$ is not normal b/c $K = \mathbb{Q}(\alpha)$ is not the splitting field of f

$\pm\sqrt[4]{2}$ $\pm i\sqrt[4]{2}$ are the roots

if $\alpha = \pm\sqrt[4]{2}$ can't get $\pm i\sqrt[4]{2}$

& vice versa.

(b) $\mathbb{Q}(\sqrt[4]{2}, i)$ deg 8

$$\begin{array}{c} \mathbb{Q}(\sqrt[4]{2}, i) \\ | \\ \mathbb{Q} \end{array}$$

$\sigma = \sqrt[4]{2} \longmapsto i^a \sqrt[4]{2}$ $0 \le a \le 3$

$\tau = i \longmapsto \pm i$