

1. (a) We should have  $|X| = \sum_{i=1}^r |O_i|$ ,  $O_i$  are orbits, since  $|G| = |G_s||O_i|$  where  $G_s$  is the corresponding stabilizer,  $|O_i| = 1, 3, 9$  or  $27$ . then there are at least 2  $O_i$ 's such that  $|O_i|=1$  since  $|X|=50 \equiv 2 \pmod{3}$

(b)  $0 \rightarrow A \hookrightarrow B \xrightarrow{f} C \rightarrow 0$  is exact, regard  $A$  as a subgroup of  $B$

then  $C \cong B/\ker f = B/\text{Im } f = B/A$ , thus  $A \trianglelefteq B$  and  $|B| = [B:A] |A| = |B/A| |A| = |A| |C| = 1350 = 2 \times 3^3 \times 5^2$ , thus has a Sylow subgroup  $D$  of order  $27$ , since  $(27, 50) = 1$ ,  $D \cap A = 1$ ,  $f(D) = C$

(c) If  $A$  is abelian, then  $A \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$  or  $A \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$ , thus  $H := \mathbb{Z}/2\mathbb{Z} \trianglelefteq A \trianglelefteq B$ , let  $h$  denote 1 in  $H = \mathbb{Z}/2\mathbb{Z}$ , then  $\forall b \in B, bhb^{-1} \in A$  with order 2 which are only be  $h$  itself, thus  $1 \neq h \in Z(B)$  is non-trivial

2. (a) Assume  $a_1 \in S = \{a_1, \dots, a_n\} \subseteq F$  is not a root of unity, then  $a_1^n \neq a_1^m$ ,  $\forall n \neq m$ , otherwise  $a_1^{n-m} = 1$ , hence  $a_1 \mapsto a_1^m \mapsto a_1^{m^2} \mapsto \dots$  would generate infinitely many different elements which is a contradiction

(b) Since  $M \in GL_n(\mathbb{C})$ , assume the characteristic polynomial of  $M$  is  $(t-\lambda_1) \cdots (t-\lambda_n)$ , then the characteristic polynomial of  $M^m$  is  $(t-\lambda_1^m) \cdots (t-\lambda_n^m)$ , since  $M^m$  are similar to  $M$ , they have the same characteristic polynomials, then apply result in (a). with  $F = \mathbb{C}$ ,  $S = \{\lambda_1, \dots, \lambda_n\}$

3.  $\forall x \frac{a}{b} \in xR_\pi \cap R$ , then  $b|x$ , since  $(b, \pi) = 1$ ,  $b\pi^r|x$ , hence  $x \frac{a}{b} = \pi^r \frac{x}{b\pi^r} a \in \pi^r R$ ,

Conversely,  $\forall \pi^r a \in \pi^r R$ ,  $\pi^r a = x \frac{a}{\pi^r} \in xR_\pi \cap R$

4. (a) I get to be send to  $\bigoplus_{i \in F} M_i$  for some finite subset  $F$  of  $I$ , so is the image of  $R$

(b) Since  $J \rightarrow \bigoplus_{i=1}^{\infty} J/J_i \hookrightarrow \bigoplus_{i=1}^{\infty} M_i$  and  $\bigoplus_{i=1}^{\infty} M_i$  is injective, there is an extension  $R \rightarrow \bigoplus_{i=1}^{\infty} M_i$ , by (a),  $\exists N$  such that  $\bigoplus_{i \leq N} M_i$  contains the image of  $R$ , hence the image of  $J$

(c) From (b), we know  $\bigoplus_{i \leq N} J/J_i$  contains the image of  $J$ , thus  $J_i = J \ \forall i \geq N$  therefore  $R$  is Noetherian

5. (a)  $x^{10} + \dots + 1$  is irreducible over  $\mathbb{Q}[x]$ , thus  $1, \zeta, \dots, \zeta^9$  are linearly independent over  $\mathbb{Q}$ , hence for any 10 elements of  $S$  could be transform into  $1, \dots, \zeta^9$  by multiplying  $\zeta^k$  for some  $k$

(b)  $2 \in (\mathbb{Z}/11\mathbb{Z})^\times$  is a generator corresponding to  $\sigma$ , then  $\sigma(\alpha) = \zeta^2 + \zeta^6 + \zeta^8 + \zeta^{10} + \zeta^7 \neq \alpha$  since they are linearly independent, thus  $\alpha \notin \mathbb{Q}$

(c) Notice  $\sigma^2(\alpha) = \alpha$ ,  $|\text{Aut}(\mathbb{Q}(\beta)/\mathbb{Q}(\alpha))| = |\{1, \sigma^2, \sigma^4, \sigma^6, \sigma^8\}| = 5$  by Galois Correspondence theorem, we have  $[\mathbb{Q}(\alpha):\mathbb{Q}] = [\text{Aut}(\mathbb{Q}(\beta)/\mathbb{Q}):\text{Aut}(\mathbb{Q}(\beta)/\mathbb{Q}(\alpha))] = 2$

6. (a) Suppose  $\rho$  is not injective, denote  $\ker \rho = H$ ,  $\bar{\rho}: G/H \rightarrow GL_n(\mathbb{C})$  is a representation, but then  $G/H$  is abelian,  $\bar{\rho}$  is completely reducible to a direct sum of representations of degree one,  $\rho$  is not irreducible which is a contradiction

(b) Consider  $H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}$ ,  $K = \{-1, 1\}$ ,  $G := H \times K$

$\rho: G \rightarrow GL_2(\mathbb{C})$  via quotient map  $H \times K \rightarrow H \times K/K \cong H \leqslant GL_2(\mathbb{C})$

Then this is a irreducible representation which is not injective

1. (a)  $\forall \sigma \in \text{Aut}(N)$ ,  $\sigma(aba^{-1}b^{-1}) = \sigma(a)\sigma(b)\sigma(a)^{-1}\sigma(b)^{-1} \in N'$ , hence  $N'$  is a characteristic subgroup of  $N$ , thus  $N' \trianglelefteq G$

(b) Since  $G$  is solvable, so is  $N$ , consider  $I = N_0 \trianglelefteq N_1 \trianglelefteq \dots \trianglelefteq N_{r-1} \trianglelefteq N_r = N$  with  $N_{i+1}/N_i$  abelian, thus  $N' \leq N_{r-1}$ , but  $N' \trianglelefteq G$  and  $N$  is minimal, hence  $N'$  can only be  $I$ , thus  $N = N/N'$  is abelian

(c) Since  $N$  is abelian, finite and minimal,  $|N| = p^r$ , and  $N \cong (\mathbb{Z}/p\mathbb{Z})^r$  otherwise,  $N$  would have some nontrivial proper characteristic subgroup which would be a normal subgroup of  $G$ , contradicts the minimality of  $N$

2. Take the basis of  $V$  such that the matrix of  $T$  is of Jordan canonical form, consider the following simple case  $T = \begin{pmatrix} \lambda & 1 & & \\ & \ddots & & \\ & & \lambda & \\ & & & \lambda \end{pmatrix}$ , then

$\text{rank}(T) = \begin{cases} n, & \lambda \neq 0 \\ n-1, & \lambda = 0 \end{cases}$ ,  $\text{rank}(I-T) = \begin{cases} n, & \lambda \neq 1 \\ n-1, & \lambda = 1 \end{cases}$ , hence  $\text{rank}(T) + \text{rank}(I-T) \leq 2n$ . else, thus  $\text{rank}(T) + \text{rank}(I-T) = n$  iff  $n=1$ ,  $\lambda=0$  or  $1$ , therefore,

$\text{rank}(T) + \text{rank}(I-T) \geq \dim V$ , equality holds iff  $T = \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}$  then  $T^2 = T$

3. (a) Irreducible elements are prime elements in a UFD

(b)  $0 \neq P \subsetneq R$  is a prime ideal, then  $\exists 0 \neq a \in P$ ,  $a = \pi_1 \cdots \pi_k$  a product of irreducible elements, then one of  $\pi_k$  and  $\pi_1 \cdots \pi_{k-1}$  must belongs to  $P$ , by induction we know  $P$  contains a prime ideal of the form  $\pi R$  for some irreducible  $\pi$ .

(c) Suppose  $m \subsetneq R$  is a nonzero maximal ideal, then it's also prime, by (b),  $\pi R \subseteq m$  for some irreducible  $\pi$ , but then  $\pi R$  is a prime thus maximal ideal, hence  $m = \pi R$ . namely every maximal ideal is a prime ideal. Since  $I := \langle S \rangle \subsetneq R$ ,  $I \subseteq m = \pi R$  for some maximal ideal, thus there is an irreducible  $\pi$  such that  $\pi$  divides  $r_i$  for all  $i$

(d)  $0 \neq I \subsetneq R$  is an ideal, suppose  $S := \{r_i\}_{i \in I}$  is a set of generators, then by (c),  $\exists \pi$  divides  $r_i$ , then let  $S' := \{r'_i = \frac{r_i}{\pi}\}_{i \in I}$ ,  $\langle S \rangle = \pi \langle S' \rangle$  continue doing so until one of  $r_i$  becomes 1, thus  $\langle S \rangle = \pi^k R$  which is principle

4. (a)  $GF(x) = G(f_1(x), \alpha(x)) = \beta f_1(x) - f_2 \alpha(x) = 0$ . Conversely, if  $(P, k) \in \text{Ker } G$ , then  $g_2 \beta(P) = g_2 f_2(k) = 0$ , hence  $\text{id}_M g_1(P) = g_2 \beta(P) = 0 \Rightarrow g_1(P) = 0 \Rightarrow \exists x \in K_1$ , such that  $f_1(x) = P$ , then  $f_2 \alpha(x) = \beta f_1(x) = \beta(P) = f_2(k)$ , since  $f_2$  is injective,  $\alpha(x) = k$ , hence  $F(x) = (f_1(x), \alpha(x)) = (P, k)$ ,  $0 \rightarrow K_1 \xrightarrow{F} P_1 \oplus P_2 \xrightarrow{G} P_2 \rightarrow 0$  is exact

(b) Since  $P_2$  is projective,  $K_2 \oplus P_1 \cong K_1 \oplus P_2$ , namely the exact sequence splits

(c) Suppose  $A \oplus B = \langle (a_1, b_1), \dots, (a_n, b_n) \rangle$ , then  $\forall a \in A$ ,  $(a, 0) = r_1(a_1, b_1) + \dots + r_n(a_n, b_n) = (r_1 a_1 + \dots + r_n a_n, r_1 b_1 + \dots + r_n b_n) \Rightarrow a = r_1 a_1 + \dots + r_n a_n$ , thus  $A = \langle a_1, \dots, a_n \rangle$

(d) There should be a commutative diagram involving two exact sequences

$$\begin{array}{ccccccc} 0 & \rightarrow & K & \rightarrow & P & \rightarrow & R/I \rightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \rightarrow & I & \rightarrow & R & \rightarrow & R/I \rightarrow 0 \end{array} \quad \text{where } R \text{ is evidently finitely generated and free hence projective}$$

If both  $K$  and  $P$  are finitely generated and  $P$  is projective, then by (b) and (c)  $P \oplus I \cong K \oplus R$  is finitely generated, hence so should  $I$  which is a contradiction

5. You can draw a picture easily showing the subgroups

(a) Subextensions  $F/\mathbb{Q}$  such that  $[F:\mathbb{Q}]$  corresponds to

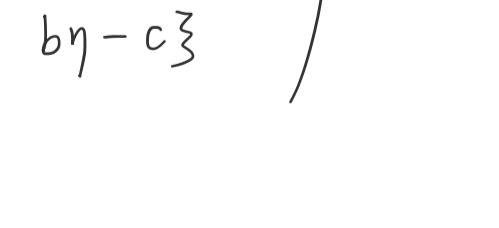
subgroups of order 4

(b)  $c$  corresponds to  $-1$  since it's the only element of order

2 and  $\bar{z} = z \forall z \in C$ , thus we can take  $\sigma$  to be  $i$

(c) By (a) we know that  $\text{Aut}(L/F) = \{1, -1, i, -i\}$  or  $\{1, -1, j, -j\}$  or  $\{1, -1, k, -k\}$

hence  $c$  acts trivially on  $F$



6. In order to decide how many trivial representations  $\tilde{\rho}$  contains. We need to decide the dimension of  $\bigcap_{g \in G} \text{Ker}(\rho(g)M\rho(g)^{-1}) = \bigcap_{g \in G} \text{Ker}(\rho(g)M - M\rho(g))$

Since  $\rho(g)^k = 1$ , thus each  $\rho(g)$  is diagonalizable,

$$\text{And } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \lambda & \bar{z} \\ \bar{z} & \mu \end{pmatrix} - \begin{pmatrix} \lambda & \bar{z} \\ \bar{z} & \mu \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} b\bar{\eta} - c\bar{z} & \bar{z}(a-d) - b(\bar{\lambda}-\bar{\mu}) \\ c(\bar{\lambda}-\bar{\mu}) - \bar{\eta}(a-d) & b\bar{\eta} - c\bar{z} \end{pmatrix} = 0 \iff$$

$$\begin{cases} b\bar{\eta} = c\bar{z} \\ b(\bar{\lambda}-\bar{\mu}) = \bar{z}(a-d) \\ c(\bar{\lambda}-\bar{\mu}) = \bar{\eta}(a-d) \end{cases}$$

(a) If  $\rho$  is irreducible, then find a basis such that  $\rho(g) = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ ,  $\lambda \neq \mu$ , for some  $g$ , we get  $b=c=0$ , but since  $\rho$  is irreducible, on this basis,  $\exists g \neq h \in G$ , such that  $h$  is not a diagonal matrix, which means  $\bar{z}, \bar{\eta}$  are not both zeros, hence  $a=d$ , thus  $\tilde{\rho}$  contains the trivial representation exactly once.

(b) If  $\rho$  is the sum of two distinct one-dimensional representations, then on some basis and for some  $g$ ,  $\rho(g) = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$  and  $\rho(h)$ ,  $\forall h \in G$  are all diagonal matrices, by analysis in (a), we know that  $\tilde{\rho}$  contains the trivial representation exactly twice

(c) If  $\rho$  is the sum of two equal one-dimensional representations, then on any basis,  $\forall g \in G$ ,  $\rho(g)$  are scalar matrices, thus  $\tilde{\rho}$  equals the sum of four copies of the trivial representation

2012 January

Saturday, January 12, 2019 12:38

2. For any  $A \in S$ , since  $A$  is nilpotent,  $\text{Ker}A \neq 0$ , but if  $\text{Ker}A = \mathbb{C}^n$ , then  $A=0$  which can be ignored, pick  $A \neq 0$ , then since  $AB=BA, \forall A, B \in S$ , we have  $A(B(\text{Ker}A)) = B(A(\text{Ker}A)) = 0 \Rightarrow B(\text{Ker}A) \subseteq \text{Ker}A, \forall B \in S$ , thus find a basis for  $\text{Ker}A$ , then  $B = \begin{pmatrix} B_1 & B_2 \\ 0 & B_3 \end{pmatrix}, \forall B \in S$ , since

$$BC = \begin{pmatrix} B_1 & B_2 \\ 0 & B_3 \end{pmatrix} \begin{pmatrix} C_1 & C_2 \\ 0 & C_3 \end{pmatrix} = \begin{pmatrix} B_1C_1 & B_1C_2 + B_2C_3 \\ 0 & B_3C_3 \end{pmatrix} = \begin{pmatrix} C_1B_1 & C_1B_2 + C_2B_3 \\ 0 & C_3B_3 \end{pmatrix} = CB, \quad \begin{cases} B_1C_1 = C_1B_1, \\ B_3C_3 = C_3B_3 \end{cases}$$

similarly we have  $B_1, B_3$  are nilpotent

Then we should use induction to continue this process

1. Since  $N \not\subset Z(G)$  and  $|N|=3$ ,  $N \cap Z(G)=1$ , consider the group action by conjugation, since  $N$  is a normal subgroup, assume  $N=\{1, \alpha, \alpha^2\}$ , then  $g\alpha g^{-1}=\alpha$  or  $\alpha^2$ , if  $\forall g \in G$ ,  $g\alpha g^{-1}=\alpha$ , then  $\alpha \in Z(G)$  which is impossible, thus  $\{\alpha, \alpha^2\}$  is an orbit, then the stabilizer of  $\alpha$   $H$  is a subgroup such that  $[G:H]=2$

2. (a) Since  $\text{rank}(A)=1$ ,  $A\vec{1}=n\vec{1}$ , thus  $\text{ch}_A(x)=x^{n-1}(x-n)$

(b)  $m_A(x) | x(x-n)$ , hence  $m_A(x)=x(x-n)$ , thus the Jordan normal form is  $\begin{pmatrix} n & & \\ & 0 & \\ & & \ddots & 0 \end{pmatrix}$

$$3. (a) \frac{a}{b} \otimes \frac{c}{d} = \left(d \frac{a}{bd}\right) \otimes \left(c \frac{1}{d}\right) = cd \left(\frac{a}{bd}\right) \otimes \frac{1}{d} = \left(c \frac{a}{bd}\right) \otimes \left(d \frac{1}{d}\right) = \frac{ac}{bd} \otimes 1$$

$$(b) \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q} \otimes_{\mathbb{Z}} 1 \cong \mathbb{Q}$$

4. Let  $\Sigma = \{I \subseteq R \text{ ideal} \mid I \text{ doesn't contain any product of prime ideals}\}$ , Suppose  $\Sigma$  is not empty, since  $R$  is Noetherian,  $\Sigma$  has a maximal element  $J$ , evidently  $J$  itself can't be prime, by suppose  $x, y \notin J$ , then  $J \subsetneq J+(x)$  contains a product of primes, so is  $J+(y)$ , by then so does  $J+(xy) = (J+(x))(J+(y))$ , hence  $xy \notin J$ , namely  $J$  is prime which is a contradiction

5. (a) Suppose  $2 \leq \deg f \leq 4$ , then consider  $A_5$  acts on its roots, thus there is a homomorphism  $A_5 \rightarrow S_n$  where  $n = \deg f$ , since  $60 = |A_5| > |S_n|$ , thus the kernel will be a nontrivial normal subgroup of  $A_5$  which then can only be  $A_5$  itself since  $A_5$  is a simple group, but then  $A_5$  acts trivially on roots of  $f$  which is a contradiction

(b) Consider the subgroup  $H$  generated by  $(1\ 2\ 3)$ , then  $|H|=3$ , hence the intermediate field  $F$  fixed by  $H$  satisfies  $[K:F]=[H]$ , thus  $[F:\mathbb{Q}]=20$ , since  $\mathbb{Q}$  is a characteristic 0, there is a primitive element  $\alpha \in F$  such that  $F = \mathbb{Q}(\alpha)$  then the minimal polynomial  $g(x) \in \mathbb{Q}[x]$  is of degree 20 and irreducible

6. (a) Normal subgroup should consist of conjugacy classes, try the computation would show that  $G$  is simple, but since  $G$  has irreducible representations of degree  $> 1$ , thus  $G$  is not abelian, hence  $G$  is not solvable

**Remark:** The number of irreducible degree 1 complex representations is  $1=|G/G'|$ , hence  $G=G'$ ,  $G$  can't be solvable

(b) Consider the irreducible representations of  $G$  of deg 3, shows there is a homomorphism from  $G \rightarrow GL_3(\mathbb{C})$  which is not trivial, thus must be injective

**Remark:** From  $\chi_2$  or  $\chi_3$ , we know the corresponding representations are injective

(c) Notice any two subgroups of order 3 intersects at identity, hence the number of order 3 elements must be even, from  $\chi_2$  we see that  $\zeta_1 + \zeta_2 + \zeta_3 \neq \frac{-1 \pm \sqrt{7}i}{2}$ ,  $\forall \zeta_1, \zeta_2, \zeta_3 \in \{1, \omega, \omega^2\}$ , thus the number of order 3 elements could only be 42, the number of order 3 subgroups is then 21

**1. (a)** Let  $|K|=j$ , then  $|G|:=n=ij$ ,  $(i,j)=1$ , since  $K$  is normal,  $|G/K|=i$ , hence  $\forall x \in G$ ,  $\overline{x^i} = \overline{x}^i = 1 \Rightarrow x^i \in K$ . Also, since  $(i,j)=1$ ,  $ai+bj=1$  thus  $\forall x \in K$ ,  $1=x^{bj}=x^{-ai} \Rightarrow x=x^{ai}$ , therefore  $K=\{x^i \mid x \in G\}$

**(b)** Consider  $G=S_3$ ,  $K=\{\text{id}, (1 2)\}$  which is not a normal subgroup,  $|K|=2$ ,  $[G:K]=3$  are relatively prime, but  $(2 3)^3=(2 3) \notin K$

**2.** Since  $T^2=T$ , its Jordan canonical form should be  $\begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}$ , but then  $I-\alpha T = \begin{pmatrix} (1-\alpha)I & 0 \\ 0 & I \end{pmatrix}$  which is invertible provided  $\alpha \neq 1$

**3. (a)** Consider  $(x^2+1)(x^4-x^2+1)=x^6+1$  in  $\mathbb{Z}[x]/I$  shows that  $\mathbb{Z}[x]/I$  is not an integral domain, hence  $I$  is not prime

**(b)** Consider  $B=(3, X)$ ,  $A=(3)$ , since 3 is an irreducible element in  $\mathbb{Z}[X]$ ,  $A$  is prime,  $\mathbb{Z}[x]/B \cong \mathbb{Z}/3\mathbb{Z}$  which is a field,  $B$  is maximal hence prime, also  $A \subset I \subset B \subset \mathbb{Z}[x]$

**4.** Let  $F=R_{e_1}+\dots+R_{e_n}$  be a finitely generated  $R$ -module, if  $F$  is flat, then

$\forall I \subseteq R$ ,  $0 \rightarrow I \hookrightarrow R$  is exact, so is  $0 \rightarrow I \otimes_R F \hookrightarrow R \otimes_R F$ , but  $I \otimes_R F \cong IF$ ,  $R \otimes_R F \cong F$ ,

hence  $IF \hookrightarrow F$  is an inclusion, now suppose  $r \in R$  is not a zero divisor and

$rf=0$  for  $f \in F$ , Let  $I=Rr$ , we know that  $f=0$  which shows that  $F$  is torsion

free. Conversely, if  $F$  is torsion free,  $R \cong Re_1$ , hence

$\forall M \hookrightarrow N$ ,  $M \otimes Re_1 \cong M \otimes R \cong M \hookrightarrow N \cong N \otimes R \cong N \otimes Re_1$ , thus  $M \otimes F = M \otimes (Re_1 + \dots + R_{e_n})$

$\cong M \otimes Re_1 + \dots + M \otimes R_{e_n} \hookrightarrow N \otimes Re_1 + \dots + N \otimes R_{e_n} \cong N \otimes (Re_1 + \dots + R_{e_n}) = N \otimes F$

Thus  $F$  is flat

**5. (a)** Since  $K/\mathbb{Q}$  is Galois,  $|G|=[K:\mathbb{Q}]=21$ , and  $G$  is non-abelian, use Sylow's theorems, we know that  $G$  has only one normal subgroup of order 7, and 7 subgroups of order 3, it is obvious that the splitting field of  $f(x)$  denoted by  $L$  is contained in  $K$ , and since  $f$  is irreducible,  $[L:\mathbb{Q}] \geq 7$ , thus  $H:=\text{Gal}(K/L) \cong G$  with  $|H| \leq 3$ , thus  $H$  can only be the trivial group and  $L=K$

**(b)** According to Sylow's theorems, we know that all 7 subgroups of order 3 are conjugate to each other, hence there are 7 distinct fields  $F_i$ ,  $1 \leq i \leq 7$  with  $\mathbb{Q} \leq F_i \leq K$ ,  $[F_i:\mathbb{Q}]=7$ , let  $H_i = \text{Gal}(K/F_i)$ , then  $\exists g \in G$  such that  $g^{-1}H_1g = H_2$  thus  $\forall \sigma \in G$ , such that fixes  $g(F_1)$  means  $g\sigma g^{-1}$  fixes  $F_1 \Leftrightarrow g\sigma g^{-1} \in H_1 \Leftrightarrow \sigma \in g^{-1}H_1g = H_2$ , hence  $g(F_1) = F_2$

**(c)** Since  $\mathbb{Q}(\alpha_i) \cong \mathbb{Q}[x]/(f(x))$ ,  $[\mathbb{Q}(\alpha_i):\mathbb{Q}]=7$ , consider  $G$  acting on  $\{\alpha_1, \dots, \alpha_7\}$  transitively, with stabilizer of order 3, thus  $\text{Gal}(K/\mathbb{Q}(\alpha_i))$  corresponds to those subgroups of order 3, and thus  $\mathbb{Q}(\alpha_i)$  are exactly  $F_i$ 's

**6. (a)** Consider  $T: G \rightarrow G$  by sending elements to its inverses, which is a permutation of order 2,  $T^2=T$ , hence  $\forall r = \sum \beta_i g_i \in R$ , we have  $P_2(g) \circ T(r) = \sum \beta_i P_2(g) \circ T(g_i) = \sum \beta_i P_2(g)(g_i^{-1}) = \sum \beta_i gg_i^{-1}$ , and on the other hand  $T \circ P_1(g)(r) = \sum \beta_i T \circ P_1(g)(g_i) = \sum \beta_i T(g_i g_i^{-1}) = \sum \beta_i gg_i^{-1}$ , thus  $P_2$  and  $P_1$  are equivalent

**(b)**  $P_1(g)$  always takes elements of  $G$  to its conjugates, particularly,  $C_1$  will be a  $G$ -invariant subspace,  $P_2(g)$  act on  $G$  as permutations, thus always irreducible, but  $P_1$  is irreducible only if  $G$  is trivial. Conversely, if  $G$  is trivial,  $P_1$  and  $P_2$  are both trivial hence equivalent

**(c)** Consider  $\varphi: G \rightarrow G$ ,  $g \mapsto g^2$  which is a homomorphism since  $G$  is abelian. If  $P_2$  and  $P_4$  are equivalent, and  $P_2$  is faithful, so is  $P_4$ , but if  $G$  has even order, then  $P_4 = P_2 \circ \varphi$  won't be faithful. Conversely, If  $G$  has odd order, then  $\varphi$  would be an isomorphism since 2 and  $|G|$  are relatively prime. Hence  $P_4$  and  $P_2$  are both irreducible and of degree  $|G|$ , hence they are equivalent

1. (a)  $|B| = 85 \times 9 = 5 \times 17 \times 3^2$ , thus  $B$  has a subgroup of order 9, denoted  $H$ , then  $H \cap A = 1$ ,  $g(H) = C$

(b) By Sylow's theorems,  $A \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}$ , thus  $|\text{Aut}(A)| = 64$ , by sending  $(1, 0)$  to  $(n, 0)$ ,  $1 \leq n \leq 4$ , and  $(0, 1)$  to  $(0, m)$ ,  $1 \leq m \leq 16$  independently

(c) Consider  $B$  acts on  $A$  by conjugation, which would induce a homomorphism  $B \rightarrow \text{Aut}(A)$ , and  $A$  is in the kernel since it's abelian, thus  $B$  is the kernel, hence  $A \leq Z(B)$ , thus elements of  $A$  and  $H$  commutes, hence  $B \cong A \times H$  thus abelian since  $H$  is also abelian

2. (a) Notice  $M^n = I$ , and  $x^n - 1 = 0$  has  $n$  different roots, thus its characteristic and minimal polynomials are both  $x^n - 1$

(b) Let  $N = J + K$ , where  $J = \begin{pmatrix} 0 & 1 & & \\ & 0 & \cdots & \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix}$ ,  $K = \begin{pmatrix} 0 & & & \\ & 0 & \cdots & \\ & & \ddots & 0 \\ & & & 0 \end{pmatrix}$ , then  $JK = KJ = K^2 = 0$ , thus  $(J+K)^n = J^n$ , hence  $N^n = 0$  and  $N^{n-1} \neq 0$ , therefore, its characteristic and minimal polynomials are both  $x^n$

3. (a) Notice  $C = C/M$  is a  $R$ -module, verify that  $M \times M \rightarrow C$  sending  $(f, g)$  to  $\frac{\partial f}{\partial X}(0, 0) \frac{\partial g}{\partial Y}(0, 0)$  is an  $R$ -bilinear map, thus induce  $M \otimes_R M \rightarrow C$  an  $R$ -homomorphism which is also the well-defined map of vector spaces over  $C$

(b) Consider the image of  $Z$  in  $M \otimes_R M \rightarrow C$  which would be  $1 \neq 0$  thus  $Z \neq 0$  in  $M \otimes_R M$

(c) Consider  $r = XY \neq 0$  in  $R$ , but  $rz = (XY)(X \otimes Y - Y \otimes X)$   
 $= (XY) \otimes (XY) - (XY) \otimes (XY) = 0$

4. (a) We only need to show that if  $I \cap J \subseteq P$ , so is one of  $I$  or  $J$ .

Suppose not,  $\exists i \in I \setminus P, j \in J \setminus P$ , but  $ij \in IJ \subseteq I \cap J \subseteq P$  which is a contradiction

(c) Suppose there is another minimal prime ideal  $P$ , then  $m_1 \cap \dots \cap m_n = (0) \subseteq P$  which by (a) implies one of  $m_i \subseteq P$  since  $P$  is minimal,  $P = m_i$

5. Since each extension  $K_{i+1}/K_i$  is Galois and of degree 3, thus  $K_n/\mathbb{Q}$  is also Galois and of degree of a power of 3, but if  $\mathbb{Q}(\sqrt[3]{2}) \subseteq K_n$ , then  $K_n$  contains the splitting field of  $\sqrt[3]{2}$  denoted by  $L$ , but then  $L/\mathbb{Q}$  is Galois but of degree 6 which leads to a contradiction

$K_n/\mathbb{Q}$  is of degree of a power of 3

1. (a) By Sylow's theorems, since  $H$  is not normal,  $H$  can only have exactly 7 conjugates including itself

(b) Consider  $G$  acts on  $H$  by conjugation induces a homomorphism  $\phi: G \rightarrow S_7$ .  $\ker \phi = \cap \text{stabilizers } \leq H$ , and  $\ker \phi \neq H$ ,  $|H| = p^2$ ,  $|\ker \phi| = 1 \text{ or } p$ , thus  $p$  divides  $|\text{Im } \phi|$

2. (a) Suppose the characteristic polynomial  $ch(t) = f(t)g(t)$  is reducible over  $F$ , then we know  $\{v, T v, \dots, T^{n-1} v\}$  is a basis of  $V$  for any  $v \neq 0$  assuming  $\dim V = n$ , then for some  $v \neq 0$  we have  $w = g(T)v \neq 0$ , but then  $f(T)w = f(T)g(T)v = ch(T)v = 0$  which is a contradiction

(b) Suppose  $v \neq 0$  is not a cyclic vector for  $T$ , namely,  $Tv = \lambda v$  for some  $\lambda \in F$  which is a contradiction since  $ch(t)$  is irreducible

3. If  $0 = f^N = a_0^N + g(x)x, g \in R[[x]] \Rightarrow a_0^{N_0} = 0$  then we have  $(f - a_0)^{2N_0} = 0$  since in the expansion every term contains a power of either  $f$  or  $a_0$  which  $\geq N_0$ , thus  $(f - a_0)^{2N_0} = X^{2N_0} h^{2N_0} = 0 \Rightarrow h^{2N_0} = 0 \Rightarrow a_1^{2N_0} = 0$ , thus make an induction.

Conversely, If  $a_n^{N_n} = 0$ , then consider ideals  $I_n = (a_0, \dots, a_n)$ ,  $I_0 \subseteq \dots \subseteq I_n$  is an ascending chain, thus  $I_k = I_{k+1} = \dots$ , hence  $a_{k+1}, a_{k+2}, \dots$  can be generated by  $a_0, \dots, a_k$ , suppose  $a_0^M = \dots = a_k^M = 0$ ,  $a_j = r_{j0}a_0 + \dots + r_{jk}a_k$ . Let  $N = (k+1)M$  then coefficients of the monomials in the expansion has a power at least of order  $M$  on one of  $\{a_0, \dots, a_k\}$ , thus  $f^N = 0$

4. Suppose  $\{v_1, \dots, v_n\}, \{w_1, \dots, w_m\}$  are base for  $V$  and  $W$  correspondingly, and let  $\{v_i^*, \dots, v_n^*\}$  be a dual basis such that  $\langle v_i, v_j^* \rangle = v_j^*(v_i) = \delta_{ij}$ , let  $\{\zeta_{ij} \in \text{Hom}(V^*, W)$  such that  $\zeta_{ij}(v_k^*) = \delta_{ik}w_j$ , then  $\zeta_{ij}$  form a basis for  $\text{Hom}(V^*, W)$ , since  $\dim V \otimes W = \dim \text{Hom}(V^*, W) = nm$ , we only need to show that  $\phi$  is surjective, but notice  $\phi(v_i \otimes w_j)(v_k^*) = v_k^*(v_i)w_j = \delta_{ik}w_j$ , thus  $\phi(v_i \otimes w_j) = \zeta_{ij}$

5. (a) Notice that  $u - v = (r_1 - r_4)(r_3 - r_2)$ , since  $f$  is irreducible over  $\mathbb{Q}$  which has characteristic 0,  $r_1, r_2, r_3, r_4$  must be distinct, thus  $u \neq v$

(b)  $g(x)$  is invariant under  $S_4$ , hence coefficients of  $g$  are symmetric in  $r_1, r_2, r_3, r_4$ , hence  $\in \mathbb{Q}$

(c)  $u, v, w \notin \mathbb{Q}$ , otherwise it would be invariant under  $S_4$ , then some two of them must be equal which contradicts (a). subsequently  $g(x)$  is irreducible, otherwise would have some as root in  $\mathbb{Q}$

(d) Consider  $(1 \ 2), (1 \ 2 \ 3) \in S_4$  induce  $(u \ v), (u \ w \ v) \in S_3$ , and  $\text{Gal}(\mathbb{Q}(u, v, w)/\mathbb{Q}) \leq S_3$ , hence  $\text{Gal}(\mathbb{Q}(u, v, w)/\mathbb{Q}) = S_3$

6. (a)  $1^2 + 1^2 + 1^2 + a^2 = 12 \Rightarrow a = 3$ , Assume  $|C_2| = r_2, |C_3| = r_3, |C_4| = r_4$ , then from the orthogonal relation we know that

$$\begin{cases} 1 + r_2 + r_3 w^2 + r_4 w = 0 \\ 1 + r_2 + r_3 w + r_4 w^2 = 0 \end{cases} \Rightarrow r_3 = r_4, \text{ on the other hand, from the class equation we can deduce that } r_2 = 3, r_3 = r_4 = 4,$$

equation we can deduce that  $r_2 = 3, r_3 = r_4 = 4$ , then use orthogonal relation again, we have

$$\begin{cases} 3 + 3b + 4c + 4d = 0 \\ 3 + 3b + 4cw^2 + 4dw = 0 \\ 3 + 3b + 4cw + 4dw^2 = 0 \end{cases} \Rightarrow \begin{cases} b = -1 \\ c = 0 \\ d = 0 \end{cases}$$

(b) Since  $G$  has has only one orbit of size 3, hence it has a normal subgroup of order 4

(c) If  $G$  has a normal subgroup of order 2, then  $G$  should have two orbits of size 1 which is a contradiction

2016 August

Sunday, January 13, 2019 22:41

5. (a) Suppose  $f(x) = (x-\alpha_1)\cdots(x-\alpha_m)(x-\beta_1)\cdots(x-\beta_n) = hg$ , let  $S_1 = \{\alpha_1, \dots, \alpha_m\}$ ,  $S_2 = \{\beta_1, \dots, \beta_n\}$ ,  $S = S_1 \cup S_2$ ,  $L = K(S)$ ,  $G = \text{Aut}(L/\mathbb{Q})$ ,  $H = \text{Aut}(L/K)$ ,  $G/H \cong \text{Aut}(K/\mathbb{Q})$ . Since  $f$  is irreducible over  $\mathbb{Q}$ ,  $g, h$  are irreducible over  $K$ ,  $\exists \rho \in G$  such that  $\rho(\alpha_1) = \beta_1$ , hence  $0 = \rho(h(\alpha_1)) = \rho(h)(\beta_1) \Rightarrow g | \rho(h) \Rightarrow \deg g \leq \deg h$ , similarly consider  $\rho^7$  we have  $\deg h \leq \deg g$ , thus  $g = \rho(h)$ ,  $H$  acts on  $h$  trivially, thus induce  $\sigma = \rho H \in G/H \cong \text{Aut}(K/\mathbb{Q})$ , Therefore we have  $g = \sigma(h)$ .

(b) Consider  $K = \mathbb{Q}(\sqrt[3]{2})$ ,  $K/\mathbb{Q}$  is not Galois,  $f = x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4}) = hg$  which have different degrees.