Linear Representations of Finite Groups

This is my solution set of the *Linear Representations of Finite Groups*, Serre, 1977. This is based on the homework given in the lecture, Group representation, POSTECH. Since the lecture covered the chapters in the book from 1 to 12 except 4 and 5, this solution set contains the all exercises in those chapters. In fact, the lecture covered chapter 13 and 14, but it is too hard for me to solve the exercises as it is not my major, and I think it would be better to study latter chapters if I need it.

If time permits, I'll supplement the exercises in the chapter 4 and 5.

Reading guide: If you only know about the group, you will struggle to read after chapter 3. (The only advanced fact while chapter 3 is the advanced linear algebra.) If you are familiar with undergraduate abstract algebra, it will be easy to read the book and solution while you don't enter chapter 12. In chapter 12, some facts from commutative algebra is necessary, so I'll writes some fact in front of the solution at that chapter.

As the lecture also gave some exercises in the *Abstract Algebra*, Dummit and Foote, 3rd ed., I'll include some solutions about those exercises.

General notation

G will denote a group.

H will generally denote a subgroup of G.

g will denote the order of G, but sometimes denote an element in G; if you confused with it, it is my fault. By the same reason h will denote the order of H.

s,t will denote elements of G.

V,W will denote $\mathbb{F}$-vector space. $\mathbb{F} = \mathbb{C}$ in this paper; note that it may not be $\mathbb{C}$ after chapter 12.

ρ,η will denote group representations.

χ will denote group character.

D&F 10.4.2 As $\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$ is tensored by $\mathbb{Z}$,

$$2 \otimes 1 = 2 \cdot (1 \otimes 1) = 1 \otimes 2 = 1 \otimes 0. \tag{1}$$

Since

$$1 \otimes 0 + 1 \otimes 0 = 1 \otimes (0 + 0) = 1 \otimes 0, \tag{2}$$

$1 \otimes 0 = 0$, i.e. zero element in $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$.

D&F 10.4.3 Since $\mathbb{R}$ is a submodule of $\mathbb{C}$, $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is a $\mathbb{R}$-module.

I'll show that $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$ is isomorphic to $\mathbb{C}$ as a $\mathbb{C}$-module. Construct a map $\varphi : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ by $\varphi : (a, b) \mapsto ab$. Since this is $\mathbb{C}$-linear, there exists a well-defined $\mathbb{C}$-module homomorphism $\Phi : \mathbb{C} \otimes_{\mathbb{C}} \mathbb{C} \to \mathbb{C}$ factor thorugh φ. Note that if $1 \otimes a = 0$, then it means $a = 0$.

For any $\sum_{i=1}^{n} a_i \otimes b_i \in \mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$, we can make $\sum_{i=1}^{n} a_i \otimes b_i = \sum_{i=1}^{n} 1 \otimes a_i b_i = 1 \otimes (\sum_{i=1}^{n} a_i b_i)$, so any element in $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$ can be presented by $1 \otimes a$ for some $a \in \mathbb{C}$. Furthermore, this presentation

is unique as $1 \otimes a_1 = 1 \otimes a_2$ means $a_1 = a_2$. This argument shows that Φ is bijective, so it is a $\mathbb{C}$-module isomorphism. Note that Φ is indeed $\mathbb{R}$-module isomorphism.

From the example above,(p. 375) $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is free of rank 4 as a module over $\mathbb{R}$, but $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C} \simeq \mathbb{C}$ is free of rank 2 as a module over $\mathbb{R}$. Therefore, the two are not isomorphic.

D&F 10.4.20 Assume that $2 \otimes 2 + x \otimes x = a(x) \otimes b(x)$ for some $a(x), b(x) \in I$. Let's construct a R-bilinear map $\varphi : I \times I \mapsto R$ by defining

$$\varphi : (p(x), q(x)) \mapsto p(x)q(x). \tag{3}$$

This is well-defined R-linear map. By universal property of tensor product, there exists a R-module homomorphism $\Phi : I \otimes_R I \to R$. Since $2 \otimes 2 + x \otimes x = a(x) \otimes b(x)$, $4 + x^2 = a(x)b(x)$, but $x^2 + 4$ is irreducible polynomial in $\mathbb{Z}[x]$, so $a(x) = 1$ or $b(x) = 1$. Since $1 \notin I$, it is impossible. Therefore, $2 \otimes 2 + x \otimes x$ can not be reduced to simple tensor.

D&F 10.4.24 Let's define a map $\varphi : \mathbb{Z}[i] \times \mathbb{R} \to \mathbb{C}$ by $\varphi : (a + bi, r) \mapsto (ra) + (rb)i$. This is $\mathbb{Z}$-balanced map:

$$\varphi((a_1 + b_1 i) + (a_2 + b_2 i), r) = r(a_1 + a_2) + r(b_1 + b_2)i = \varphi((a_1 + b_1 i), r) + \varphi((a_2 + b_2 i), r)$$
$$\varphi(a + bi, r_1 + r_2) = (r_1 + r_2)a + (r_1 + r_2)bi = \varphi(a + bi, r_1) + \varphi(a + bi, r_2) \tag{4}$$
$$\varphi(n(a + bi), r) = nr(a + bi) = \varphi(a + bi, nr).$$

Therefore, there exists a group homomorphism $\Phi : \mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{R} \to \mathbb{C}$ by universal property.

For any $(a + bi) \otimes r \in Z[i] \otimes_{\mathbb{Z}} \mathbb{R}$, we can decompose it to $a \otimes r + (bi) \otimes r$, so

$$\sum_{j=1}^{n} (a_j + b_j i) \otimes r_j = \sum_{j=1}^{n} a_j \otimes r_j + \sum_{j=1}^{n} (b_j i) \otimes r_j = \sum_{j=1}^{n} 1 \otimes a_j r_j + \sum_{j=1}^{n} i \otimes b_j r_j$$
$$= 1 \otimes \left(\sum_{j=1}^{n} a_j r_j \right) + i \otimes \left(\sum_{j=1}^{n} b_j r_j \right). \tag{5}$$

It shows that any element in $Z[i] \otimes_{\mathbb{Z}} \mathbb{R}$ can be written by $1 \otimes r_1 + i \otimes r_2$ for some $r_1, r_2 \in \mathbb{R}$.

For any $a + bi \in \mathbb{C}$, $\Phi : 1 \otimes a + i \otimes b \mapsto a + bi$, so Φ is surjective. Also, if $\Phi(1 \otimes r_1 + i \otimes r_2) = r_1 + r_2 i = 0$, then $r_1 = r_2 = 0$, so the kernel of φ is trivial. Therefore, Φ is group isomorphism, and the presentation is unique.

Let's give a ring structure on $Z[i] \otimes_{\mathbb{Z}} \mathbb{R}$ as following: for $1 \otimes r_1 + i \otimes r_2, 1 \otimes r_3 + i \otimes r_4 \in Z[i] \otimes_{\mathbb{Z}} \mathbb{R}$,

$$(1 \otimes r_1 + i \otimes r_2) \cdot (1 \otimes r_3 + i \otimes r_4) = 1 \otimes (r_1 r_3 - r_2 r_4) + i \otimes (r_2 r_3 + r_1 r_4). \tag{6}$$

Since the presentation is unique, this operation is well-defined on $Z[i] \otimes_{\mathbb{Z}} \mathbb{R}$. Now, I need to check that this operation satisfies the axiom of multiplication, but it is naturally follows as this operation imitate the multiplication in complex number. Also, it has 1 which is $1 \otimes 1 + i \otimes 0$. Therefore, $(Z[i] \otimes_{\mathbb{Z}} \mathbb{R}, +, \times)$ is a well-defined ring with 1. Finally, Φ preserves multiplication operation since

$$\Phi((1 \otimes r_1 + i \otimes r_2) \cdot (1 \otimes r_3 + i \otimes r_4)) = (r_1 r_3 - r_2 r_4) + (r_2 r_3 + r_1 r_4)i = \Phi((1 \otimes r_1 + i \otimes r_2)) \Phi((1 \otimes r_3 + i \otimes r_4)) \tag{7}$$

It shows Φ is a ring isomorphism between $Z[i] \otimes_{\mathbb{Z}} \mathbb{R}$ and $\mathbb{C}$.

D&F 10.4.25 (I'll first assume that $R \neq 0$. If $S = \mathbb{Z}$ and $R = 0$, then $\mathbb{Z}[x]$ is not is not isomorphic to $\mathbb{Z} \otimes_R 0 = 0$. Also, I'll assume $1_R = 1_S$.)

By seeing $S \otimes_R R[x]$ as a extension of scalar from R to S, it is a well-defined S-module. Let $\varphi : R[x] \to S[x]$ be the natural inclusion map, which is R-module homomorphism, then by theorem 8, there exists S-module homomorphism $\Phi : S \otimes_R R[x] \to S[x]$ such that φ factors through Φ. I'll first show that this is in fact isomorphism.

I'll first show that any element in $S \otimes_R R[x]$ can be written as $\sum_{i=0}^n s_i \otimes x^i$. For $s \in S$ and $p(x) = \sum_{i=0}^m r_i x^i \in R[x]$,

$$s \otimes p(x) = \sum_{i=0}^m s \otimes r_i x^i = \sum_{i=0}^m sr_i \otimes x^i. \tag{8}$$

Therefore, finite sum of simple tensors can be rearranged by collecting $\cdot \otimes x^i$ terms, so it can be written by $\sum_{i=0}^n s_i \otimes x^i$.

For any $\sum_{i=0}^n s_i x^i \in S[x]$,

$$\Phi : \sum_{i=0}^n s_i \otimes x^i \mapsto \sum_{i=0}^n s_i x^i. \tag{9}$$

Also, if $\Phi\left(\sum_{i=0}^n s_i \otimes x^i\right) = 0$, then it means all $s_i = 0$ and kernel is 0. Therefore, Φ is isomorphism, and the presentation is unique.

Using proposition 21, we can get R-algebra structure on $S \otimes_R R[x]$; as $1_R = 1_S$, we can treat S as a R-algebra. Explicitly, for $s_1, s_2 \in S$ and $p_1(x), p_2(x) \in R[x]$, the multiplication operation is

$$(s_1 \otimes p_1(x))(s_2 \otimes p_2(x)) = (s_1 s_2 \otimes p_1(x) p_2(x)). \tag{10}$$

We can extend $S \otimes_R R[x]$ to S-algebra by defining right S action by

$$(s_1 \otimes p(x)) s_2 = (s_1 s_2 \otimes p(x)) \tag{11}$$

as S is a commutative ring.

D&F 11.5.8(a) Let $\frac{a}{b}, \frac{c}{d} \in F$, i.e. $a, c \in R$ and $b, d \in R^\times$. As

$$\begin{aligned}
\frac{a}{b} \otimes \frac{c}{d} &= \left(d \cdot \frac{a}{bd}\right) \otimes \frac{c}{d} = \frac{a}{bd} \otimes c = \frac{ca}{bd} \otimes 1 \\
\frac{c}{d} \otimes \frac{a}{b} &= \left(b \cdot \frac{c}{bd}\right) \otimes \frac{a}{b} = \frac{c}{bd} \otimes a = \frac{ac}{bd} \otimes 1,
\end{aligned} \tag{12}$$

it shows that $\frac{a}{b} \wedge \frac{c}{d} = 0$ and $\bigwedge^2 F = 0$.

D&F 11.5.9 I'll first check that M is R-module. Checking the R action is well defined: for $r = r_1 = n_1 + n_2\sigma, r_2 = n_3 + n_4\sigma, m = m_1 = a_1 e_1 + a_2 e_2$, and $m_2 = a_3 e_1 + a_4 e_2$,

1.

$$\begin{aligned}
(r_1 + r_2)m &= ((n_1 + n_3) + (n_2 + n_4)\sigma)(a_1 e_1 + a_2 e_2) \\
&= (n_1 m + n_2 \sigma(m)) + (n_3 m + n_4 \sigma(m)) \\
&= r_1 m + r_2 m
\end{aligned} \tag{13}$$

2. Let's first calculate $\sigma(\sigma(m))$.

$$\sigma(\sigma(m)) = \sigma(a_1(e_1 + 2e_2) - a_2e_2) = a_1(e_1 + 2e_2 - 2e_2) - a_2(-e_2) = m \tag{14}$$

Therefore,

$$
\begin{aligned}
r_1(r_2m) &= r_1(n_3m + n_4\sigma(m)) \\
&= n_1n_3m + n_2n_3\sigma(m) + n_1n_4\sigma(m) + n_2n_4\sigma(\sigma(m)) \\
&= (n_1n_3 + n_2n_4)m + (n_1n_4 + n_2n_3)\sigma(m) \\
&= (r_1r_2)m.
\end{aligned} \tag{15}
$$

3.

$$
\begin{aligned}
r(m_1 + m_2) &= (n_1 + n_3\sigma)((a_1 + a_3)e_1 + (a_2 + a_4)e_2) \\
&= (n_1 + n_3\sigma)(a_1e_1 + a_2e_2) + (n_1 + n_3\sigma)(a_3e_1 + a_4e_2) = rm_1 + rm_2
\end{aligned} \tag{16}
$$

4.

$$1(m) = m \tag{17}$$

Therefore, it is well-defined R-module. Since $e_1 \wedge e_1 = e_2 \wedge e_2 = 0$, $\bigwedge^2 M$ is generated by $e_1 \wedge e_2$. Since

$$e_1 \wedge e_2 = \sigma(e_1) \wedge \sigma(e_2) = (e_1 + 2e_2) \wedge (-e_2) = -e_1 \wedge e_2, \tag{18}$$

it is order 2.

D&F 18.1.10 Assume there is a subgroup of $GL_2(\mathbb{R})$ which is isomorphic to Q_8, and i and j corresponds to matrices A and B. Since $A^4 - I = (A - I)(A + I)(A^2 + I) = 0$, the minimal polynomial of A and B can be $x - 1$, $x + 1$, $(x - 1)(x + 1) = x^2 - 1$, or $x^2 + 1$ as it should divide $x^4 - 1$ in $\mathbb{R}[x]$. Since $A^2 \neq I$, the only possible case is $x^2 + 1 = 0$. Fix a basis for A making it rational canonical form. The corresponding rational canonical form is

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{19}$$

Let $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then,

$$\begin{pmatrix} a^2 + bc & b(a + d) \\ c(a + d) & d^2 + bc \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \tag{20}$$

If $b = 0$ or $c = 0$, then $a^2 = -1$, which is impossible. Therefore, $a = -d$. Also,

$$
\begin{aligned}
\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \begin{pmatrix} -c & -d \\ a & b \end{pmatrix} \\
\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} &= \begin{pmatrix} b & -a \\ d & -c \end{pmatrix},
\end{aligned} \tag{21}
$$

so $b = c$, which means that $a^2 + b^2 = -1$, which is impossible. Therefore, there is no subgroup of $GL_2(\mathbb{R})$ which is isomorphic to Q_8.

D&F 18.1.1 φ is a group homomorphism, so φ induces faithful representation(=injective group homomorphism) from $G/\ker\varphi$ to $GL(V)$. (If $\varphi(a) = \varphi(b)$, then $\varphi(ab^{-1}) = \text{id}$, so $ab^{-1} \in \ker\varphi$, and $[a] = [b]$ in $G/\ker\varphi$.)

D&F 18.1.2 Let's define a group homomorphism $\phi : G \to F^\times$ by $\phi : g \mapsto \det(\varphi(g))$. Since $\det : GL_n(F) \to F^\times$ is a well-defined group homomorphism, ϕ is again well-defined group homomorphism. As $F^\times = GL_1(F)$, the representation has degree 1.

D&F 18.1.3 Let $\varphi : G \to GL_1(F)$ be a representation of G. For $g_1, g_2 \in G$,

$$\varphi([g_1, g_2]) = [\varphi(g_1), \varphi(g_2)] = 0 \tag{22}$$

as $GL_1(F)$ is an abelian group. Therefore, $\tilde{\varphi} : G/G' \to GL_1(F)$ is naturally induced from φ. Conversely, if a representation $\tilde{\varphi} : G/G' \to GL_1(F)$ is given, we can define $\varphi : G \to GL_1(F)$ by $\varphi(g) = \tilde{\varphi}(g + G')$ by the above reason.

D&F 18.1.4 Let $G = \{g_1, \ldots, g_n\}$ where $n < \infty$. Consider a set $A = \{g_1 v, \ldots, g_n v\}$. (Note that $1 \in G$.) I claim that $M = \operatorname{span} A$ on F is a FG-module. If I prove it, then it has dimension not bigger than $|G|$ containing v.

Note that M is already F-module, so I need to check that FG action is well-defined, i.e. the result of FG action on M is again in M. For $a \in F$, $g \in G$, and $m = \sum_{i=1}^n b_i(g_i v)$ with $b_i \in F$,

$$ag(m) = \sum_{i=1}^n (ag)(b_i(g_i v)) = \sum_{i=1}^n (ab_i)((gg_i v)), \tag{23}$$

and as $gG = G$, it is in M. It ends the proof.

D&F 18.1.5 Let M be a irreducible FG-module. By the above exercise, if M has dimension bigger than $|G|$, then it has non-trivial submodule of dimension not bigger than $|G|$ by choosing $v \neq 0$, which is contradiction. Therefore, I can assume M has dimension not bigger than $|G|$.

Assume M has dimension $|G| > 1$. For non-zero v, consider

$$w = \sum_{i=1}^{|G|} g_i v. \tag{24}$$

If $w \neq 0$, then as w is G-stable, $\operatorname{span} w$ forms a 1-dim FG-submodule, which is contradiction, so w should be 0. It means that $\operatorname{span}\{g_1 v, \ldots, g_n v\}$ has dimension smaller than $|G|$. Also, it should be M to satisfy irreducible condition. Therefore, M has dimension smaller than $|G|$.

13(D&F 18.1.8)

(a) Let $\{e_i\}_{i=1}^n \subset V$ be the basis of V and $v = \sum_{i=1}^n a_i e_i \in V$ be an element with $\{a_i\} \subset F$ satisfying $\sigma \cdot v = v$ for all $\sigma \in S_n$. Assume $a_{i_1} \neq a_{i_2}$ for some $i_1 \neq i_2$. Then, for $(i_1\ i_2) \in S_n$,

$$(i_1\ i_2) \cdot \left(\sum_{i=1}^n a_i e_i \right) = \left(\sum_{i=1, i \neq i_1, i_2}^n a_i e_i \right) + a_{i_2} e_{i_1} + a_{i_1} e_{i_2}, \tag{25}$$

which is different from v as V is vector space over F. It is contradiction, so all the coefficients must be same.

(b) For $n = 2$ and char $F \neq 2$, there are two different submodules that each is generated by $e_1 - e_2$ and $e_1 + e_2$. Therefore, I'll assume $n \geq 3$.

The submodule generated by $\sum_{i=1}^{n} e_i$ is definitely 1-dim submodule, so I'll show that this is unique 1-dim submodule. Assume there is another 1-dim submodule V and choose an element $v = \sum_{i=1}^{n} a_i e_i \in V$ with $\{a_i\} \subset F$. Assume $a_{i_1} \neq a_{i_2}$ for some $i_1 \neq i_2$ and WLOG, assume $a_{i_1} \neq 0$. Then, for $(i_1 \ i_2) \in S_n$,

$$\sigma \cdot v - v = a_{i_2} e_{i_1} + a_{i_1} e_{i_2} - (a_{i_1} e_{i_1} + a_{i_2} e_{i_2}) = (a_{i_2} - a_{i_1})(e_{i_1} + e_{i_2}) \neq 0. \tag{26}$$

If $a_i \neq 0$ for some $i \neq i_1, i_2$, then $\sigma \cdot v - v$ and v are linearly independent, which is contradiction to the dimension condition. Therefore, $a_i = 0$ if $i \neq i_1, i_2$. However, it again generates contradiction since choosing $j \neq i_1, i_2$, $(j \ i_1)(\sigma \cdot v - v)$ is again linearly independent to $(\sigma \cdot v - v)$. ($n \geq 3$ is used in this procedure.) Therefore, V has the unique 1-dim submodule.

D&F 18.3.5 Let G be a group and V be a $\mathbb{C}$ vector space. Let f be a class function.

$\Rightarrow$ It means that there exists a linear representation $\phi : G \to GL(V)$ which generates characteristic f. Let's decompose V by irreducible subspaces: there exist $V_1, \dots, V_k$ and $m_1, \dots, m_k \in \mathbb{N}$ such that V is isomorphic to

$$V = m_1 V_1 \oplus \cdots \oplus m_k V_k. \tag{27}$$

Let χ_i be the irreducible character for each V_i, then we get

$$f = \sum_{i=1}^{k} m_i \chi_i. \tag{28}$$

$\Leftarrow$ Assume χ_i be the irreducible character for each V_i, and

$$f = \sum_{i=1}^{k} m_i \chi_i \tag{29}$$

for $m_1, \dots, m_k \in \mathbb{N}$. Let $V = \oplus_{i=1}^{k} \oplus_{j=1}^{m_i} V_i$, and ϕ_i be irreducible linear representation on V_i. We can construct $\phi : G \to GL(V)$ by

$$\phi(g)v = (\phi_1(g)v_{11}, \dots, \phi_1(g)v_{1m_1}, \phi_2(g)v_{21}, \dots, \phi_k(g)v_{km_k}) \tag{30}$$

for $v = (v_{11}, \dots, v_{1m_1}, v_{21}, \dots, v_{km_k}) \in V$ with $v_{i.} \in V_i$. Since $\phi(g)$ is a $\mathbb{C}$-linear map and invertible with inverse $\phi(g^{-1})$, it is well-defined, and group homomorphism by the definition, so it is a representation. Finally, we get χ as a characteristic of the ϕ.

D&F 18.3.6 Note that W is G-stable subspace, so we can decompose V by $V = W \oplus W^0$ where W^0 is complement to W and G-stable. Since any 1-dim subspace of W is G-stable, taking irreducible subspace decomposition, it is completely decomposed into 1-dim subspaces, which is irreducible. Since φ is identity on each subspace, these irreducible representations are isomorphic to trivial representations.

To show that $(\psi, \chi_1) = \dim W$, I need to show that there is no irreducible subspaces in irreducible decomposition of W^0. Assume there is such subspace $W' \leq W^0$ and $f : \mathbb{C} \to W'$ be a representation isomorphism. Since $\dim W' = 1$, it is generated by one-element, and let the element $f(1) = w'$. Since it is not in W, there exists $g \in G$ such that $g \cdot w' \neq w'$, but it means that

$$g \cdot f(1) = g \cdot w' \neq w' = f(g \cdot 1). \tag{31}$$

Therefore, it is contradiction, and we get the identity.

S 2.1 Let $\rho : G \to GL(V_1)$ and $\rho' : G \to GL(V_2)$ be representations of G generating characters χ and χ'. Then, $\chi + \chi'$ is the character of the direct sum representation on $V_1 \oplus V_2$.

Let $s \in G$. Using proposition 3, we get

$$\begin{aligned}
(\chi + \chi')_\sigma^2(s) &= \frac{1}{2}\left((\chi + \chi')^2(s) + (\chi + \chi')(s^2)\right) \\
&= \frac{1}{2}\left(\chi^2(s) + \chi(s^2) + (\chi')^2(s) + \chi'(s^2) + 2\chi(s)\chi'(s)\right) \\
&= \chi_\sigma^2(s) + (\chi')_\sigma^2(s) + \chi\chi'(s).
\end{aligned} \tag{32}$$

Therefore,

$$(\chi + \chi')^2_\sigma = \chi^2_\sigma + (\chi')^2_\sigma + \chi\chi'. \tag{33}$$

By the similar calculation, we get

$$
\begin{aligned}
(\chi + \chi')^2_\alpha(s) &= \frac{1}{2}\left((\chi + \chi')^2(s) - (\chi + \chi')(s^2)\right) \\
&= \frac{1}{2}\left(\chi^2(s) - \chi(s^2) + (\chi')^2(s) - \chi'(s^2) + 2\chi(s)\chi'(s)\right) \\
&= \chi^2_\alpha(s) + (\chi')^2_\alpha(s) + \chi\chi'(s).
\end{aligned} \tag{34}
$$

D&F 18.3.11 Let ϕ be the irreducible representation of G on V generating χ. Let z is in the center of G, then we get

$$\phi(z)\phi(g) = \phi(g)\phi(z) \tag{35}$$

for all $g \in G$, which means that $\phi(z)$ is an $\mathbb{C}G$ module automorphism on V. By schur's lemma, it shows that $\phi(z)$ is a homothety, i.e., for $\lambda \in \mathbb{C}$, $\phi(z) = \lambda \cdot \mathrm{id}$, so $\chi(z) = \lambda\chi(1)$. Since $|z| < \infty$, $\lambda^{|z|} = 1$ and λ is some root of unity in $\mathbb{C}$.

D&F 18.3.15 This is basis-dependent argument(private communication with TA): For a cyclic group $G = <\sigma : \sigma^3 = 1>$, consider a group representation ϕ on F^2 given by

$$\rho_\sigma = \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(\frac{2\pi i}{3}\right) \end{pmatrix}. \tag{36}$$

I'll denote $u = \exp\left(\frac{2\pi i}{3}\right)$. For $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2 F$, the similar transformation is given by

$$A^{-1}\rho_\sigma A = \frac{1}{ad - bc}\begin{pmatrix} ad - ubc & bd(1 - u) \\ ac(-1 + u) & uad - bc \end{pmatrix}. \tag{37}$$

For arbitrary nonzero $f \in F$, if I set $a = 1 + f$, $b = c = d = 1$, then

$$\frac{ad - ubc}{ad - bc} = \frac{f - u + 1}{f} = \frac{-u + 1}{f} + 1. \tag{38}$$

If $\mathbb{Q}(\varphi)$ implies collecting all entries of φ upto similar transformation, it means that F is finite extension of $\mathbb{Q}[u]$, which is contradiction. Therefore, I'll fix a basis for $GL_n(F)$.

Define

$$A = \cup_{s \in G} \cup_{a^s_{ij} \text{ is an entry of } \varphi(s)} \{a^s_{ij}\}, \tag{39}$$

then it is finite since $|G| < \infty$ and $\varphi(s) \in GL_n(F)$. Furthermore, $a^s_{ij} \in F$, so each $[\mathbb{Q}(a^s_{ij}) : \mathbb{Q}] < \infty$. Therefore, $[\mathbb{Q}(A) : \mathbb{Q}] < \infty$, which shows that $\mathbb{Q}(\varphi)$ is finite extension of $\mathbb{Q}$.

D&F 18.3.16 Fix $s \in G$. Since σ is a automorphism on F, for $a_i, b_i \in F$,

$$\sigma\left(\sum_i a_i b_i\right) = \sum_i \sigma(a_i)\sigma(b_i). \tag{40}$$

Therefore, $\sigma(AB) = \sigma(A)\sigma(B)$ for $A, B \in GL_n(F)$, which shows that φ^σ is a group homomorphism from G to $GL_n(F)$, so φ^σ is a representation if φ is a representation. Furthermore, $\text{tr}(\sigma(A)) = \sigma(\text{tr}(A))$ by the same reason, so we get the character of $\varphi^\sigma = \sigma \circ \psi$.

D&F 18.3.17 Since $(\varphi^\sigma)^{\sigma^{-1}} = \varphi$, it is enough to show that φ is irreducible implies φ^σ is irreducible.

Assume φ^σ is not irreducible, so there exists a proper subspace W of V such that $\varphi^\sigma|_W$ is an automorphism on W. It means that there exists a complement W^0 of W which also satisfies $\varphi^\sigma|_{W^0} \in Aut(W^0)$. Therefore, the matrix form of φ can be decomposed into smaller block matrices, which have determinant non-zero. Taking σ^{-1} to each entries of the decomposed matrix, we get the same block decomposed matrices with non-zero determinant since σ is field isomorphism. It shows that φ is not irreducible, which is contradiction. It ends the proof.

D&F 19.3.1 For basis $1 \otimes e_1, 1 \otimes e_2, 1 \otimes e_3, (1\,2) \otimes e_1, (1\,2) \otimes e_2, (1\,2) \otimes e_3\}$, the matrix representation is given by the following: for

$$P_1 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$P_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

(41)

we get

$$1 \mapsto \begin{pmatrix} I_3 & 0 \\ 0 & I_3 \end{pmatrix},$$

$$(1\,2) \mapsto \begin{pmatrix} 0 & I_3 \\ I_3 & 0 \end{pmatrix},$$

$$(1\,3) \mapsto \begin{pmatrix} 0 & \varphi((1\,2\,3)) \\ \varphi((1\,3\,2)) & 0 \end{pmatrix} = \begin{pmatrix} 0 & P_1 \\ P_2 & 0 \end{pmatrix},$$

$$(2\,3) \mapsto \begin{pmatrix} 0 & \varphi((1\,3\,2)) \\ \varphi((1\,2\,3)) & 0 \end{pmatrix} = \begin{pmatrix} 0 & P_2 \\ P_1 & 0 \end{pmatrix},$$

$$(1\,2\,3) \mapsto \begin{pmatrix} \varphi((1\,2\,3)) & 0 \\ 0 & \varphi((1\,3\,2)) \end{pmatrix} = \begin{pmatrix} P_1 & 0 \\ 0 & P_2 \end{pmatrix}, \text{ and}$$

$$(1\,3\,2) \mapsto \begin{pmatrix} \varphi((1\,3\,2)) & 0 \\ 0 & \varphi((1\,2\,3)) \end{pmatrix} = \begin{pmatrix} P_2 & 0 \\ 0 & P_1 \end{pmatrix}.$$

(42)

D&F 19.3.2(a) Since induced representation is unique upto isomorphism, it is enough to calculate the character with some fixed representatives of G/H. Since $< (1\,2) >$ has order 2, it has two irreducible representations: trivial and non-trivial one. The non-trivial irreducible character ψ is $\psi(1) = 1$ and $\psi((1\,2)) = -1$. For representatives $\{1, (1\,3), (2\,3)\}$, the induced character Ψ is

$$\Psi(1) = 3\psi(1) = 3$$
$$\Psi((1\,2)) = \Psi((1\,3)) = \Psi((2\,3)) = \psi((1\,2)) = -1$$
$$\Psi((1\,2\,3)) = \Psi((1\,3\,2)) = 0.$$

(43)

Using the character table of S_3 in section 19.1, we get $\Psi = \chi_2 + \chi_3$.

D&F 19.3.4 Let $R = \{1, g_1, \ldots, g_m\}$ be the representation set of G/H and Φ be the induced representation of φ which is a representation on V. Fix $g_i \in R$. For $v \in V$ and $n \in N \leq H$, there exists $n' \in N$ such that $ng_i = g_i n'$ since N is a normal subgroup of G. Therefore,

$$n \cdot (g_i \otimes v) = ng_i \otimes v = g_i n' \otimes v = g_i \otimes (n' \cdot v) = g_i \otimes v. \tag{44}$$

It shows that N is contained in the kernel of induced presentation.

1 Chapter 2

Before solving the problems, I'll first show a useful proposition.

Proposition 1. *Let $\rho : G \to GL(V)$ be a group representation and $s \in G$, then $\rho(s)$ is diagonalizable.*

Proof. You need some fact about minimal polynomial of matrices in linear algebra; see chapter 11 in *Abstract Algebra*, Dummit and Foote.

Since $s^{|G|} = 1$, $\rho(s)$ has minimal polynomial dividing $x^{|G|} - 1$. Since $x^{|G|} - 1$ is a separable polynomial in $\mathbb{C}[x]$ and $\mathbb{C}$ is algebraically closed, $\rho(s)$ is diagonalizable. $\square$

S 2.1 Using proposition 3, we get

$$
\begin{aligned}
(\chi + \chi')^2_\sigma(s) &= \frac{1}{2} \left((\chi(s) + \chi'(s))^2 + (\chi + \chi')(s^2) \right)^2 \\
&= \frac{1}{2} \left((\chi(s)^2 + \chi(s^2)) + (\chi'(s)^2 + \chi'(s^2)) \right)^2 + \chi(s)\chi'(s) \\
&= \chi^2_\sigma(s) + \chi'^2_\sigma(s) + \chi(s)\chi'(s).
\end{aligned}
\tag{45}
$$

It shows that $(\chi + \chi')^2_\sigma = \chi^2_\sigma + \chi'^2_\sigma + \chi\chi'$. By the same computation, we also get $(\chi + \chi')^2_\alpha = \chi^2_\alpha(s) + \chi'^2_\alpha(s) + \chi(s)\chi'(s)$.

S 2.2 Let's enumerate $X = \{x_1, \ldots, x_n\}$. Let's define index set $I_s = \{i \in \{1, \ldots, n\} : s \cdot x_i = x_i\}$, Writing ρ_s as a matrix $A_s = (a_{ij})$ with basis $\{x_1, \ldots, x_n\}$, we get $a_{ji} = 1$ if and only if $s \cdot x_i = x_j$. Therefore,

$$
\operatorname{tr} A_s = \sum_{i=1}^{n} a_{ii} = \sum_{i \in I} 1 = |I_s|.
\tag{46}
$$

It shows that $\chi_X(s) = \operatorname{tr} A_s$ is the number of elements of X fixed by s.

S 2.3 I'll first show the uniqueness: if there exist such representations ρ'_1 and ρ'_2, then for fixed $x' \in V'$ and $s \in G$,

$$
\langle \rho_s x, ((\rho'_1)_s - (\rho'_2)_s) \, x' \rangle = \langle x, x' \rangle - \langle x, x' \rangle = 0
\tag{47}
$$

for all $x \in V$. Since $\rho_s \in GL(V)$, it is automorphism on V, and it means that $\rho'_1 = \rho'_2$.

Now, I'll show the existence. Let's define $\rho'_s x' := x' \circ \rho_{s^{-1}}$. Since ρ_s is invertible and linear, ρ'_s is well-defined linear mapping. Also, it satisfies

$$
\langle \rho_s x, \rho'_s x' \rangle = x' \left(\rho_{s^{-1}}(\rho_s x) \right) = x'(x) = \langle x, x' \rangle.
\tag{48}
$$

Finally, it satisfies homomorphism property since for $s, t \in G$,

$$
\rho'_t(\rho'_s x') = (x' \circ \rho_{s^{-1}}) \circ \rho_{t^{-1}} = x' \circ (\rho_{s^{-1}} \circ \rho_{t^{-1}}) = x' \circ (\rho_{(ts)^{-1}}) = \rho'_{ts} x'.
\tag{49}
$$

It ends the proof.

S 2.4 I'll first check that ρ is a linear representation. By definition, it is indeed linear, and for $s, t \in G$,

$$
\begin{aligned}
\rho_t(\rho_s f) &= \rho_{2,t} \circ \left(\rho_{2,s} \circ f \circ \rho_{1,s}^{-1} \right) \circ \rho_{1,t}^{-1} \\
&= \rho_{2,ts} \circ f \circ \rho_{1,ts}^{-1} = \rho_{ts} f
\end{aligned}
\tag{50}
$$

To compute the character, let's fix a basis of V_1 and V_2. Let m and n be the dimension of V_1 and V_2 over $\mathbb{C}$, then we can write $f \in W$ as a m by n matrix. Let's choose the basis for W by the matrix basis:

$$
\{\beta_{11}, \dots, \beta_{mn}\} = \left\{ \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} \right\}.
\tag{51}
$$

Let matrices $A = \rho_{2,s}$, $B = f$, and $C = \rho_{1,s}^{-1}$ with elements a_{ij}, b_{ij}, and c_{ij}. Computing matrix multiplication,

$$
(ABC)_{ij} = \sum_{k,l} a_{ik} b_{kl} c_{lj}.
\tag{52}
$$

The characterstic is

$$
\sum_{i,j} (A\beta_{ij}C)_{ij} = \sum_{i,j} \sum_{k,l} a_{ik} \delta_{ki} \delta_{lj} c_{lj} = \sum_{i,j} a_{ii} c_{jj} = \left(\sum_i a_{ii} \right) \left(\sum_j c_{jj} \right).
\tag{53}
$$

Since $(\sum_i a_{ii}) = \chi_2$ and $\left(\sum_j c_{jj} \right) = \chi_1^*$, the characterstic is $\chi_1^* \cdot \chi_2$.

Let's construct a isomorphism between ρ and $\rho_1' \otimes \rho_2$. Let $\overline{\varphi} : V_1' \times V_2 \to W$ a map such that for $(v_1', v_2) \in V_1' \times V_2$, for $v \in V_1$

$$
(\overline{\varphi}(v_1', v_2)) v = (v_1'(v)) v_2.
\tag{54}
$$

It is $\mathbb{C}$-bilinear map, so by the universal property, there exists a vector space homomorphism $\varphi : V_1' \otimes V_2 \to W$ which factors through $\overline{\varphi}$. φ is surjective: for a basis $\{e_i\} \subset V_1$, if I want to map $e_i \mapsto v_i \in V_2$, then I just take a dual basis element $\{e_i'\} \subset V_1'$ making $e_i'(e_j) = \delta_{ij}$ and take

$$
\sum_{i=1}^{m} e_i' \otimes v_i.
\tag{55}
$$

By dimension analysis, it means that φ is vector space isomorphism.

Now, I need to show the commutativity $\varphi \circ \left(\rho_{1,s}' \otimes \rho_{2,s} \right) = \rho_s \circ \varphi$ for any $s \in G$. By linearlity, it is enough to show it for simple tensor, but for $v_1' \otimes v_2 \in V_1' \otimes V_2$, for $v \in V_1$,

$$
\begin{aligned}
\left(\varphi \circ \left(\rho_{1,s}' \otimes \rho_{2,s} \right) (v_1' \otimes v_2) \right)(v) &= \left(\varphi \circ \left(\rho_{1,s}'(v_1') \otimes \rho_{2,s}(v_2) \right) \right)(v) \\
&= \left(\rho_{1,s}'(v_1') \right)(v) \rho_{2,s}(v_2) \\
(\rho_s \circ \varphi(v_1' \otimes v_2))(v) &= \left(\rho_{2,s} \circ \varphi(v_1' \otimes v_2) \circ \rho_{1,s}^{-1} \right)(v) \\
&= \rho_{2,s} \circ \left(v_1'(\rho_{1,s}^{-1}(v)) v_2 \right) \\
&= v_1'(\rho_{1,s}^{-1}(v)) \rho_{2,s}(v_2) \\
&= \left(\rho_{1,s}'(v_1') \right)(v) \rho_{2,s}(v_2).
\end{aligned}
\tag{56}
$$

It ends the proof.

Remark: If $V_2 = \mathbb{C}$, then $W = V_1'$ and ρ_s corresponds to the dual representation of ρ.

S 2.5 This problem is continuation of problem **D&F** 18.3.6. For each irreducible representation component of ρ, if it is not isomorphic to the trivial(=unit) representation, the scalar product with trivial representation is 0, and 1 if it is isomorphic to the representation. Therefore, we get the identity.

S 2.6

1. Before solving it, I'll first show the proposition.

   Proposition 2. *Let a finite group G acts transitively on a finite set $X = \{x_1, \ldots, x_k\}$. Set M be free $\mathbb{Z}$-module on X, then we can treat M as a $\mathbb{Z}G$-module using the group action. For $v = \sum_{g \in G} g \cdot x_i \in M$ for some fixed $1 \le i \le k$, each coefficient of x_j, $1 \le j \le k$, in v is same.*

   Proof. Let G_{x_i} be the stabilizer of x_i in G, then $\left| G : G_{x_i} \right| = |X|$ since G acts transitively on X and we get the coefficient of each x_j in j by $\left| G_{x_i} \right|$. (cf. proposition 2 in **D&F** p. 114.) $\square$

   Choose an orbit $O \subset X$ and $x \in O$. Taking permutation representation V, consider $v = \sum_{g \in G} g \cdot x$. Then v is contained in the subspace spanned by the orbit elements containing x. Also, the 1-dim subspace generated by v is G-stable since

   $$g \cdot v = g \sum_{g' \in G} g' \cdot v = \sum_{g' \in G} gg' \cdot v \sum_{g' \in g^{-1}G} g' \cdot v = v. \tag{57}$$

   Therefore, it has unit representation. This argument can be applied to each distinct orbits, so $(\chi | 1) \ge c$.

   Let W be the subspace of V composing all the 1-dim subspaces discovered above. Note that W is G-stable, so there exists complement subspace W^0 which is also G-stable. To show $(\chi | 1) = c$, I need to show that there is no irreducible subspace with unit representation in W^0. Assume it is not and spanned by $w^0 \in W^0$. Since $w^0 \ne 0$, there exists x_i having non-zero coefficient. Let $O = \{x_i^1, \ldots, x_i^k\}$ be the orbit containing x_i, then by the above proposition, each coefficient of x_i^j in $\sum_{g \in G} g \cdot w^0$ should be same, but as $g \cdot w^0 = w^0$ for all g, $\sum_{g \in G} g \cdot w^0 = |G| w^0$. It is contradiction since we chose w^0 complement to W. Therefore, $(\chi | 1) = c$.

   If G is transitive, then $c = 1$, then the rest propositions follow from the above argument. For example, we can construct $\theta : G \to GL(W^0)$ such that for the projection $P : W \to W^0$ and inclusion $i : W^0 \to W$, $\theta_s = P \circ \rho_s \circ i$.

2. Fix $s \in G$. Let $\{\xi_1, \ldots, \xi_n\}$ be the eigenvectors of ρ_s with corresponding eigenvalues λ_i in the basis $X = \{x_1, \ldots, x_n\}$. (Note that ρ_s is diagonalizable in $\mathbb{C}$.) For $X \times X$, take basis $\{(x_1, x_1), \ldots, (x_1, x_n), (x_2, x_1), \ldots, (x_n, x_n)\}$ and write

   $$\left(\sum_{i=1}^n a_i x_i, \sum_{j=1}^n b_j x_j \right) := \sum_{i=1}^n \sum_{j=1}^n a_i b_j \left(x_i, x_j \right). \tag{58}$$

Then,

$$s \cdot (\xi_i, \xi_j) = \lambda_i \lambda_j (\xi_i, \xi_j), \tag{59}$$

which means that $\{(\xi_i, \xi_j)\}_{i,j=1}^{n}$ forms a complete set of eigenvectors of the permutation representation of s. Therefore, the trace is

$$\sum_{i=1}^{n} \sum_{j=1}^{n} \lambda_i \lambda_j = \chi^2(s). \tag{60}$$

for all s, and we get the characteristic function χ^2.

3. (i)$\Leftrightarrow$(ii) As the hint says, it is obvious.

(ii)$\Leftrightarrow$(iii) The character of the permutation representation on $X \times X$ is χ^2 from (b) and $(\chi^2|1) = 2$ if and only if there is two orbits in $X \times X$.

(iii)$\Leftrightarrow$(iv) I'll follow the hint. By the definition of ψ, $1 + \psi = \chi$ and by the bi-linearlity of $(\cdot|\cdot)$, we get $(\psi|1) = 0$ as G is transitive on X. Therefore,

$$(\chi^2|1) = (1 + 2\psi + \psi^2|1) = 1 + (\psi^2|1). \tag{61}$$

Therefore, (iii) is equivalent to say $(\psi^2|1) = 1$. As a character of permutation representation, χ is real-valued, so ψ is. It means that

$$(\psi^2|1) = \frac{1}{g} \sum_{s \in G} \psi(s)^2 = \frac{1}{g} \sum_{s \in G} \psi(s)\overline{\psi(s)} = (\psi|\psi). \tag{62}$$

By theorem 5, we get the equivalence of (iii) and (iv).

S 2.7 Let r be the regular representation on W with basis $\{e_s\}_{s \in G}$. Since G acts on $\{e_s\}$ transitively, by the previous homework, we know that W has only one unit representation 1, which is irreducible. Therefore, for any character with $\rho_s = 0$ for all $s \neq 1$, for $c \in \mathbb{C}$ with $cr_G = \rho$,

$$(\rho, 1) = c(r_G, 1) = c \in \mathbb{N}. \tag{63}$$

S 2.8

(a) Decomposing V into irreducible subspace, let $m_i = \dim V_i / \dim W_i$. Since we are only interested in calculating the dimension of H_i, transform each irreducible subspaces in V_i is copy of W_i by taking isomorphism for each space. Let each copy W_{ij} for $1 \leq j \leq m_i$. Abusing notation, we can treat ρ as a irreducible representation on W_{ij} in each V_i.

Fix an non-zero element $w \in W_i$. Since W_i is irreducible, $\mathbb{C}G \cdot w = W_i$. Now, assume $h(w) \in W_{ij}$ for some j and non-zero; if $h(w) = 0$, then $h \equiv 0$ as $0 = h \circ \rho_s(w)$ for $s \in G$. Since $h \circ \rho_s(w) = \rho_s \circ h(w) \in W_{ij}$ and W_i is irreducible, $\operatorname{Im} h \subset W_{ij}$. Using Schur's lemma, identifying $W_{ij} = W_i$, we get $h = \lambda \cdot \operatorname{id}$ for some $\lambda \in \mathbb{C}^\times$. If $h(w) \notin V_i \setminus \{0\}$, then again by Schur's lemma, $h \equiv 0$. This argument illustrates the possible functions in H_i. Finally, if I set $h = \lambda \cdot \operatorname{id} : W_i \to W_{ij}$, it satisfies $h \circ \rho_s = \rho_s \circ h$, so such function exists in H_i.

For any $h \in H_i$ we can decompose h into $P_1 \circ h, \ldots, P_{m_i} \circ h$ such that P_j is the projection onto W_{ij}. Each $P_j \circ h$ is a multiple of id by the above argument, note that $P_j \circ \rho = \rho \circ P_j$ for representation ρ on V_i since W_{ij} is G-stable. It shows that H_i is spanned by $\{h_{ij}\}_{j=1}^{m_i}$ such that $h_{ij} : W_i \to W_{ij}$ and is identity by identifying $W_i = W_{ij}$. (By retrieving using the isomorphism, we can find the actual function $h_{ij} : W_i \to V_{ij}$ where V_{ij} is the jth position of the decomposition of V_i.) It shows $\dim H_i = \dim V_i / \dim W_i$.

(b) Let's define $F' : H_i \times W_i \to V_i$ by

$$F' : (h_\alpha, w_\alpha) \mapsto h_\alpha(w_\alpha) \tag{64}$$

and extend it to satisfy $\mathbb{C}$-linearity. This is $\mathbb{C}$-bilinear, so by the universal property, we get the well-defined vector space homomorphism $F : H_i \otimes W_i \to V_i$ which factors through F'. By (a), we know that that F' is surjective, so F is surjective. By dimension analysis, it means F is vector space isomorphism.

(c) By tensor-hom adjuction, we get natural isomorphism

$$\operatorname{Hom}(H_i \otimes W_i, V_i) \simeq \operatorname{Hom}(H_i, \operatorname{Hom}(W_i, V_i)), \tag{65}$$

which shows that the F maps each $(h_1, \ldots, h_k)$ to a linear map $h : \oplus_{j=1}^{m_i} W_i \mapsto V_i$ by

$$h : (w_{i1}, \ldots, w_{im_i}) \mapsto \sum_{j=1}^{m_i} h_j(w_{ij}). \tag{66}$$

I'll show that h is surjective, then by dimension analysis, it is vector space isomorphism. First, consider the basis $\{e_1, \ldots e_{m_i}\} \in H_i$ I set in (a), which is isomorphic from W_i to jth irreducible component of V_i in representation sense. In this setting, it is easy to see that h is surjective. Now, let $\{h_1, \ldots, h_{m_i}\} \in H_i$ be an aribtrary basis of H_i, and let

$$h_\alpha = \sum_{\beta=1}^{m_i} a_{\alpha\beta} e_\beta. \tag{67}$$

Let's denote $A = (a_{\alpha\beta}) \in GL_{m_i}(\mathbb{C})$ and $A^{-1} = (b_{\alpha'\beta'})$. For $\sum_j v_j \in V_i$, there exists $(w_{i1}, \ldots, w_{im_i}) \in \oplus_{j=1}^{m_i} W_i$ such that $e_j(w_{ij}) = v_j$ and $e_j(w_{ik}) = 0$ if $j \neq k$. Finally, for

$$w'_{i\alpha'} = \sum_{\beta'=1}^{m_i} b_{\beta'\alpha'} w_{i\beta'} \tag{68}$$

we get

$$\sum_{\alpha=1}^{m_i} h_\alpha(w'_{i\alpha}) = \sum_{\alpha=1}^{m_i}\sum_{\beta=1}^{m_i}\sum_{\beta'=1}^{m_i} a_{\alpha\beta} e_\beta(b_{\beta'\alpha} w_{i\beta'}) = \sum_{\beta=1}^{m_i}\sum_{\alpha=1}^{m_i} a_{\alpha\beta} b_{\beta\alpha} v_\beta = \sum_{\beta=1}^{m_i} v_\beta. \tag{69}$$

Finally, it is isomorphism of representations as we chose h_i to satisfy $\rho \circ h_i = h_i \circ \rho$.

2 Chapter 3

S 3.1 Let's decompose V into irreducible subspaces V_i with representation function ρ_i. For any $s_1, s_2 \in G$, we get

$$(\rho_i)_{s_1} \circ (\rho_i)_{s_2} = (\rho_i)_{s_2} \circ (\rho_i)_{s_1} \tag{70}$$

as G is abelian group. Using Schur's lemma, $(\rho_i)_s = \lambda_s \circ \operatorname{id}$ for some $\lambda \in \mathbb{C}^\times$ for all $s \in G$, but it means that V_i is not irreducible if $\dim V_i > 1$ since ρ can be decomposed into block matrices. Therefore, all the V_i are degree 1.

S 3.2

(a) By the same argument in 3.1, ρ_s is a homothety for each $s \in C$. Since eigenvalues of ρ_s are absolute value 1, we get $|\chi(s)| = n$ for $s \in C$.

(b) Since $|G| \geq |C|$,
$$g = \sum_{s \in G} |\chi(s)|^2 \geq \sum_{s \in C} |\chi(s)|^2 = cn^2, \tag{71}$$
so $n^2 \leq g/c$.

(c) For each $s \in C$, we can write the scalar $\lambda = \exp(2\pi i q)$ for some $q \in [0, 2\pi) \cap \mathbb{Q}$. Let $q_0 = \min_{s \in C} q$. If $q_0 = a/b$ with $(a, b) = 1$, then by Fermat's little theorem, we get $1/b \leq a/b$, so q_0 is of form $1/n$ for some $n \in \mathbb{N}$ and corresponding group element s_0. Assume there exists s' which is not in $\{1, s, \ldots, s^{n-1}\}$ and the corresponding phase $q' = 1/b'$. If $b' \nmid n$, we can make phase $1/\text{lcm}(b', n)$ taking combination of s and s', so assume $b' \mid n$. However, it also makes a contradiction since
$$s^{n/b'}(s')^{-1} = 1. \tag{72}$$

Therefore, C is a cyclic group.

S 3.3 Since G is abelian, any irreducible representation has degree 1. For irreducible representations ρ_1 and ρ_2 on V_1 and V_2, $\rho_1 \otimes \rho_2$ is again irreducible since $V_1 \otimes V_2$ also has degree 1. Therefore, for any irreducible character χ_1 and χ_2, $\chi_1 \chi_2$ is also irreducible. As a function from G to $\mathbb{C}$, this operation satisfies associative, has identity element $\chi(s) = 1$ for all s, and inverse $\overline{\chi}$: for a representation $\rho : G \to \mathbb{C}^\times$, $\overline{\rho}$ is also a representation having character $\overline{\chi}$. Since the number of classes of G is g, the number of irreducible representations is g, so $\hat{G}$ is an abelian group of order g.

For fixed $x \in G$, let's define $\varphi_x : \hat{G} \to \mathbb{C}$ by $\varphi_x(\chi) = \chi(x)$. This is well-defined group homomorphism with image in $\mathbb{C}^\times$, so it is an element of the $\hat{\hat{G}}$. Let $h : G \to \hat{\hat{G}}$ by $h(x) = \varphi_x$. h is group homomorphism since $\varphi_{xy^{-1}}(\chi) = \chi(xy^{-1}) = \chi(x)\chi(y^{-1}) = \varphi_x \varphi_{y^{-1}}$. If $\varphi_x \equiv 1$, then it means $\chi(x) = 1$ for all irreducible character $\chi \in \hat{G}$. If $x \neq 1$, then $\sum_{i=1}^{g} \chi_i(1)^* \chi_i(x) = g \neq 0$ according to proposition 7 in chapter 2, which is contradiction. Therefore, $x = 1$, and it shows $\ker h = 0$. Since $\left|\hat{\hat{G}}\right| = g$, h is an isomorphism.

S 3.4 From example 1, we know that the regular representation ρ on G is induced by the regular representation θ on H. Let's decompose $\rho = \oplus_{i=1}^{n}\rho_i$ and $\theta = \oplus_{i=1}^{m}\theta_i$ into irreducible representations. By Corollary 5.1 in chapter 2, every irreducible representations on G and H is contained in ρ and θ.

Let ρ_i' be the induced representation of θ_i, then by example 3, we know that $\oplus_{i=1}^{m}\rho_i'$ is induced by $\oplus_{i=1}^{m}\theta_i$. By the uniqueness of induced representation, $\oplus_{i=1}^{m}\rho_i'$ and ρ are isomorphic, so each irreducible components of ρ is contained in some ρ_i', which shows the statement in the problem.

Since $A \leq G$ is abelian, each θ_i has degree 1. It means that the induced representation ρ_i' of θ_i has degree g/a for all i, so each ρ_i should have degree not greater than g/a.

S 3.5 Before start, I'll show that ρ is a well-defined representation. For $s_1, s_2 \in G$, $(\rho_{s_1}(\rho_{s_1^{-1}})f)(u) = f(us_1 s_1^{-1}) = f(u)$ and by the same reason, $(\rho_{s_1^{-1}}(\rho_{s_1})f)(u) = f(u)$, so $\rho_s \in GL(V)$ for all $s \in G$. Also,

$$(\rho_{s_1 s_2^{-1}}f)(u) = f(us_1 s_2^{-1}) = (\rho_{s_1}(\rho_{s_2^{-1}}f))(u) = (\rho_{s_1}(\rho_{s_2}^{-1}f))(u). \tag{73}$$

Therefore, it is a well-defined group action, i.e. group homomorphism from G to $GL(V)$.

To show $w \mapsto f_w$ is an isomorphism, I'll first show that $f_w \in V$. For $t \in H$ and $u \in G$, if $tu \in H$, which means that $u \in H$,

$$f_w(tu) = \theta_{tu}w = \theta_t\theta_u w = \theta_t f_w(u). \tag{74}$$

If $tu \notin H$, $f_w(u) = 0$ since $u \notin H$, so it also satisfies $f_w(tu) = \theta_t f_w(u)$. Therefore, $f_w \in V$.

To show the isomorphism from W to W_0, it is enough to show that $\varphi : w \mapsto f_w$ is injection from W. If $w_1 \neq w_2$, then $f_{w_1}(1) = w_1 \neq w_2 = f_{w_2}(1)$, so $f_{w_1} \neq f_{w_2}$.

Now, I'll show that ρ is induced by θ. Let's first fix a representatives $R = \{1 = \sigma_1, \ldots, \sigma_n\} \in G$ of G/H. I'll first show that $\{\rho_{\sigma_i}f_{w_j}\}$ forms a basis of V. For linearly independence, assume there exists $a_{ij} \in \mathbb{C}$ satisfying

$$\sum_{i,j} a_{ij}\rho_{\sigma_i}f_{w_j} = 0. \tag{75}$$

It means that for $u \in G$,

$$\sum_{i,j} a_{ij}\rho_{\sigma_i}f_{w_j}(u) = \sum_{i,j} a_{ij}f_{w_j}(u\sigma_i) = \sum_{j}\sum_{u\sigma_i \in H} a_{ij}\theta_{u\sigma_i}w_j = 0. \tag{76}$$

Note that u acts on G/H by permutation, so there exists only one i_0 such that $u\sigma_{i_0} \in H$, which means that

$$\sum_{j} a_{i_0 j}\theta_{u\sigma_{i_0}}w_j = 0. \tag{77}$$

Since $\theta_{u\sigma_{i_0}}$ is automorphism on W and w_j is a basis on W, $a_{i_0 j} = 0$ for all j. Since this is true for arbitrary $u \in G$ and G acts on G/H transitively, we get $a_{ij} = 0$ for all i, j. Therefore, $\{\rho_{\sigma_i}f_{w_j}\}$ is linearly independent.

Now, I'll show that the $\{\rho_{\sigma_i}f_{w_j}\}$ spans V. Fix arbitrary $f \in V$. Even though I chose left coset of G/H, it also works as a right coset of $H\backslash G$. Therefore, it is enough to show that I can generate $f(\sigma_i)$ using the basis to generate the f: for any $u \in G$, there exists $\sigma \in R$ and $t \in H$ such that $tu = \sigma$, so $f(u) = f(t^{-1}tu) = \theta_{t^{-1}}f(\sigma)$. Let's write $f(\sigma_i) = \sum_{i,j} a_{ij}w_j$. If I set

$$\phi = \sum_{i,j} a_{ij}\rho_{\sigma_i^{-1}}f_{w_j}, \tag{78}$$

for any $\sigma_k \in R$,

$$\phi(\sigma_k) = \sum_{i,j} a_{ij}\rho_{\sigma_i^{-1}}f_{w_j}(\sigma_k) = \sum_{i,j} a_{ij}f_{w_j}(\sigma_k\sigma_i^{-1}) = \sum_j a_{kj}w_j = f(\sigma_k). \tag{79}$$

Therefore, $\phi = f$.

By writing $W_{\sigma_i} = \mathrm{span}\{\rho_{\sigma_i}f_{w_1}, \ldots, \rho_{\sigma_i}f_{w_m}\}$, we get $V = \oplus_{\sigma \in R} W_\sigma$, which means that ρ is induced by θ.

S 3.6 Since $G = H \times K$, $hk = kh$ for all $h \in H$ and $k \in K$. It shows that $H \trianglelefteq G$ and $G/H \simeq K$. Therefore, We can take the representatives of G/H by the elements of K, and for any $k \in K$ and $h \in H$, we get $h(kH) = kH$. I'll write the representatives $R = \{k_1, \ldots, k_n\}$ with $n = |K|$ if enumerating is necessary.

Let W and L be vector spaces such that $\theta : H \to GL(W)$ and $r_K : K \to GL(L)$, i.e. L has basis $\{e_k\}_{k \in K}$. Since $\rho : G \to GL(V)$ is induced by θ, we can write

$$V = \oplus_{k \in K} W_k. \tag{80}$$

Let's construct a vector space isomorphism $\varphi : W \otimes L \to V$ by

$$\varphi(w \otimes l) = \varphi(\sum_{k \in K} a_k(w \otimes e_k)) = \sum_{k \in K} a_k \rho_k w. \tag{81}$$

Indeed, we know that $W \otimes L$ is a vector space having basis as a simple tensor of basis elements in W and L, this is well-defined map, and this is surjective since for any $\sum_{k \in K} w_k \in V$ such that $w_k \in W_k$,

$$\varphi : \sum_{k \in K} \rho_{k^{-1}} w_k \otimes e_k \mapsto \sum_{k \in K} w_k. \tag{82}$$

By dimension analysis, φ is a vector space isomorphism. Finally, this is isomorpshim of representation between $\theta \otimes r_K$ and ρ: with the same notation above and $s = hk_i \in G$ for some $k_i \in K$ and $h \in H$,

$$\rho_s(\varphi(w \otimes l)) = \sum_{k \in K} a_k \rho_s \rho_k w = \sum_{k \in K} a_k \rho_{k_i k} \rho_h w$$

$$\varphi\left((\theta \otimes r_K)_s (w \otimes l)\right) = \varphi\left(\theta_h(w) \otimes (r_K)_{k_i}\left(\sum_{k \in K} a_k e_k\right)\right) = \varphi\left(\theta_h(w) \otimes \left(\sum_{k \in K} a_k e_{k_i k}\right)\right) = \sum_{k \in K} a_k \rho_{k_i k} \rho_h w. \tag{83}$$

(To write it more precise, I need to introduce the inclusion map $i : W \to V$ and use $i(\theta_h(w)) = \rho_h(i(w))$.) Therefore, $\theta \otimes r_K$ and ρ are isomorphic.

3 Chapter 6

I'll first write the definition of terminologies related to semisimplicty and simplicity.(Ref. *Algebra*, Lang.)

For a division ring R with 1, (as we only consider $R = K[G]$, where K is a field in this homework.)

Definition 3. R-module E is simple if it is non-zero and has no submodule other than 0 or E.

Note that this is same as irreducibile module.

Definition 4. R-module E is semisimple if for any submodule F of E, there exists a submodule F' such that $E = F \oplus F'$. For a ring R with $1 \neq 0$, it is semisimple if it is semisimple as a left module over itself.

S 6.1 I'll first prove (i)→(ii). Let $F = \{\sum_{s \in G} a_s s \in K[G] : \sum_{s \in G} a_s = 0\}$. It is $k[G]$ submodule of $K[G]$ since for any $s' \in G$,

$$s' \cdot \left(\sum_{s \in G} a_s s \right) = \sum_{s \in G} a_s s' s = \sum_{s \in G} a_{(s')^{-1}s} s \in F. \tag{84}$$

By the definition of semisimple module (or ring), there should exists a submodule F' such that $K[G] = F \oplus F'$. Since F, F' are K-vector space, it can be viewed as a decomposition of the vector space. For K-linear $\phi : K[G] \to K$ by $\phi(\sum_{s \in G} a_s s) = \sum_{s \in G} a_s$, it is surjective and F is the kernel, so $\dim F = |G| - 1$. It means $\dim F' = 1$. Now, assume it is spanned by $u = \sum_{s \in G} a_s s \in F'$, then $\sum_{s' \in G} s' u = \sum_{s \in G} \sum_{s' \in G} a_{s'} s \in F' \cap F$ as

$$\sum_{s \in G} \sum_{s' \in G} a_{s'} = g \sum_{s' \in G} a_{s'} = 0. \tag{85}$$

It means $\sum_{s \in G} \sum_{s' \in G} a_{s'} s = 0$ and $\sum_{s \in G} a_s = 0$, implying that $u \in F' \cap F$, so zero. This is impossible. Therefore, F is not a direct summand of $K[G]$ and $K[G]$ is not semisimple.

Conversely, assume char $K \nmid g$, then $\frac{1}{g}$ is non-zero in K, so $p^0 = g^{-1} \sum_{s \in G} s p s^{-1}$ for K-linear projection from $K[G]$ to F is well-defined and the same argument in theorem 1 in 1.3 is well-applied. It shows that $K[G]$ is a semisimple.

S 6.2 By the definition of $\langle \cdot, \cdot \rangle$, it is bilinear. Also, by the construction of $\tilde{\rho}_i$ and linearlity of Tr_{W_i}, the formula for $\langle u, v \rangle$ is also bilinear. Therefore, I can reduce to the case $u, v \in G$. For $a, b \in G$,

$$\langle a, b \rangle = g \sum_{s \in G} \delta_{s^{-1}a} \delta_{sb} = g \delta_{ab}. \tag{86}$$

Also, by the corollary 5.2 in the chapter 2,

$$\langle a, b \rangle = \sum_{i=1}^{h} n_i \mathrm{Tr}_{W_i}(\rho_i(ab)) = \sum_{i=1}^{h} n_i \chi_i(ab) = g \delta_{ab}. \tag{87}$$

Therefore, we get

$$\langle u, v \rangle = \sum_{i=1}^{h} n_i \mathrm{Tr}_{W_i}(\tilde{\rho}_i(uv)) \tag{88}$$

S 6.3 Note: Since $\mathbb{C}[G]$ is $\mathbb{C}$-algebra isomorphic to product of matrix algebras over $\mathbb{C}$, it is not multiplicative group as some elements does not have inverse. Therefore $\mathbb{C}[G]$ is not itself a multiplicative group.

(a) Since U contains G, $s^{-1}u \in U$ for $s \in G$. As U is finite, $(s^{-1}u)^{|U|} = 1$, which implies that $(\tilde{\rho}_i(s^{-1}u))^{|U|} = \tilde{\rho}_i((s^{-1}u)^{|U|}) = I$ and the minimal polynomial of $\tilde{\rho}_i(s^{-1}u)$ should divide $x^{|U|} - 1 = 0$. Since $\mathbb{C}$ is algebraically closed field of characteristic 0 and $x^{|U|} - 1$ is separable, $\tilde{\rho}_i(s^{-1}u)$ is diagonalizable and eigenvalues are roots of unity.

Since $u'u = 1$, $\tilde{\rho}_i(u's)\tilde{\rho}_i(s^{-1}u) = I$. As an inverse matrix of a diagonalizable matrix, each eigenvalue of $\tilde{\rho}_i(u's)$ is inverse of an eigenvalue of $\tilde{\rho}_i(s^{-1}u)$, and we have shown that each eigenvalues have absolute value 1 above. Therefore,

$$\mathrm{Tr}_{W_i}(\rho_i(s^{-1})u_i)^* = \mathrm{Tr}_{W_i}(\tilde{\rho}_i(s^{-1}u))^* = \mathrm{Tr}_{W_i}(\tilde{\rho}_i(u's)) = \mathrm{Tr}_{W_i}(u'_i\rho_i(s)) \tag{89}$$

As $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$ for matrices A and B, we get

$$\mathrm{Tr}_{W_i}(\rho_i(s^{-1})u_i)^* = \mathrm{Tr}_{W_i}(\rho_i(s)u'_i) \tag{90}$$

Using Fourier inversion formula, we get $u(s)^* = u'(s^{-1})$.

(b) Note that

$$uu' = \sum_{s \in G}\left(\sum_{s' \in G} u(ss')u'((s')^{-1})\right)s. \tag{91}$$

Since $uu' = 1$, $\sum_{s' \in G} u(s')u'((s')^{-1}) = \sum_{s' \in G} u(s')u(s')^* = \sum_{s \in G}|u(s)|^2 = 1$.

(c) By (b), we get $u(s)$ are all zero except one which is equal to ± 1. As it contains G and U is contained in $G \cup (-G)$.

(d) Let $u \in Z[G]$ has finite order about multiplication, then $U = \langle u, G \rangle$ is a finite subgroup of multiplicative group of $Z[G]$ as the generators are commutative and have finite order. By (c), U is contained in $G \cup (-G)$, so $u \in G \cup (-G)$. It proves the proposition.

S 6.4 Note that χ_i is a class function on G for each i, so for any conjugacy class $c \subset G$, $\chi_i(s_1^{-1}) = \chi_i(s_2^{-1})$ for $s_1, s_2 \in c$. Therefore, p_i is in the center of $\mathbb{C}[G]$. Also,

$$\omega_i(p_j) = g^{-1}\sum_{s \in G}\chi_j(s^{-1})\chi_i(s) = \delta_{ij} \tag{92}$$

from the theorem 3 in chapter 2. Since $(\omega_i)_{1 \le i \le h}$ defines an algebra isomorphism from center of $\mathbb{C}[G]$ to $\mathbb{C}^h$, which is $\mathbb{C}$-vector space isomorphism, and each $(p_i)_{1 \le i \le h}$ maps onto the basis of $\mathbb{C}^h$, p_i forms a basis of center of $\mathbb{C}[G]$.

The rest properties are the consequence of calculations. Since

$$\omega_i(p_jp_k) = \omega_i(p_j)\omega_i(p_k) = \delta_{ij}\delta_{ik}, \tag{93}$$

and $(\omega_i)_{1 \le i \le h}$ is an isomorphism, $p_i^2 = p_i$ and $p_ip_j = 0$. Also, $\omega_i(1) = 1$ for all i, and

$$(\omega_i)_{1 \le i \le h} : \sum_{j=1}^{h} p_j \mapsto (1, 1, \ldots, 1), \tag{94}$$

so $\sum_{j=1}^{h} p_j = 1$.

Now, I'll prove the theroem 8 of 2.6. For a representation $\rho : G \to GL(V)$, $\rho(p_i)^2 = \rho(p_i)$, so $\rho(p_i)$ is a projection matrix. Also, $\operatorname{Im} \rho(p_i) \cap \operatorname{Im} \rho(p_j) = 0$ for $i \neq j$ for $p_i p_j = 0$. Finally, as $\sum_{i=1}^{h} p_i = 1$, $\oplus_{i=1}^{h} \operatorname{Im} \rho(p_i) = V$. Now, I need to show $\operatorname{Im} \rho(p_i) = V_i$, which is constructed by collecting irreducible submodules isomorphic to W_i.

For $j \neq i$, assume that there exists a irreducible submodule $v \in L \subset V$ which is isomorphic to W_j and $\rho(p_i)(v) \neq 0$. Since p_i is in center of $\mathbb{C}[G]$ and L is irreducible, we can restrict the domain of $\rho(p_i)$ by L and get $\operatorname{End}_{\mathbb{C}[G]}(L)$. By Schur's lemma, $\rho(p_i)$ is a homothety and $\operatorname{Tr}(\rho(p_i)) = \frac{n_i}{g} \sum_{s \in G} \chi_i(s^{-1}) \chi_j(s) = 0$. Therefore, it is contradiction, and it implies $\sum_{j \neq i} V_j \subset \ker \rho(p_i)$. It shows that $\ker \rho(p_i) = V_i$, which ends the proof.

S 6.5 Let ϕ be the algebra homomorphism from center of $\mathbb{C}[G]$ to $\mathbb{C}$. Since $\sum_{i=1}^{h} p_i = 1 \in \mathbb{C}[G]$ is maps to 1 in $\mathbb{C}$, there should exists p_{i_0} such that p_{i_0} is maps to non-zero a. Assume it is not 1, then $\frac{1}{a} p_{i_0}$ maps to 1, so $\sum_{i=1}^{h} p_i - \frac{1}{a} p_{i_0}$ maps to 0. However,

$$\phi : \left(\sum_{i=1}^{h} p_i - \frac{1}{a} p_{i_0} \right) p_{i_0} = \left(1 - \frac{1}{a} \right) p_{i_0}^2 = \left(1 - \frac{1}{a} \right) p_{i_0} \mapsto a - 1 \neq 0, \tag{95}$$

which is contradiction. Therefore, $a = 1$. Since $\phi(p_{i_0} p_j) = \phi(p_{i_0}) \phi(p_j) = 0$ for $j \neq i_0$, $\phi(p_j) = 0$ except i_0, and it should be same as ω_{i_0}. It shows that each homomorphism of center of $\mathbb{C}[G]$ is equal to one of the ω_i.

S 6.6 Let $\{c_i\}_{i=1}^{h}$ be the conjugacy classes of G. The center of $\mathbb{C}[G]$ is $\oplus_{i=1}^{h} \mathbb{C} e_i$ where $e_i = \sum_{s \in c_i} s$. Therefore, $\oplus_{i=1}^{h} \mathbb{Z} e_i$ is contained in the center of $\mathbb{Z}[G]$. Conversely, if u is in the center of $\mathbb{Z}[G]$, then $us = su$ for all $s \in G$ and $\mathbb{C}$ is in the center of $\mathbb{C}[G]$, so $uu' = u'u$ for all $u' \in \mathbb{C}[G]$. Therefore, $u \in \left(\oplus_{i=1}^{h} \mathbb{C} e_i \right) \cap \mathbb{Z}[G] = \oplus_{i=1}^{h} \mathbb{Z} e_i$.

S 6.7 Since the eigenvalues of $\rho(s)$ have absolute value 1,

$$|\chi(s)| = \left| \sum_{i=1}^{n} \lambda_i \right| \leq \sum_{i=1}^{n} |\lambda_i| = n. \tag{96}$$

The equality holds if any only if $\lambda_i = \sigma_i \lambda$ for some $\lambda \in \mathbb{C}$ with $|\lambda| = 1$ and $\sigma_i = \pm 1$ with $\sigma_i \sigma_j > 0$ for all i, j. It shows that $\rho(s)$ is homothety if and only if $|\chi(s)| \leq n$. If $\chi(s) = 1$, then $\lambda_i = 1$ and $\rho(s)$ is a homothety, which means that $\rho(s) = 1$.

S 6.8 I'll use Galois theory to solve this problem. For each λ_i, set $[\mathbb{Q}(\lambda_i) : \mathbb{Q}] = m_i$. Consider the multiple of irreducible polynomials having distinct root λ_i, we get a separable polynomial $p(x)$, and let K be the splitting field of $p(x)$. Now, we get the Galois extension $K/\mathbb{Q}$. Also, the $\operatorname{Gal}(K/\mathbb{Q})$ is a subgroup of $\prod_i \operatorname{Gal}(\mathbb{Q}(\lambda_i)/\mathbb{Q})$.

Now, let L be the splitting field of the irreducible monic polynomial having root $\xi = n^{-1} \sum_{i=1}^{n} \lambda_i$. (Since ξ is an algebraic integer, such monic polynomial should exist.) Since $\xi \in K$, L is a subfield of K, so a subgroup of $\operatorname{Gal}(K/\mathbb{Q})$. It means that the other roots of the irreducible polynomial is again a sum of roots of unity. Let $\{\sigma_i\} = \operatorname{Gal}(L/\mathbb{Q})$, then $\eta = \prod_i \sigma_i(\xi) \in \mathbb{Q}$. Furthermore, η is an algebraic integer since it is the multiple of algebraic integers, which is the sum of root of unity. Finally, each $|\sigma_i(\xi)| \leq 1$, so $|\eta| \leq 1$. It shows $\eta = \pm 1$ or 0. If $|\eta| = 1$, $|\xi| = 1$ and we get $a = \lambda_i$. If

$\eta = 0$, then there exists some σ_i such that $\sigma_i(\xi) = 0$. Then, $\sigma_i^{-1}(\sigma_i(\xi)) = \xi = 0$.

S 6.9 Let $c(s)$ be the number of elements conjugate with s. It is integer and $c(s) = c(s')$ if s and s' are in a same conjugate class. By cor 16.1, we know that $\sum_{s \in G} \frac{c(s)}{n} \chi(s)$ is an algebraic integer.

Since $\chi(s)$ and $\frac{c(s)}{n}\chi(s)$ are algebraic integer, $\mathbb{Z}\left[\chi(s), \frac{c(s)}{n}\chi(s)\right]$ which has ring structure is finitely generated as $\mathbb{Z}$ module. Since $\frac{1}{n}\chi(s) \in \mathbb{Z}\left[\chi(s), \frac{c(s)}{n}\chi(s)\right]$, $\mathbb{Z}\left[\frac{1}{n}\chi(s)\right]$ is contained $\mathbb{Z}\left[\chi(s), \frac{c(s)}{n}\chi(s)\right]$ and $\frac{1}{n}\chi(s)$ is an algebraic integer. By the previous problems, $\rho(s)$ is a homothety.

S 6.10 Let $c(s) = p^n$ for some $n \in \mathbb{Z}_{\geq 0}$. For a trivial character 1_G and an irreducible character χ not equal to trivial character (if exists),

$$\sum_{i=1}^{h} n_i \chi_i(s) = 1 + \sum_{\chi \neq 1} \chi(1)\chi(s) = g\delta_s. \tag{97}$$

Since $s \neq 1$, the RHS is zero. If there is no character satisfying $\chi(s) \neq 0$ and $\chi(1) \not\equiv 0 \mod p$,

$$1 + \sum_{\chi \neq 1} \chi(1)\chi(s) = 1 + p \sum_{\chi \neq 1} (\chi(1)/p)\chi(s) = 0. \tag{98}$$

Since $(\chi(1)/p) \in \mathbb{Z}$ and $\chi(s)$ is the sum of root of unities, so algebraic integers; therefore, $\sum_{\chi \neq 1}(\chi(1)/p)\chi(s)$ is an algebraic integer. It shows that $1/p$ is an algebraic integer, which is not true. Therefore, there should exist such irreducible character. Since $c(s)$ and n are relatively prime and $\chi(s) \neq 0$, $\rho(s)$ is an homothety by the ex. 6.9. Assume the ρ is not a unit representation, so the kernel is not G, then ρ is well-defined on G/N, and $\rho(s)$ belongs to the center of G/N...

4 Chapter 7

S 7.1

(a) Let f (resp. g) be a representation of H (resp. G) generating the character ψ (resp. φ). ψ and $\mathrm{Res}_\alpha \varphi$, are characters of H since $g \circ \alpha$ generates the character $\mathrm{Res}_\alpha \varphi$. Therefore, we get

$$\langle \psi, \mathrm{Res}_\alpha \varphi \rangle_H = \dim_\mathbb{C} \mathrm{Hom}^H(W, \mathrm{Res}_\alpha E)$$
$$\langle \mathrm{Ind}_\alpha \psi, \varphi \rangle_G = \dim_\mathbb{C} \mathrm{Hom}^G(\mathbb{C}[G] \otimes_{\mathbb{C}[H]} W, E). \tag{99}$$

I'll construct a isomorphism Ψ from $\mathrm{Hom}^H(W, \mathrm{Res}_\alpha E)$ to $\mathrm{Hom}^G(\mathbb{C}[G] \otimes_{\mathbb{C}[H]} W, E)$. For $h \in \mathrm{Hom}^H(W, \mathrm{Res}_\alpha E)$, set $\Psi(h)(g \otimes w) = g \cdot h(w)$. I'll first show that this is well-defined: for $h' : \mathbb{C}[G] \times W \to E$ by setting $h' : (g, w) \mapsto g \cdot h(w)$, it is $\mathbb{C}$-bilinear, in fact, it is $\mathbb{C}[H]$-bilinear since for $s \in H$,

$$h'(g\alpha(s), w) = (g\alpha(s)) \cdot h(w) = g \cdot (\alpha(s) \cdot h(w)) = g \cdot h(sw) = h'(g, sw). \tag{100}$$

Therefore, h' can be extend to $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} W$ and by the uniqueness, it is $\Psi(h)$. By giving $\mathbb{C}[G]$ action on $\Psi(h)$ by $g_1 \cdot (\Psi(h)(g_2 \otimes w)) = \Psi(h)(g_1 g_2 \otimes w)$, it is in $\mathrm{Hom}^G(\mathbb{C}[G] \otimes_{\mathbb{C}[H]} W, E)$.

Conversely, let $h' \in \mathrm{Hom}^G(\mathbb{C}[G] \otimes_{\mathbb{C}[H]} W, E)$, then construct h by $h(w) = h'(1 \otimes w)$ with H action given by $h(sw) = h'(1 \otimes sw) = h'(\alpha(s) \otimes w) = \alpha(s)h'(1 \otimes w) = sh(w)$ since $h(w) \in \mathrm{Res}_\alpha E$. Finally, $\Psi(h)(g \otimes w) = g \cdot h(w) = g \cdot (h'(1 \otimes w)) = h'(g \otimes w)$. It shows Ψ is an isomorphsim and we get the result.

(b) Let W^0 be the subspace of W stable under N. It exists since $0 \in W^0$. Consider a map $\psi : \mathbb{C}[G] \times W \to \mathbb{C}[G] \otimes_{\mathbb{C}[G]} W^0$ by $\psi : (gN, w) \to gN \otimes (\sum_{n \in N} nw)$. It is $\mathbb{C}[H]$ bilinaer: for $h = g'n'$ for some $h \in H$, $g' \in H/N$, and $n' \in N$,

$$\psi((gh, w)) = ghN \otimes \left(\sum_{n \in N} nw \right) = gg'N \otimes \left(\sum_{n \in N} nw \right)$$
$$\psi((g, hw)) = gN \otimes \left(\sum_{n \in N} nhw \right) = gN \otimes (g'N) \left(\sum_{n \in N} nw \right) = gg'N \otimes \left(\sum_{n \in N} nw \right). \tag{101}$$

Therefore, by the universal property, there exists a unique homomorphism $\Psi : \mathbb{C}[G] \otimes_{\mathbb{C}[H]} W \to \mathbb{C}[G] \otimes_{\mathbb{C}[G]} W^0$. If I choose $w \in W^0$, $\psi(gN, w) = gN \otimes w$, so Ψ is surjective. Also, if $\sum_i c_i g_i N \otimes w_i \mapsto 0$, it means

$$\sum_i c_i \otimes g_i \left(\sum_{n \in N} nw_i \right) = \sum_i c_i \otimes \left(\sum_{n \in N} ng_iw_i \right) = 0 \tag{102}$$

and

$$\sum_i c_i g_i N \otimes w_i = \sum_i c_i g_i N g_i^{-1} \otimes g_i w_i = \sum_i c_i N \otimes g_i w_i = \sum_i c_i N \otimes ng_i w_i, \tag{103}$$

for all $n \in N$, so ... bijective and isomorphism.

S 7.2 Using the definition of induced class function, we get

$$\text{Ind}_H^G(1_H)(s) = h^{-1} \sum_{\substack{t \in G \\ t^{-1}st \in H}} 1_H(t^{-1}st). \tag{104}$$

It is the number of $t \in G$ divided by h such that $t^{-1}st \in H$, i.e. for given representatives $\{\sigma_i\}$ of G/H, the number of representatives satisfying $\sigma_i^{-1}s\sigma_i \in H$. Since $s \cdot (\sigma_i H) = \sigma_i H$ if and only if $\sigma_i^{-1}s\sigma_i \in H$, we get

$$\text{Ind}_H^G(1_H) = \chi. \tag{105}$$

Now, we know $\text{Ind}_H^G(1_H) = \chi$ and $\text{Res}_H 1_G = 1_H$. Using the Frobenius reciprocity formula,

$$1 = \langle 1_H, \text{Res}_H 1_G \rangle = \langle \chi, 1_G \rangle. \tag{106}$$

It means that the representation generating the character χ has one unit irreducible representation. Decomposing the representation into irreducible ones, we get $\chi = 1 \oplus \theta$ for some (not necessarily irreducible) representation θ and the character of θ is $\chi - 1$. (In fact, it may be 0: if $H = G$, then $\chi = 1_G$, so θ is 0 representation. If $[G : H] \geq 2$, then it has dimension bigger than 1, so θ is not 0 representaion.)

From the exercise 2.6, $\chi - 1$ is irreducible if and only if G acts on G/H doubly transitively, or equivalently it satisfies $\langle \chi, \chi \rangle = 2$; note that $\chi(s)$ is real-valued for all s as it is just counting representatives σ_i making $\sigma_i^{-1}s\sigma_i \in H$. Definitely, H is not a normal subgroup of G if it is doubly transitive on G/H.

S 7.3

(a) Since $H \cap tHt^{-1} = 1$ for all $t \notin H$, for a represetation $\{r_i\} \subset G$ of G/H with $r_1 = 1$, $H \cap r_i H r_i^{-1} = 1$ for $i \geq 2$. Also, for $i \neq j$ with $i, j \geq 2$, $H \cap r_1^{-1}r_2 H (r_1^{-1}r_2)^{-1} = 1$, so $r_1 H r_1^{-1} \cap r_2 H r_2^{-1} = 1$. Finally, for any $t = r_i h \in G$, $tHt^{-1} = r_i h H h^{-1} r_i^{-1} = r_i H r_i^{-1}$. It shows that

$$N = G \setminus \left(\cup_{t \in G} tHt^{-1} \right) = G \setminus \left(\cup_{r \in R} rHr^{-1} \right), \tag{107}$$

and

$$|N| = |G| - |R|(|H| - 1) - 1 = g - \frac{g}{h}(h - 1) - 1 = \frac{g}{h} - 1. \tag{108}$$

(b) Note that the conjugacy class of 1 is always 1. Let's define $\tilde{f}$ by

$$\tilde{f}(g) = \begin{cases} f(h) & \text{if there exists } t \in G \text{ and } h \in H \text{ such that } tht^{-1} = g \\ f(1) & \text{if } g \in N. \end{cases} \tag{109}$$

I'll show that this is well-defined class function. If $s \notin N$, there exists $t \in G$ and $h \in H$ such that $tht^{-1} = s$. Assume there exists another $t_1 \in G$ and $h_1 \in H$ making $t_1 h_1 t_1^{-1} = g$, then $h_1 = t_1^{-1}th(t_1^{-1}t)^{-1}$, so $f(h_1) = f(h)$. Therefore, it is well-defined function. Now, assume h_1 and h_2 are in a same conjugacy class in G, i.e. there exists $t \in G$ such that $th_1t^{-1} = h_2$. If $h_2 \notin N$, $h_1 \notin N$ and we get $\tilde{f}(h_1) = \tilde{f}(h_2)$ by the definition. If $h_2 \in N$, then $h_1 \in N$ and it also have same $\tilde{f}$ value. Therefore, it is a class function.

I'll show the uniqueness. However, by the definition of N, there exists $t \in G$ such that $t^{-1}st \in H$ if and only if $s \in N^c$. Therefore, $\tilde{f}$ which extends f and $\tilde{f} \equiv f(1)$ on N is unique.

(c) I'll divide the case into three cases: $s = 1$, $s \in N \setminus \{1\}$, and $s \in N^c \setminus \{1\}$.

1. If $s = 1$, $\tilde{f}(1) = \frac{g}{h} f(1) - f(1) \left(\frac{g}{h} - 1 \right) = f(1)$.

2. If $s \in N \setminus \{1\}$, $\tilde{f}(s) = 0 - f(1)(0 - 1) = f(1)$, cf. the definition of induced character.

3. If $s \in N^c \setminus \{1\}$, then there exists $t \in G$ and $h \in H$ such that $tht^{-1} = s$. Since $s \neq 1$ and H is a Frobenius subgroup of G, the only possible t' making $(t')^{-1} st' \in H$ is $t' \in tH$. Therefore,

$$\operatorname{Ind}_H^G f(s) = \frac{1}{|H|} \sum_{\substack{t' \in G \\ (t')^{-1} st' \in H}} f((t')^{-1} st') = f(t^{-1} st) = f(h), \tag{110}$$

and

$$\tilde{f}(s) = f(h) - f(1)(1_H(h) - 1_G(s)) = f(h). \tag{111}$$

(d) In the proof of (c), note that for any $s \in H$, $\tilde{f}(s) = \operatorname{Ind}_H^G f(s)$. Therefore, $\operatorname{Res}_H \operatorname{Ind}_H^G f(s) = f(s)$ for any class function f. There is no confusion about the subscript G and H of inner product, so I'll omit it. Also, note that $f(1) \in \mathbb{R}$.

$$
\begin{aligned}
\langle \tilde{f}, \tilde{f} \rangle &= \langle \operatorname{Ind}_H^G f - f(1)(\operatorname{Ind}_H^G(1_H) - 1), \operatorname{Ind}_H^G f - f(1)(\operatorname{Ind}_H^G(1_H) - 1_G) \rangle \\
&= \langle \operatorname{Ind}_H^G f, \operatorname{Ind}_H^G f \rangle - 2f(1) \langle \operatorname{Ind}_H^G f, \operatorname{Ind}_H^G(1_H) - 1 \rangle + (f(1))^2 \langle \operatorname{Ind}_H^G(1_H) - 1_G, \operatorname{Ind}_H^G(1_H) - 1_G \rangle \\
&= \langle \operatorname{Ind}_H^G f, \operatorname{Ind}_H^G f \rangle - 2f(1) \left(\langle \operatorname{Ind}_H^G f, \operatorname{Ind}_H^G(1_H) \rangle - \langle \operatorname{Ind}_H^G f, 1_G \rangle \right) \\
&\quad + (f(1))^2 \left(\langle \operatorname{Ind}_H^G(1_H), \operatorname{Ind}_H^G(1_H) \rangle - 2 \langle \operatorname{Ind}_H^G(1_H), 1_G \rangle + \langle 1_G, 1_G \rangle \right) \\
&= \langle f, \operatorname{Res}_H \operatorname{Ind}_H^G f \rangle - 2f(1) \left(\langle f, \operatorname{Res}_H \operatorname{Ind}_H^G(1_H) \rangle - \langle f, 1_H \rangle \right) \\
&\quad + (f(1))^2 \left(\langle 1_H, \operatorname{Res}_H \operatorname{Ind}_H^G(1_H) \rangle - 2 \langle 1_H, \operatorname{Res}_H(1_G) \rangle + \langle 1_G, 1_G \rangle \right) \\
&= \langle f, \operatorname{Res}_H \operatorname{Ind}_H^G f \rangle - 2f(1) \left(\langle f, 1_H \rangle - \langle f, 1_H \rangle \right) + (f(1))^2 \left(\langle 1_H, 1_H \rangle - 2 \langle 1_H, 1_H \rangle + \langle 1_G, 1_G \rangle \right) \\
&= \langle f, f \rangle.
\end{aligned}
\tag{112}
$$

In the third to fourth line, I used the Frobenius reciprocity formula.

(e) Since $\tilde{f}(1) = f(1)$ and $f(1) \in \mathbb{Z}_{\geq 0}$, $\tilde{f} \in \mathbb{Z}_{\geq 0}$. Also, $\langle \tilde{f}, \tilde{f} \rangle = \langle f, f \rangle = 1$. Note that we don't know whether $\tilde{f}$ is a character now on.

For any irreducible representation φ of G,

$$
\begin{aligned}
\langle \varphi, \tilde{f} \rangle &= \langle \varphi, \operatorname{Ind}_H^G f \rangle - f(1) \langle \varphi, \operatorname{Ind}_H^G 1_H - 1_G \rangle \\
&= \langle \operatorname{Res}_H \varphi, f \rangle - f(1) \left(\langle \operatorname{Res}_H \varphi, 1_H \rangle - \langle \varphi, 1_G \rangle \right).
\end{aligned}
\tag{113}
$$

Since f and 1_H are irreducible characters of H, $\operatorname{Res}_H \varphi$ is a character, and 1_G is an irreducible character of G, all the terms in the above equation are in $\mathbb{Z}_{\geq 0}$. Therefore, $\tilde{f}$ is a linear combination with integer coefficients of irreducible character of G. Note that we don't know whether $\tilde{f}$ is a character in this step since the coefficient may be negative. Let's write $\tilde{f} = \sum_{i=1}^m n_i \varphi_i$ where $n_i \in \mathbb{Z}$ and φ_i are irreducible characters of G, then

$$\langle \tilde{f}, \tilde{f} \rangle = \sum_{i=1}^m n_i^2 \tag{114}$$

25

and it is 1 if and only if $n_i = 0$ except one i, which should be ± 1. Also, if the coefficient were 1, $\tilde{f}(1) < 0$, which is not true. Therefore, $\tilde{f}$ is an irreducible character of G.

Since $\tilde{f}(1) = f(1) = \tilde{f}(n)$ for all $n \in N$ and $\tilde{f}(1)$ represents the degree of the representation corresponding to the character, using exercise 6.7, we get $\rho(s) = 1$ for all $s \in N$.

(f) Let $\rho : H \to GL(V)$ be an irreducible representation of H. By the previous analysis, the character χ of ρ extends to an irreducible character χ' of G; let the corresponding irreducible representation ρ'. Since $\mathrm{Res}_H \rho'$ have the same character as ρ as checked above, it is isomorphic to ρ, which explains the term "extension".

Any linear representation ρ of H is decomposed into irreducible ones and the character becomes the sum of the irreducible characters. Since Ind_H^G and Res_H are linear maps for class functions, the above arguments applies to each irreducible character consisting the character function. Finally, the sum of extended irreducible character is a character of some linear representation ρ' of G, which can be considered as a extension of ρ since $\mathrm{Res}_H \rho'$ is isomorphic to ρ by the same reason above.

$\rho' = \oplus_{i=1}^m \rho_i'$ where ρ_i' is the extension of irreducible representation ρ_i of H and $\rho_i'(n) = 1$ for all $n \in N$ and i, so $\rho'(n) = 1$. Therefore, $(\rho')^{-1}(1)$ contains $N \cup 1$. If $N \cup 1$ forms a subgroup in G, it is a normal subgroup of G as a subgroup of the kernel. Also, $(N \cup \{1\}) \cap H = 1$, so if $n_1 h_1 = n_2 h_2$ in $(N \cup \{1\})H$, $n_2^{-1} n_1 = h_2 h_1^{-1} \in (N \cup \{1\}) \cap H$, so $n_1 = n_2$ and $h_1 = h_2$, which implies $|(N \cup \{1\})H| = |N \cup \{1\}||H| = g$ and $(N \cup \{1\})H = G$ as a set. As a result, G is the semidirect product of H and $N \cup \{1\}$.

To end the proof, I need to show that $N \cup \{1\}$ is a subgroup of G. Consider a regular representation r_H of H. The character χ of r_H is 0 except at 1, $|H|$. Therefore,

$$\tilde{\chi}(s) = \begin{cases} n & s \in N \cup \{1\} \\ 0 & s \in (N \cup \{1\})^c. \end{cases} \tag{115}$$

which means that the kernel of extension of r_H is exactly $N \cup \{1\}$. It shows that $N \cup \{1\}$ is a normal subgroup of G.

(g) I'll write $H^* = H \setminus \{1\}$ and $A^* = A \setminus \{1\}$. If H is a Frobenius subgroup of G, then the latter statement is easily followed by the definition since $A^* \cap H^* = \emptyset$, for each $s \in H^*$ and $t \in A^*$, $t \notin H$ and $tst^{-1} \neq s$. Hence, I'll show the converse. Assume there exists $h \in H^*$ and $t \notin H$ such that $tht^{-1} \in H$. Writing $G = A \rtimes H$, $t = (a', 1)(1, h')$ for some $a' \in A^*$ and $h' \in H$. Therefore,A

$$tht^{-1} = (a', 1)(1, h'h(h')^{-1})((a')^{-1}, 1) \in H \tag{116}$$

Since $h \in H^*$, $h'h(h')^{-1} \in H^*$. It means that $a'((h'h(h')^{-1}) \cdot (a')^{-1}) = 1$ in A. By replacing $t = ((a')^{-1}, 1)$, $s = (1, h'h(h')^{-1})$,

$$sts^{-1} = (1, h'h(h')^{-1})((a')^{-1}, 1)(1, h'h^{-1}(h')^{-1}) = ((h'h(h')^{-1}) \cdot (a')^{-1}, 1) = ((a')^{-1}, 1) = t \tag{117}$$

which contradicts the assumption. Therefore, H is a Frobenius subgroup of G.

S 7.4 Let's first configure what is H_s. For $s = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ and $t = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, sts^{-1} is

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} = \begin{pmatrix} a\alpha\delta - b\alpha\gamma - d\gamma\beta & -a\alpha\beta + b\alpha^2 + d\alpha\beta \\ a\gamma\delta - b\gamma^2 - d\gamma\delta & -a\beta\gamma + b\alpha\gamma + d\alpha\delta \end{pmatrix} \tag{118}$$

To make it be contained in H, we need to impose $a\gamma\delta - b\gamma^2 - d\gamma\delta = 0$. Assume $s \notin H$, then $\gamma \neq 0$, so $\delta(a - d) - b\gamma = 0$. Therefore,

$$\begin{pmatrix} a\alpha\delta - b\alpha\gamma - d\gamma\beta & -a\alpha\beta + b\alpha^2 + d\alpha\beta \\ a\gamma\delta - b\gamma^2 - d\gamma\delta & -a\beta\gamma + b\alpha\gamma + d\alpha\delta \end{pmatrix} = \begin{pmatrix} d & -a\alpha\beta + b\alpha^2 + d\alpha\beta \\ 0 & a \end{pmatrix} \tag{119}$$

using $\alpha\delta - \gamma\beta = 1$. Also,

$$\gamma(-a\alpha\beta + b\alpha^2 + d\alpha\beta) = \alpha(-a\beta\gamma + \delta(a - d)\alpha + d\gamma\beta) = \alpha(a - d), \tag{120}$$

so

$$\begin{pmatrix} d & -a\alpha\beta + b\alpha^2 + d\alpha\beta \\ 0 & a \end{pmatrix} = \begin{pmatrix} d & \alpha\gamma^{-1}(a - d) \\ 0 & a \end{pmatrix} \tag{121}$$

Therefore,

$$H_s = \left\{ \begin{pmatrix} d & \alpha\gamma^{-1}(a - d) \\ 0 & a \end{pmatrix} : ad = 1 \right\}. \tag{122}$$

Therefore, for $s \notin H$,

$$\begin{aligned}
\langle \rho^s, \operatorname{Res}_{H_s}(\rho) \rangle &= \frac{1}{|H_s|} \sum_{t \in H_s} \rho^s(t^{-1}) \left(\operatorname{Res}_{H_s} \rho \right)(t) \\
&= \frac{1}{k} \sum_{d \in k \setminus \{0\}} \chi_\omega^s \left(\begin{pmatrix} a & -\alpha\gamma^{-1}(a - d) \\ 0 & d \end{pmatrix} \right) \chi_\omega \left(\begin{pmatrix} d & \alpha\gamma^{-1}(a - d) \\ 0 & a \end{pmatrix} \right) \\
&= \frac{1}{k} \sum_{d \in k \setminus \{0\}} \chi_\omega \left(\begin{pmatrix} d & -b \\ 0 & a \end{pmatrix} \right) \chi_\omega \left(\begin{pmatrix} d & \alpha\gamma^{-1}(a - d) \\ 0 & a \end{pmatrix} \right) = \frac{1}{|k|} \sum_{d \in k \setminus \{0\}} \omega^2(d)
\end{aligned} \tag{123}$$

Assume $\omega^2 \neq 1$. Since k is finite field, k^* is a cyclic group about an element $x \in k^*$.(cf. **D&F** proposition 9.18.) Therefore, $\omega^2(x) \neq 1$ is a root of unity such that the order of $\omega^2(x)$ divides $|k| - 1$. It shows that

$$\sum_{d \in k \setminus \{0\}} \omega^2(d) = \sum_{i=1}^{|k|-1} \left(\omega^2(x) \right)^i = 0. \tag{124}$$

Now, the induced representation satisfies all the conditions in the Mackey's criterion, so it is irreducible. (Since χ_ω is the character of degree 1, the condition (a) is automatically satisfied.)

5 Chapter 8

(**S 8.1**) For each i, the number of element in each class X/H is h/h_i, and the number of irreducible representations of A is a. Therefore, we get

$$a = \sum_i h/h_i. \tag{125}$$

Since $\deg \chi_i = 1$ and the sum of squares of the degrees of the irreducible representatinos of H_i is h_i, we get

$$\sum_\rho \left(\theta_{i,\rho}(1) \right)^2 = \frac{h^2}{h_i^2} \sum_\rho \rho(1)^2 = \frac{h^2}{h_i} \tag{126}$$

Finally, we get

$$h \sum_i h/h_i = ha = g. \tag{127}$$

It means that $\theta_{i,\rho}$ is the all of the irreducible representations of G.

S 8.2

I'll first show a (trivial) proposition.

Proposition 5. *Let $(\rho_1, V_1), (\rho_2, V_2)$ are representations on a group G. If ρ_2 has degree 1, $\rho_1 \otimes \rho_2 \simeq \rho_2 \rho_1$, which act on V_1 by $\rho_2(s)(\rho_1(s))(v)$ identifying $\rho_2(s) \in \mathbb{C}^\times$.*

Proof. Since $\dim V_2 = 1$, $V_2 \simeq \mathbb{C}$. Identifying V_2 with $\mathbb{C}$, for each $s \in G$, $\rho_2(s)$ acts on $\mathbb{C}$ by scalar multiplication, so in $\mathbb{C}^\times$. Let $\varphi : V_1 \otimes_{\mathbb{C}} V_2 \to V_1$ by $(v_1, c_2) \mapsto c_2 v_1$. This is definitely vector space isomorphism. Furthermore, it is representation isomorphism since

$$\begin{aligned} \varphi \left((\rho_1 \otimes \rho_2(s))((v_1, c_2)) \right) &= \varphi \left((\rho_1(s))(v_1), (\rho_2(s))(c_2) \right) \\ &= (\rho_2(s))(c_2)(\rho_1(s))(v_1) \\ &= (\rho_2(s))(1)(\rho_1(s))(c_2 v_1) \\ &= (\rho_2 \rho_1(s)) \circ \varphi(v_1, c_2). \end{aligned} \tag{128}$$

for any $s \in G$, $v_1 \in V_1$, and $c_2 \in \mathbb{C}$. $\qquad \square$

Remark 6. If ρ_2 is trivial, then $\rho_1 \otimes \rho_2 \simeq \rho_1$.

Remark 7. Since $\rho_1 \otimes \rho_2 \simeq \rho_2 \otimes \rho_1$, we get $\rho_1 \otimes \rho_2 \simeq \rho_2$ if ρ_1 is trivial.

D_n The textbook denotes the dihedral group with order $2n$ by $D_n = \{r^k s^\sigma; \sigma \in \{0, 1\}, 0 \le k \le n - 1\}$. For the generator $s, r \in D_n$, let's write $A = \{r^k : 0 \le k < n\}$, $H = \{1, s\}$. Note that both subgroups are abelian and normal to D_n. Since $A \cap H = \{1\}$ and $|A||H| = 2n = |D_n|$, we get $D_n = AH$ as AH forms a subgroup in D_n and it has same cardinal as D_n. Finally, it has inner semi-direct product structure: for any $a_1, a_2 \in A$ and $h_1, h_2 \in H$,

$$a_1 h_1 a_2 h_2 = (a_1 h_1 a_2 h_1^{-1})(h_1 h_2). \tag{129}$$

Note that for $0 \leq m \leq n-1$, $\chi_m(r^k) = \exp\left(\frac{2\pi imk}{n}\right)$ are well-defined irreducible group representations from A to $\mathbb{C}^\times$. Each χ_i are distinct since

$$(\chi_i, \chi_j) = \frac{1}{n} \sum_{k=0}^{n-1} \exp\left(\frac{2\pi(i-j)mk}{n}\right) = \delta_{ij}. \tag{130}$$

Also, note that χ_i forms a group X under multiplication since $\chi_i \chi_j = \chi_{i+j \mod n}$. The conjugation action of s to r^k is $s^{-1} r^k s = r^{-k}$, so $s\chi_i = \chi_{n-i}$.

If n is even, $\chi_{0 \leq i \leq n/2}$ is a system of representatives for the orbits of H in X with $\chi_0 \equiv 1$ and $s\chi_{n/2} = \chi_{n/2}$. For $1 \leq i < n/2$, $1 \in H$ only fixes χ_i. Let' set $H_i = 1$, then any irreducible representatinos of H_i is trivial and we just need to consider $\mathrm{Ind}_A^G \chi_i \simeq \mathbb{C}[G] \otimes_{\mathbb{C}[A]} \mathbb{C}$. Under basis $1 \otimes 1$ and $s \otimes 1$,

$$\mathrm{Ind}_A^G \chi_m(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$\mathrm{Ind}_A^G \chi_m(r) = \begin{pmatrix} \exp\left(\frac{2\pi im}{n}\right) & 0 \\ 1 & \exp\left(-\frac{2\pi im}{n}\right) \end{pmatrix} \tag{131}$$

for $1 \leq m < n/2$.

For $m = 1$, χ_0 is trivial, so any element in H fixes χ_0. Therefore, extend χ_0 to $G = AH$ by setting $\chi_0(r^k s^\sigma) = \chi_0(r^k)$. For the trivial representation ρ of H, let $\tilde{\rho}(r^k s^\sigma) = \rho(s^\sigma)$, which becomes a representation on $G = AH$. Now, $\chi_0 \otimes \tilde{\rho}$ is a trivial representation on G. For another representation ρ' on H which sends s to -1, we can repeat the above argument and get a representation $\chi_0 \otimes \tilde{\rho}' \simeq \tilde{\rho}'$ on G since χ_0 is trivial.

For $m = n/2$, repeat the above argument and get

$$(\chi_{n/2} \otimes \tilde{\rho})(r^k s^\sigma) = (-1)^k$$
$$(\chi_{n/2} \otimes \tilde{\rho}')(r^k s^\sigma) = (-1)^k(-1)^\sigma. \tag{132}$$

Finally, apply proposition 25 to say that we found all the irreducible representations of G.

For odd n, we can repeat the above argument except considering $n/2$ case: $\mathrm{Ind}_A^G \chi_m$ for $1 \leq m \leq \frac{n-1}{2}$, $\chi_0 \otimes \tilde{\rho}$, and $\chi_0 \otimes \tilde{\rho}'$.

$\mathfrak{A}_4$ Let's consider $\mathfrak{A}_4$ as the group of even permutation of a set $\{1, 2, 3, 4\}$. Set $t = (1\ 2\ 3)$. For $A = \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ and $H = \{1, t, t^2\}$, I'll show that $\mathfrak{A}_4 \simeq A \rtimes H$ which is again given by inner semidirect product structure. Note that A is a normal subgroup of $\mathfrak{A}_4$ since conjugation action just permutes the numbers in the orbits, for example, for $\sigma \in \mathfrak{A}_4$,

$$\sigma(1\ 2)(3\ 4)\sigma^{-1} = (\sigma(1)\ \sigma(2))(\sigma(3)\ \sigma(4)). \tag{133}$$

It shows that AH forms a subgroup of $\mathfrak{A}_4$. Since $A \cap H = \{1\}$ and $|A||H| = 12 = |\mathfrak{A}_4|$, $\mathfrak{A}_4 = AH$. Finally, it satisfies the inner semidirect product structure following the argument in D_n.

Let's construct group representation of A by following:

	1	(1 2)(3 4)	(1 3)(2 4)	(1 4)(2 3)
χ_1	1	1	1	1
χ_2	1	1	-1	-1
χ_3	1	-1	1	-1
χ_4	1	-1	-1	1

Note that $(\chi_i, \chi_j) = \delta_{ij}$, so each are irreducible and distinct to each other. It forms a group X about multiplication: χ_1 is identity, $\chi_2\chi_3 = \chi_3\chi_2 = \chi_4$, $\chi_3\chi_4 = \chi_4\chi_3 = \chi_2$, $\chi_4\chi_2 = \chi_2\chi_4 = \chi_3$, and $\chi_{2\leq i\leq 4}^2 = \chi_1$. For conjugation about t by $t^{-1}st$ for $s \in A$,

$$
\begin{aligned}
1 &\mapsto 1 \\
(1\ 2)(3\ 4) &\mapsto (1\ 3)(2\ 4) \\
(1\ 3)(2\ 4) &\mapsto (1\ 4)(2\ 3) \\
(1\ 4)(2\ 3) &\mapsto (1\ 2)(3\ 4).
\end{aligned}
\tag{134}
$$

It shows that $t\chi_4 = \chi_3$, $t\chi_3 = \chi_2$, and $t\chi_2 = \chi_4$ where the action is given by $(t\chi)(s) = \chi(t^{-1}st)$. It shows that χ_1, χ_2 are a system of representatives for the orbits of H in X. For χ_1, all $h \in H$ satisfies $h\chi_1 = \chi_1$ and for χ_2, only 1 makes $1\chi_2 = \chi_2$.

For χ_1, consider irreducible representations $\rho_m : H \to \mathbb{C}^\times$ such that $\rho_m(t) = \exp\left(\frac{2\pi i m}{3}\right)$ for $0 \leq m \leq 2$; since H is cyclic group, ρ_m are all the irreducible representations of H. For $G = AH$, extend χ_i to G by $\chi_i(ah) = 1$, and let $\tilde{\rho}_m(ah) = \rho_m(h)$. Since $\chi_1 \otimes \tilde{\rho}_m$ is already a representation on G having degree 1, the induced representation is again $\chi_1 \otimes \tilde{\rho}_m$. Also, it is isomorphic to $\tilde{\rho}_m$ since χ_1 is trivial.

For χ_2, the fixing group $H_2 = 1$, so the irreducible representation is only trivial representation for H_2. Now, we take $\mathrm{Ind}_A^G \chi_2 \simeq \mathbb{C}[G] \otimes_{\mathbb{C}[A]} \mathbb{C}$, which have matrix form under basis $1 \otimes 1$, $t \otimes 1$, and $t^2 \otimes 1$:

$$
\begin{aligned}
\mathrm{Ind}_A^G \chi_2(1) &= 1 \\
\mathrm{Ind}_A^G \chi_2(t) &= \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \\
\mathrm{Ind}_A^G \chi_2((1\ 2)(3\ 4)) &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \\
\mathrm{Ind}_A^G \chi_2((1\ 3)(2\ 4)) &= \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
\mathrm{Ind}_A^G \chi_2((1\ 4)(2\ 3)) &= \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.
\end{aligned}
\tag{135}
$$

The above representations are all irreducible, distinct, and shows all the irreducible representations of $\mathfrak{A}_4$ by proposition 25.

$\mathfrak{S}_4$ Again set A as in $\mathfrak{A}_4$ and set $H = \{s \in \mathfrak{S}_4 : s \cdot 4 = 4\}$. By the same reason in $\mathfrak{A}_4$, we get $G = AH$ with inner semi-direct product structure since $|H| = 6$. Unfortunately, H is not an

cyclic group now, but we know that H is group isomorphic to D_3, so we can use the first case. χ_1, χ_2 are a system of representatives for the orbits of H in X, and only (1 2) fixes χ_2 in H.

Since χ_1 is trivial, any element in H fixes χ_1. For any irreducible representation ρ on H, we can extend it by $\tilde{\rho}$ to $G = AH$ as in $\mathfrak{A}_4$; note that $\chi_1 \otimes \tilde{\rho} \simeq \tilde{\rho}$. For the degree 2 irreducible representation ρ of H, we get

$$
\begin{aligned}
\tilde{\rho}(a) &= 1 \\
\tilde{\rho}((1\ 2\ 3)) &= \begin{pmatrix} \exp\left(\frac{2\pi i}{3}\right) & 0 \\ 0 & \exp\left(-\frac{2\pi i}{3}\right) \end{pmatrix} \\
\tilde{\rho}((1\ 2)) &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}
\end{aligned}
\tag{136}
$$

for $a \in A$. For non-trivial degree 1 representation ρ' of H,

$$
\begin{aligned}
\tilde{\rho}'(a) &= 1 \\
\tilde{\rho}'((1\ 2\ 3)) &= 1 \\
\tilde{\rho}'((1\ 2)) &= -1
\end{aligned}
\tag{137}
$$

for $a \in A$. The left one is trivial representation on G.

As χ_2 is only fixed by (1 2) in H, $H_2 = \{1, (1\ 2)\}$ and we can extend χ_2 to AH_2. For trivial representation ρ on H_2, extend it to AH_2, which is again trivial, so the tensor of two representations is isomorphic ot χ_2. Finally, considering $\mathrm{Ind}_{AH_2}^G \chi_2 \simeq \mathbb{C}[G] \otimes_{\mathbb{C}[AH_2]} \mathbb{C}$ with basis $1 \otimes 1$, $(1\ 3) \otimes 1$, and $(1\ 4) \otimes 1$,

$$
\begin{aligned}
\mathrm{Ind}_{AH_2}^G \chi_2(1) &= 1 \\
\mathrm{Ind}_{AH_2}^G \chi_2((1\ 2\ 3)) &= \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix} \\
\mathrm{Ind}_{AH_2}^G \chi_2((1\ 2)) &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix} \\
\mathrm{Ind}_{AH_2}^G \chi_2((1\ 2)(3\ 4)) &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \\
\mathrm{Ind}_{AH_2}^G \chi_2((1\ 3)(2\ 4)) &= \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
\mathrm{Ind}_{AH_2}^G \chi_2((1\ 4)(2\ 3)) &= \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.
\end{aligned}
\tag{138}
$$

For the non-trivial irreducible representation ρ' of H_2, repeating above procedure, we get

$$\mathrm{Ind}_{AH_2}^{G}\left(\chi_2 \otimes \tilde{\rho}'\right)(1) = 1$$

$$\mathrm{Ind}_{AH_2}^{G}\left(\chi_2 \otimes \tilde{\rho}'\right)((1\ 2\ 3)) = \begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}$$

$$\mathrm{Ind}_{AH_2}^{G}\left(\chi_2 \otimes \tilde{\rho}'\right)((1\ 2)) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

$$\mathrm{Ind}_{AH_2}^{G}\left(\chi_2 \otimes \tilde{\rho}'\right)((1\ 2)(3\ 4)) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \tag{139}$$

$$\mathrm{Ind}_{AH_2}^{G}\left(\chi_2 \otimes \tilde{\rho}'\right)((1\ 3)(2\ 4)) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\mathrm{Ind}_{AH_2}^{G}\left(\chi_2 \otimes \tilde{\rho}'\right)((1\ 4)(2\ 3)) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Applying proposition 25, we get all the irreducbile distinct representations of $\mathfrak{S}_4$.

8.3 Since

$$1 \trianglelefteq \langle r \rangle \trianglelefteq D_n, \tag{140}$$

it is supersolvable. The center of D_n is non-trivial if and only if $2 \mid n$, and the center is $r^{n/2}$. Taking quotient of it, we get $D_{n/2}$, so by the induction process, we get the statement.

8.4 $\mathfrak{A}_4$ is solvable since for $V = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$, we get

$$1 \trianglelefteq V \trianglelefteq \mathfrak{A}_4. \tag{141}$$

However, it is not supersolvable since there is no normal cyclic subgroup of G. By the problem 8.5, we know that $\mathfrak{S}_4$ is also not supersolvable, but solvable by

$$1 \trianglelefteq V \trianglelefteq \mathfrak{A}_4 \trianglelefteq \mathfrak{S}_4. \tag{142}$$

8.5 Assume that G is solvable, so there exists a sequence

$$1 = G_1 \trianglelefteq \cdots \trianglelefteq G_n = G. \tag{143}$$

such that G_i/G_{i-1} are abelian. For any subgroup $H \leq G$, my claim is that

$$1 = G_1 \cap H \trianglelefteq \cdots \trianglelefteq G_n \cap H = H. \tag{144}$$

Note that I need to show two conditions: $G_{i-1} \cap H \trianglelefteq G_i \cap H$ and $(G_i \cap H)/(G_{i-1} \cap H)$ is abelian. The first one is easy: for $g \in G_i \cap H$, $g(G_{i-1} \cap H)g^{-1} \subset G_{i-1} \cap H$, and G is a finite group. For second, choose representatives $g_1, g_2 \in (G_i \cap H)/(G_{i-1} \cap H)$. Seeing $g_1, g_2 \in G_i$, we know that

$g_1^{-1}g_2^{-1}g_1g_2 \in G_{i-1}$. Since $g_1, g_2 \in H$, we know that $g_1^{-1}g_2^{-1}g_1g_2 \in G_{i-1} \cap H$, which shows that $(G_i \cap H)/(G_{i-1} \cap H)$ is abelian.

For supersolvable case, I need to show that $(G_i \cap H)/(G_{i-1} \cap H)$ is cyclic. For a generator x of G_i/G_{i-1}, choose smallest $k > 0$ such that $x^k G_{i-1} \cap H \neq \emptyset$, if there does not exists, choose $k = 0$. I claim that it is again a generator of $(G_i \cap H)/(G_{i-1} \cap H)$.

For $k = 0$ case, it means that $G_i \cap H = 1$ as $\cup_{k \in \mathbb{Z}} x^k G_{i-1} = G_i$. For $k > 0$ case, choose $y \in G_{i-1}$ such that $x^k y \in H$. It shows that $x^k y \in G_i \cap H$. Also, $\cup_{n \in \mathbb{Z}} (x^k y)^n (G_{i-1} \cap H) = G_i \cap H$: we know that

$$(\cup_{n \in \mathbb{Z}} x^n G_{i-1}) \cap H = \cup_{n \in \mathbb{Z}} ((x^n G_{i-1}) \cap H) = G_i \cap H. \tag{145}$$

Since k is the minimum number, we know that $(x^i G_{i-1}) \cap H = \emptyset$ for $0 \leq i < k$, and k is in fact the period since $x^{n_1} G_{i-1}, x^{n_2} G_{i-1} \cap H \neq \emptyset$ implies $(x^{n_1} y_1)(x^{n_2} y_2)^{-1} = x^{n_1 - n_2} y \in H$ where $y \in G_{i-1}$. It shows that

$$(\cup_{n \in \mathbb{Z}} x^n G_{i-1}) \cap H = \left(\cup_{n \in \mathbb{Z}} x^{kn} G_{i-1}\right) \cap H = \left(\cup_{n \in \mathbb{Z}} (x^k y)^n G_{i-1}\right) \cap H = G_i \cap H \tag{146}$$

For nilpotent case, I again need to show that $(G_i \cap H)/(G_{i-1} \cap H) \leq \mathcal{Z}(H/(G_{i-1} \cap H))$. Choose $g_1 \in G_i \cap H$ and $g_2 \in H$. Since $g_1 \in G_i$ and $g_2 \in G$, $g_1^{-1}g_2^{-1}g_1g_2 \in G_{i-1}$. As $g_1, g_2 \in H$, it means $g_1^{-1}g_2^{-1}g_1g_2 \in G_{i-1} \cap H$, so $g_1 g_2(G_{i-1} \cap H = g_2 g_1(G_{i-1} \cap H$ for all $g_2 \in H$. It ends the proof.

Quotient case: Note that I need to show two conditions: $G_{i-1}/H \trianglelefteq G_i/H$ and $(G_i/H)/(G_{i-1}/H)$ is abelian. The first one is easy since by considering $\pi : G \to G/H$, so

$$\pi(gG_{i-1}) = (gH)(G_{i-1}H) = (G_{i-1}H)(gH) = \pi(G_{i-1}g). \tag{147}$$

Using the second isomorphism theorem, we know that

$$(G_i/H)/(G_{i-1}/H) \simeq G_i/G_{i-1}, \tag{148}$$

which ends proof.

Note that above proof applies to supersolvable case. Now, I'll assume G is nilpotent group. The proof is in HW9...

6 Chapter 9

S 9.1

Let's write

$$\varphi = \sum_{\chi_i:\text{irr. char}} c_i \chi_i \tag{149}$$

for $c_i \in \mathbb{C}$; this is possible since the set of irreducible representation of G forms a basis of the class function space. The first condition is translated as follows:

$$\sum_{s \in G} \varphi(s) = 0. \tag{150}$$

In the problem 6.7, we showed that $|\chi(s)| \leq \chi(1)$ for irreducible character χ. For each irreducible representation χ,

$$\begin{aligned}
\text{Re}\left(\langle \varphi, \chi \rangle\right) &= \sum_{s \in G} \varphi(s^{-1}) \text{Re}\left(\chi(s)\right) = \chi(1)\varphi(1) + \sum_{s \neq 1} \varphi(s^{-1})\chi(s) \\
&\geq \chi(1)\varphi(1) + \chi(1)\sum_{s \neq 1} \varphi(s^{-1}) = \chi(1)\sum_{s \in G} \varphi(s^{-1}) = 0
\end{aligned} \tag{151}$$

as $\varphi(s) \leq 0$ for $s \neq 1$.

If $\varphi \in R(G)$, the above conditions say that $\varphi \in R^+(G)$, which is a character by the previous homework.

S 9.2 If χ is an irreducible representation, it satisfies the conditions in the problem, so I'll prove the reverse direction.

Let's write χ by

$$\sum_{\chi_i:\text{irr. char}} n_i \chi_i, \tag{152}$$

where $n_i \in \mathbb{Z}$ for each i. Note that

$$\langle \chi, \chi \rangle = \sum_i n_i^2. \tag{153}$$

Therefore, $\langle \chi, \chi \rangle = 1$ means that only one i satisfies $n_i = \pm 1$ and 0 otherwise. Let the i be i_0. Since $\chi_{i_0}(1) \geq 1$, $\chi(1) \geq 0$ means that $n_{i_0} = 1$. Therefore, χ is an irreducible representation.

S 9.3

(a) In each proof, I'll concentrate on the symmetric power part since alternating power part has the same proof struecuture. To prove the results, it is enough to show that $\sigma_T(\chi)$ is well-defined for $|T| < 1/n$ where $n = \deg \chi$. Since

$$\left|\chi_\sigma^k(s)\right| \leq \prod_{i=1}^k (|\lambda_1| + \ldots + |\lambda_n|) = n^k \tag{154}$$

for $s \in G$ where λ_i are the eigenvalues of $\rho(s)$, for $T = a/n$ for $|a| < 1$

$$\left|\chi_\sigma^k T^k\right| \leq |\chi_\sigma T|^k < |a|^k, \tag{155}$$

and the power series converges absolutely in the domain. Now, I can use the uniqueness and calculus properties of power series. By the similar argument, I can repeat the statement for $\lambda_T(\chi)$.

For eigenvalues $\{\lambda_1, \ldots, \lambda_n\}$ of $\rho(s)$, we get

$$\chi_\sigma^k(s) = \sum_{1 \leq n_1 \leq n_2 \leq \cdots \leq n_k \leq n} \lambda_{n_1} \cdots \lambda_{n_k} \tag{156}$$

Also,

$$\frac{1}{\det(I - \rho(s)T)} = \prod_{i=1}^{n} \frac{1}{1 - \lambda_i T} = \prod_{i=1}^{n} \left(\sum_{j=0}^{\infty} (\lambda_i T)^j \right). \tag{157}$$

Now, let's show a lemma.

Lemma 8. *For $s \in G$, we get*

$$\sum_{k=0}^{\infty} \chi_\sigma^k(s) T^k = \frac{1}{\det(I - \rho(s)T)} \tag{158}$$

for $|T| < 1/(\deg \chi)$.

Proof. Note that (157) converges absolutely for $|T| < 1/n$, so I just need to check whether the coefficients of T^k coincide. To show this, I'll state a proposition.

Proposition 9. *For $\{c_i\}_{i=1}^{N} \subset \mathbb{C}^\times$ and an undeterminate T in the domain $|T| < 1$, it satisfies*

$$\prod_{i=1}^{N} \sum_{j=0}^{\infty} (c_i T)^j = \sum_{k=0}^{\infty} \sum_{1 \leq n_1 \leq n_2 \leq \cdots \leq n_k \leq N} c_{n_1} \cdots c_{n_k} T^k. \tag{159}$$

Proof. Since $c_i \in \mathbb{C}^\times$ and $|T| < 1$, the series in LHS converges absolutely, so it is well-defined and change of the order of summation does not change the result. Therefore, we again need to check whether the coefficients of T^k for both side coincide.

Now, let's change the view point of RHS. The RHS can be rewritten by

$$\sum_{k=0}^{\infty} \sum_{1 \leq n_1 \leq n_2 \leq \cdots \leq n_k \leq N} c_{n_1} \cdots c_{n_k} T^k = \sum_{k=0}^{\infty} T^k \sum_{\substack{\sum_{i=1}^{N} d_i = k \\ d_i \geq 0}} c_1^{d_1} \cdots c_N^{d_N}. \tag{160}$$

To check this, it is enough to show that any element $(d_1, \ldots, d_N)$ such that $\sum_{i=1}^{N} d_i = k$ bijectively correspond to $c_1^{d_1} \cdots c_N^{d_N}$ and the set of $c_{n_1} \cdots c_{n_k}$ with

$$\underbrace{c_1 \cdots c_1}_{d_1} \cdots \underbrace{c_N \cdots c_N}_{d_N}. \tag{161}$$

Finally, the coefficient of T^k in the LHS (159) is same as the RHS in (160), so it proves the result. $\qquad \square$

Applying above proposition with (156) and (158), we get

$$\frac{1}{\det(I - \rho(s)T)} = \prod_{i=1}^{N} \sum_{j=0}^{\infty} (\lambda_i T)^j$$

$$= \sum_{k=0}^{\infty} \sum_{1 \leq n_1 \leq n_2 \leq \cdots \leq n_k \leq N} \lambda_{n_1} \cdots \lambda_{n_k} T^k \tag{162}$$

$$= \sum_{k=0}^{\infty} \chi_\sigma^k(s) T^k.$$

for $|T| < 1/n$. $\qquad\qquad\square$

Let's reproduce the same argument for $\lambda_T(\chi)$. For $k > n$, we know that $\chi_\lambda^k = 0$ by the property of the symmetric power, so we can assume $k \leq n$. For eigenvalues of $\rho(s)$, we get

$$\lambda_T(\chi)(s) = \sum_{k=0}^{n} \chi_\lambda^k(s) T^k = \sum_{1 = n_1 < n_2 < \ldots < n_k = n} \lambda_{n_1} \lambda_{n_2} \cdots \lambda_{n_k} T^k$$

$$\det(1 + \rho(s)T) = \prod_{i=1}^{n} (1 + \lambda_i T). \tag{163}$$

We can easily check that the two have same coefficient for T^k by noticing that it is equivalent to choosing k distinct element from $\{\lambda_1, \ldots, \lambda_n\}$.

To proceed next step, I need some fact from linear algebra. Fortunately, we are dealing with diagonalizable matrices, so we can easily check the fact from the linear algebra.

Let's define

$$\frac{1}{1 - A} := \sum_{k=0}^{\infty} A^k \tag{164}$$

for a diagonalizable matrix A with eigenvalues λ_i with $|\lambda_i| < 1$. This is well-defined since writing $A = V\Lambda V^{-1}$ which is diagonalization,

$$\sum_{k=0}^{N} A^k = V \left(\sum_{k=0}^{N} \Lambda^k \right) V^{-1} \tag{165}$$

and the diagonal part have $\sum_{k=0}^{N} \lambda_i^k$, which converges absolutely as $N \to \infty$. By the similar mean, we define

$$-\ln(1 - A) := \sum_{k=1}^{\infty} \frac{A^k}{k}. \tag{166}$$

for the same restriction on A. Finally, we define

$$\exp A := \sum_{k=0}^{\infty} \frac{A^k}{k!} \tag{167}$$

with arbitrary restriction on A: to check the convergence, see "Matrix exponential" article in the Wikipedia. Note that if A are diagonalizable, then the three operations preserves the diagonalizability. For diagonalizable matrix A, we know that

$$\det\left(\exp(A)\right) = \exp\left(\operatorname{tr} A\right), \tag{168}$$

so replacing A by $-\ln(1 - \rho(s)T)$ for $|T| < 1/n$, we get

$$= \det\left(\exp(-\ln(1 - \rho(s)T))\right) = \exp\left(\operatorname{tr}(-\ln(1 - \rho(s)T))\right) \tag{169}$$

Let's calculate both sides. For LHS with diagnalization $\rho(s) = V\Lambda V^{-1}$,

$$\begin{aligned}
\det\left(\exp(-\ln(1 - \rho(s)T))\right) &= \det\left(\exp\left(V\left(\sum_{k=0}^{\infty}\left(\frac{\Lambda T}{k}\right)^k\right)V^{-1}\right)\right) \\
&= \det\left(V\exp\left(\sum_{k=0}^{\infty}\left(\frac{\Lambda T}{k}\right)^k\right)V^{-1}\right),
\end{aligned} \tag{170}$$

and the center term is

$$\begin{aligned}
\exp\left(\sum_{k=0}^{\infty}\left(\frac{\Lambda T}{k}\right)^k\right) &= \begin{pmatrix} \exp\left(\sum_k \frac{\lambda_1 T}{k}\right)^k & 0 & \dots & \vdots \\ 0 & \exp\left(\sum_k \frac{\lambda_2 T}{k}\right)^k & \dots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ \dots & \dots & 0 & \exp\left(\sum_k \frac{\lambda_n T}{k}\right)^k \end{pmatrix} \\
&= \begin{pmatrix} \exp\left(-\ln(1 - \lambda_1 T)\right) & 0 & \dots & \vdots \\ 0 & \exp\left(-\ln(1 - \lambda_2 T)\right) & \dots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ \dots & \dots & 0 & \exp\left(-\ln(1 - \lambda_n T)\right) \end{pmatrix} \\
&= \frac{1}{1 - \Lambda T}.
\end{aligned} \tag{171}$$

It shows that

$$\det\left(\exp(-\ln(1 - \rho(s)T))\right) = \det\left(\frac{1}{1 - \Lambda T}\right). \tag{172}$$

Furthermore, using (171), we get

$$\det\left(\exp(-\ln(1 - \rho(s)T))\right) = \frac{1}{\det(1 - \Lambda T)} = \frac{1}{\det(1 - \rho(s)T)}. \tag{173}$$

For the RHS of (169), we again get

$$\begin{aligned}
\exp\left(\operatorname{tr}(-\ln(1 - \rho(s)T))\right) &= \exp\left(\operatorname{tr}\left(\sum_{k=1}^{\infty}\frac{(\Lambda T)^k}{k}\right)\right) \\
&= \exp\left(\sum_{k=1}^{\infty}\operatorname{tr}\Lambda^k\frac{T^k}{k}\right) = \exp\left(\sum_{k=1}^{\infty}\operatorname{tr}\rho^k(s)\frac{T^k}{k}\right) \\
&= \exp\left(\sum_{k=1}^{\infty}\operatorname{tr}\rho(s^k)\frac{T^k}{k}\right) = \exp\left(\sum_{k=1}^{\infty}\Psi^k(\chi)(s)\frac{T^k}{k}\right).
\end{aligned} \tag{174}$$

For $\lambda_T(\chi)(s)$, we repeat the similar computation. Pluggin $A = \ln(1 + \rho(s)T)$ for (168), we get

$$\det\left(\exp(\ln(1 + \rho(s)T))\right) = \exp\left(\operatorname{tr}\ln(1 + \rho(s)T)\right). \tag{175}$$

The RHS is

$$\exp\left(\operatorname{tr}\ln(1 + \rho(s)T)\right) = \exp\left(\sum_{k=1}^{\infty}(-1)^{k-1}\Psi^k(\chi)T^k/k\right), \tag{176}$$

and the LHS is

$$\det\left(\exp(\ln(1 + \rho(s)T))\right) = \det(1 + \rho(s)T). \tag{177}$$

Finally, for $|T| < 1/n$, $\sigma_T(\chi)(s)$ is smooth and has well-defined series form derivative, so we get

$$(\ln \sigma_T(\chi)(s))' = \frac{(\sigma_T(\chi)(s))'}{\sigma_T(\chi)(s)}, \tag{178}$$

and we know that $\sigma_T(\chi)(s) \neq 0$ for all $|T| < 1$ since it has exponential form, and $\sum_{k=1}^{\infty}\Psi^k(\chi)T^k/k$ converges absolutely for $|T| < 1/n$ as $\left|\Psi^k(\chi)(s)\right| \leq n$. Therefore,

$$\left(\sum_{k=1}^{\infty}\Psi^k(\chi)T^k/k\right)'\left(\sum_{k=0}^{\infty}\chi_\sigma^k T^k\right) = \sum_{n=0}^{\infty}T^n\sum_{k=1}^{n+1}\Psi^k(\chi)\chi_\sigma^{n+1-k} = \sum_{n=1}^{\infty}n\chi_\sigma^n T^{n-1}. \tag{179}$$

It shows that

$$n\chi_\sigma^n = \sum_{k=1}^{n}\Psi^k(\chi)\chi_\sigma^{n-k}. \tag{180}$$

Repeating same calculation, we again get

$$n\chi_\lambda^n = \sum_{k=1}^{n}(-1)^{k-1}\Psi^k(\chi)\chi_\lambda^{n-k}. \tag{181}$$

(b) Since Ψ^k is $\mathbb{Z}$ linear map, it is enough to show that $\Psi^k(\chi) \in R(G)$ for an irreducible character χ on G. I'll show the result for $k \geq 0$, and extend it to $\mathbb{Z}$. Let's use induction on k. For $k = 1$, it is trivial, so assume it is true for $k < K$. For $k = K$, note that

$$\Psi^K(\chi) = K\chi_\sigma^K - \sum_{k=1}^{K-1}\Psi^k(\chi)\chi_\sigma^{K-k}. \tag{182}$$

We know that $R(G)$ is closed under addition and multiplication, and $\chi_\sigma^n \in R(G)$ for all $n \geq 1$. Therefore, we get $\Psi^K(\chi) \in R(G)$ as $\Psi^k(\chi) \in R(G)$ for $k < K$ by the induction hypothesis.

For $k = 0$, it is just $\Psi^0(\chi)(s) = \chi(s^0) = \chi(1)$, so it is $\chi(1)1_G$. For $k < 0$, choose sufficiently large $m > 0$ such that $k + mg > 0$, then

$$\Psi^{k+mg}(\chi)(s) = \chi(s^{k+mg}) = \chi(s^k) = \Psi^k(\chi)(s) \tag{183}$$

for all $s \in G$. Therefore, $\Psi^k(\chi) = \Psi^{k+mg}(\chi) \in R(G)$. It ends the proof.

(If the stability means $\Psi^k : R(G) \to R(G)$ is bijective for all k, it is false: $\Psi^g(\chi) = \chi(1)1_G$ for all irreducible representation χ on G.)

S 9.4

(a) I'll first show a proposition.

Proposition 10. *Let's define $\varphi : G \to G$ by $\varphi(s) = s^n$. If $(n, g) = 1$, then φ is a bijective map.*

Proof. Since $(n, g) = 1$, there exists $k \in \mathbb{N}$ such that $kn \equiv 1 \mod g$. If $g_1^n = g_2^n$, then $g_1 = g_1^{kn} = g_2^{kn} = g_2$, so φ is injective. Since the domain and codomain have same finite cardinality, φ is bijective. $\square$

Corollary 11. *Let c_1 be a conjugacy class in G. Then the φ maps c_1 to another conjugacy class bijectively, i.e. if I write $c_1' = \mathrm{Im}\,\varphi(c_1)$, then $\varphi|_{c_1} : c_1 \to c_1'$ is bijective.*

Proof. Let's consider $\varphi|_{c_i}$, then it is contained in some conjugacy class, in fact, it is surjective on the conjugacy class: if $s_1 \in c_i$, then for any $s \in G$, $\varphi(s s_1 s^{-1}) = s s_1^n s^{-1}$, so it is contained in some conjugacy class c_1' containing s_1^n and generated any element in the class. Since φ is injective, $\varphi|_{c_1}$ is bijective. $\square$

Corollary 12. *Let $\{c_1, \ldots, c_h\}$ be the set of conjugacy classes in G. Let's define*

$$\Phi : \{c_1, \ldots, c_h\} \to \{c_1, \ldots, c_h\} \tag{184}$$

by $\Phi(c_i) = \mathrm{Im}\,\varphi(c_i)$. Then, Φ is a bijective map.

Proof. From the above consideration, the map $\Phi : \{c_1, \ldots, c_h\} \to \{c_1, \ldots, c_h\}$ is well-defeind. Since φ is bijective, Φ is again surjective, so bijective. $\square$

Using the proposition, we get

$$\langle \Psi^m(\chi), \Psi^m(\chi) \rangle = \frac{1}{g} \sum_{s \in G} \chi(s^n) \chi(s^{-n}) = \frac{1}{g} \sum_{s \in G} \chi(s) \chi(s^{-1}) = \langle \chi, \chi \rangle = 1. \tag{185}$$

Also, $\Psi^m(\chi)(1) = \chi(1) > 0$. By the problem 9.2, we know that $\Psi^m \chi$ is an irreducible character of G.

(b) The center of the algebra $\mathbb{C}[G]$ is spanned by $e_c = \sum_{s \in c} s$ where c is a conjugacy class of G; in fact, it is a basis. Now, I'll prove a lemma.

Lemma 13. *For two conjugacy classes c_1, c_2 in G, we get*

$$\sum_{s \in c_1} \sum_{s' \in c_2} s^n (s')^n = \sum_{s \in c_1} \sum_{s' \in c_2} (ss')^n. \tag{186}$$

Proof. If G were abelian, then it is easy to see, so assume G is non-abelian. Let's use proposition 13 and algebra homomorphisms ω_i which sends $\sum_{s \in G} u(s)s \in \mathrm{Cent}.\ \mathbb{C}[G]$ to $\mathbb{C}$ by

$$\omega_i \left(\sum_{s \in G} u(s)s \right) = \frac{1}{n_i} \sum_{s \in G} u(s) \chi_i(s), \tag{187}$$

where χ_i is the irreducible character corresponding to ω_i and $n_i = \deg \chi_i$. (For detailed explanation, see Chapter 6.3, **S**.) Since $(\omega_i)_{i=1}^h$, where h is the number of conjugacy classes in G, defines an isomorphism of the center of $\mathbb{C}[G]$ onto the algebra $\mathbb{C}^h$, it is enough to show that

$$\omega_i\left(\sum_{s\in c_1}\sum_{s'\in c_2}s^n(s')^n\right) = \omega_i\left(\sum_{s\in c_1}\sum_{s'\in c_2}(ss')^n.\right) \tag{188}$$

for all i.

Now, let's use corollary 11. Let's set $c_1' = \operatorname{Im}\varphi(c_1)$ and $c_2' = \operatorname{Im}\varphi(c_2)$, then we get

$$\sum_{s\in c_1}s^n = \sum_{s\in c_1'}s$$
$$\sum_{s'\in c_2}(s')^n = \sum_{s'\in c_2'}s', \tag{189}$$

and it shows that both are in the center of $\mathbb{C}[G]$. Now, we get

$$\omega_i\left(\sum_{s\in c_1}\sum_{s'\in c_2}s^n(s')^n\right) = \omega_i\left(\left(\sum_{s\in c_1}s^n\right)\left(\sum_{s'\in c_2}(s')^n\right)\right)$$
$$= \omega_i\left(\sum_{s\in c_1}s^n\right)\omega_i\left(\sum_{s'\in c_2}(s')^n\right) \tag{190}$$
$$= \frac{1}{n_i^2}\sum_{s\in c_1}\Psi^n\chi_i(s)\sum_{s'\in c_2}\Psi^n\chi_i(s').$$

From (a), we know that $\Psi^n\chi_i = \chi_j$ for some j since it is irreducible, and $n_i = n_j$ since $\Psi^n\chi_i(1) = \chi_i(1)$. It shows that

$$\omega_i\left(\sum_{s\in c_1}\sum_{s'\in c_2}s^n(s')^n\right) = \frac{1}{n_i^2}\sum_{s\in c_1}\Psi^n\chi_i(s)\sum_{s'\in c_2}\Psi^n\chi_i(s')$$
$$= \frac{1}{n_j^2}\sum_{s\in c_1}\chi_j(s)\sum_{s'\in c_2}\chi_j(s')$$
$$= \omega_j\left(\sum_{s\in c_1}s\right)\omega_j\left(\sum_{s'\in c_2}s'\right) \tag{191}$$
$$= \omega_j\left(\sum_{s\in c_1}\sum_{s'\in c_2}ss'\right).$$

Also,

$$\omega_i\left(\sum_{s\in c_1}\sum_{s'\in c_2}(ss')^n.\right) = \frac{1}{n_i}\sum_{s\in c_1,s'\in c_2}\Psi^n\chi_i(ss')$$
$$= \frac{1}{n_j}\sum_{s\in c_1,s'\in c_2}\chi_j(ss') \tag{192}$$
$$= \omega_j\left(\sum_{s\in c_1,s'\in c_2}ss'\right).$$

Therefore, (188) holds and the lemma is true for $(n, g) = 1$. □

The lemma shows that ψ_n is algebra endomorphism on the center of $\mathbb{C}[G]$ as it shows

$$\psi_n(e_{c_1})\psi_n(e_{c_2}) = \psi_n(e_{c_1}e_{c_2}) \tag{193}$$

for any conjugacy classes c_1 and c_2 in G. By the corollary 12, we know that $\operatorname{Im}\psi_n$ maps the basis $\{e_c\}$ to the basis $\{e_c\}$ surjectively. Since the domain and codomain have same dimension, it shows that φ is an algebra automorphism on the center of $\mathbb{C}[G]$.

S 9.5 For the subgroup $H = 1$, there are only one irreducible character 1_H. The induced character is r_G since $\operatorname{Ind}_H^G 1_H(1) = 12$ and 0 elsewhere. It is $3\psi + \chi_0 + \chi_1 + \chi_2 = (\psi + \chi_0 + \chi_1 + \chi_2) + 2\psi$.

For the subgroup generated by $H = \langle(1\ 2)(3\ 4)\rangle$, there are two irreducible characters: the trivial one 1_H and non-trivial one φ mapping $(1\ 2)(3\ 4)$ to -1. The centralizer of $(1\ 2)(3\ 4)$ in $\mathfrak{A}_4$ is $\{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. Also, $\{(3\ 2\ 1), (1\ 2\ 4), (4\ 3\ 1), (2\ 3\ 4)\}$ maps it to $(1\ 3)(2\ 4)$. Therefore, the induced character of each one is

$$\operatorname{Ind}_H^G 1_H(s) = \frac{1}{2} \sum_{\substack{t \in \mathfrak{A}_4 \\ t^{-1}st \in H}} 1_H(t^{-1}st) \begin{cases} 6 & s = 1 \\ 2 & s = (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3) \\ 0 & o.w. \end{cases}$$

$$\operatorname{Ind}_H^G \varphi(s) = \frac{1}{2} \sum_{\substack{t \in \mathfrak{A}_4 \\ t^{-1}st \in H}} 1_H(t^{-1}st) \begin{cases} 6 & s = 1 \\ -2 & s = (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3) \\ 0 & o.w. \end{cases} \tag{194}$$

The first one is $\chi_0 + \chi_1 + \chi_2 + \psi$ and latter one is 2ψ. For the subgroups generated by $(1\ 3)(2\ 4)$ and $(1\ 4)(2\ 3)$, the same computation yields the same characteristic function. (Or it can be deduced from the fact that the groups is the conjugation of H by $t = (1\ 2\ 3)$ or t^2.) For precise computation, see exercise 9.6 (b).

Let $H = \langle(1\ 2\ 3)\rangle$. There are three irreducible characters: 1_H, $\varphi(t) = w = \exp\left(\frac{2\pi i}{3}\right)$, $\varphi'(t) = \exp\left(\frac{4\pi i}{3}\right)$. The centralizer of $(1\ 2\ 3)$ is only $\{1, (1\ 2\ 3), (1\ 3\ 2)\}$ in $\mathfrak{A}_4$. The induced characters are

$$\operatorname{Ind}_H^G 1_H(s) = \frac{1}{3} \sum_{\substack{t \in \mathfrak{A}_4 \\ t^{-1}st \in H}} 1_H(t^{-1}st) \begin{cases} 4 & s = 1 \\ 0 & s = (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3) \\ 1 & o.w. \end{cases}$$

$$\operatorname{Ind}_H^G \varphi(s) = \frac{1}{3} \sum_{\substack{t \in \mathfrak{A}_4 \\ t^{-1}st \in H}} 1_H(t^{-1}st) \begin{cases} 4 & s = 1 \\ 0 & s = (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3) \\ w & s = (1\ 2\ 3), (1\ 2\ 4), (1\ 4\ 3), (4\ 2\ 3) \\ w^2 & o.w. \end{cases} \tag{195}$$

$$\operatorname{Ind}_H^G \varphi'(s) = \frac{1}{3} \sum_{\substack{t \in \mathfrak{A}_4 \\ t^{-1}st \in H}} 1_H(t^{-1}st) \begin{cases} 4 & s = 1 \\ 0 & s = (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3) \\ w^2 & s = (1\ 2\ 3), (1\ 2\ 4), (1\ 4\ 3), (4\ 2\ 3) \\ w & o.w. \end{cases}$$

The first one is $\chi_0 + \psi$, the second one is $\chi_1 + \psi$, and the third one is $\chi_2 + \psi$. Any element in $\mathfrak{A}_4 \setminus \{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ can be made by conjugation of $(1\,2\,3)$ or $(1\,3\,2)$, so any cyclic subgroup generated by one element in the set have above induced character. It shows that image of $\oplus_{H\in X} R^+(H)$ under Ind is generated by the five characters.

Note that above characters all have even number at $s = 1$. Conversely, assume χ is a character of $\mathfrak{A}_4$ having $\chi(1) \equiv 0 \mod 2$. Since ψ, χ_i all have odd degree, χ is generated by

$$2\psi, 2\chi_1, 2\chi_2, 2\chi_3, \psi + \chi_0, \psi + \chi_1, \psi + \chi_2, \chi_0 + \chi_1, \chi_0 + \chi_2, \chi_1 + \chi_2. \tag{196}$$

Since all the characters are generated by the five characters, we know that χ is generated by the five character and is in the image.

According to the above computation, we know that any non-zero characters induced from $R^+(H)$ where H is a cyclic subgroup have non-zero ψ part, so χ_0, χ_1, and χ_2 can not be generated by linear combination with positive rational coefficients of characters induced from cyclic subgroups.

S 9.6

(a) For irreducible $\mathbb{C}[H']$ module V, by the universal property of the induced representation, there exists a unique $\mathbb{C}[G]$ module homomorphism Ψ such that the diagram commutes; i, i', i'', and $i^{(3)}$ are the inclusion map.

$$
\begin{array}{ccc}
V & \xrightarrow{\quad i \quad} & \mathbb{C}[G] \otimes_{\mathbb{C}[H']} V \\
{\scriptstyle i'}\downarrow & {\scriptstyle i^{(3)}} & \downarrow{\scriptstyle \Psi} \\
\mathrm{Res}_{H'}\,\mathbb{C}[G] \otimes_{\mathbb{C}[H]} (\mathbb{C}[H] \otimes_{\mathbb{C}[H']} V) & \xrightarrow{\ i'' \ } & \mathbb{C}[G] \otimes_{\mathbb{C}[H]} (\mathbb{C}[H] \otimes_{\mathbb{C}[H']} V)
\end{array}
$$

Ψ is surjective map since for any $g \otimes (h \otimes v) \in \mathbb{C}[G] \otimes_{\mathbb{C}[H]} (\mathbb{C}[H] \otimes_{\mathbb{C}[H']} V)$, $\Psi(gh \otimes v) = gh \cdot \Psi(1 \otimes v) = gh \cdot (1 \otimes (1 \otimes v)) = g \otimes (h \otimes v)$. By the dimensional analysis, the Ψ is an bijective map, so it is $\mathbb{C}[G]$ module isomorphism. It shows that

$$\mathrm{Ind}_H^G \mathrm{Ind}_{H'}^H \chi' = \mathrm{Ind}_H^G \chi, \tag{197}$$

and $\mathrm{Ind}_{H'}^H \chi' - \chi \in N$.

(b) For $s, s' \in G$,

$$
\begin{aligned}
\mathrm{Ind}_{{}^sH}^G {}^s\chi(s') &= \frac{1}{|{}^sH|} \sum_{\substack{t\in G \\ t^{-1}s't\in{}^sH}} {}^s\chi(t^{-1}s't) = \frac{1}{|H|} \sum_{\substack{t\in G \\ t^{-1}s't\in sHs^{-1}}} \chi(s^{-1}t^{-1}s'ts) \\
&= \frac{1}{|H|} \sum_{\substack{t\in G \\ (ts)^{-1}s'(ts)\in H}} \chi((ts)^{-1}s'(ts)) = \frac{1}{|H|} \sum_{\substack{t\in G \\ t^{-1}s't\in H}} \chi(t^{-1}s't) \\
&= \mathrm{Ind}_H^G \chi(s'),
\end{aligned} \tag{198}
$$

we get $\chi - {}^s\chi \in N$.

(c) Let S is the collection of functions of type (a) and (b) and consider the submodule of $\oplus_{H\in X}\mathbb{Q}\otimes R(H)$ spanned by S. Let's rewrite the submodule by S. What I want to do is to show that $S = N$. To use theory of class function, let's extend the scalar to $\mathbb{C}$; if $\mathbb{C}\otimes S = \mathbb{C}\otimes N$ in $\oplus_{H\in X}\mathbb{C}\otimes R(H)$, then for a basis $\{s_\alpha\}$ of S, $1\otimes s_\alpha$ forms a basis of $\mathbb{C}\otimes S$ and so $\mathbb{C}\otimes N$. It shows that s_α is a basis of N, and $S = N$ in $\oplus_{H\in X}\mathbb{Q}\otimes R(H)$. By (a) and (b), we know that $S \subset N$.

I'll show what the hint says: let A be the collection of $(f_H) \in \oplus_{H\in X}\mathbb{C}\otimes R(H)$ such that if $H' \subset H$, then $f_{H'} = \mathrm{Res}_{H'} f_H$ and $f^s{}_H(sts^{-1}) = f_H(t)$ for any $s \in G$. It is well-defined subspace in $\oplus_{H\in X}\mathbb{C}\otimes R(H)$. Also, it is not empty set since 0 is in the set.

To use Hilbert space's property, I'll first check that $\mathbb{C}\otimes R(H)$ is a Hilbert space, but we know that $(f,g) = \sum_{s\in H} f(s)\overline{g(s)}$ is a inner product with $(f,f) \geq 0$ and $(f,f) = 0$ if and only if $f = 0$ using the fact that the irreducible characters (χ_i) forms a basis of the class function and $(\chi_i,\chi_j) = \delta_{ij}$. Since product of Hilbert space is again Hilbert space with the sum of inner product,-which will be clear writing the proof- I can take orthogonal decomposition of $\oplus_{H\in X}\mathbb{C}\otimes R(H)$ about A by $A^\perp$; note that the orthogonal spaces are unique. By the same reason, we can consider $N^\perp$.

From now on, I'll use another bilinear form $\langle\cdot,\cdot\rangle$. The only difference from $(\cdot,\cdot)$ is that the second one take complex conjugate of the coefficient of characters in right side in the sum. To avoid it, I'll take the basis of each $\mathbb{Q}\otimes R(H)$ by the irreducible characters of H and only use them in the equation since any operation such as Ind_H^G, Res_H, and the operations ${}^sH$ are $\mathbb{C}$-linear and maps a $\mathbb{Z}$ linear combination of characters to a $\mathbb{Z}$ linear combination of characters. In other words, we can safely treat only basis element in the computation identifying $\langle\cdot,\cdot\rangle$ and $(\cdot,\cdot)$.

Now, assume $S \not\supset N$, then there exists non-zero $n = (n_H) \in N$ such that $n \perp S$. It means that for any $\mathrm{Ind}_{H'}^H \chi_{H'} = \chi_H$ where $H' \subset H$ and $\chi_{H'}$ and χ_H are class functions, for $\chi \in \oplus_{H\in X}\mathbb{C}\otimes R(H)$ with 0 except H' and H having $-\chi_{H'}$ and χ_H,

$$\langle n,\chi\rangle = \langle n_H,\chi_H\rangle - \langle n_{H'},\chi_{H'}\rangle = \langle\mathrm{Res}_{H'} n_H - n_{H'},\chi_{H'}\rangle = 0. \qquad (199)$$

Also, for any $s \in G$ and $\chi = 0$ except χ_H at H, and $-\chi^s{}_H$ at ${}^sH$,

$$\begin{aligned}
\langle n,\chi\rangle &= \langle n_H,\chi_H\rangle - \langle n^s{}_H,\chi^s{}_H\rangle \\
&= \langle n_H,\chi_H\rangle - \frac{1}{|H|}\sum_{t\in H} n^s{}_H(sts^{-1})\chi^s{}_H(st^{-1}s^{-1}) \\
&= \langle n_H,\chi_H\rangle - \frac{1}{|H|}\sum_{t\in H} n^s{}_H(sts^{-1})\chi_H(t^{-1}).
\end{aligned} \qquad (200)$$

If we define $g(t) = n^s{}_H(sts^{-1})$ for $t \in H$, which is again class function in H, we get

$$\langle n,\chi\rangle = \langle n_H - g,\chi_H\rangle = 0 \qquad (201)$$

If I choose irreducible representations at each RHS, then it means $\mathrm{Res}_{H'} n_H - n_{H'} = 0$ and $n_H - g = 0$. Checking the definition of A, the second one implies that $n^s{}_H(sts^{-1}) = n_H(t)$, which implies $n \in A$. Finally, if I show that $N^\perp = A$, then it means $n \in N \cap N^\perp = 0$, which ends the proof. Therefore, it is enough to show that $A = N^\perp$.

Let $A' = \{(\operatorname{Res}_H \varphi) \in \oplus_{H \in X} C(H) : \varphi \in C(G)\}$. I'll first show that $A' = A$. $A' \subset A$ is easy to see since $\operatorname{Res}_{H'} \varphi = \operatorname{Res}_{H'} \operatorname{Res}_H \varphi$ for $H' \subset H$, and $\operatorname{Res}_{sH} \varphi = \operatorname{Res}_H \varphi$ by the definition of class function. Conversely, assume $(f_H) \in A$. Construct $\varphi \in C(G)$ as following: for any $t \in G$, there exists $t \in H \in X$ since $\cup_{H \in X} H = G$. Set $\varphi(t) = f_H(t)$. This is well-defined: assume there exists another $H' \in X$ with $t \in H'$, then $t \in H' \cap H$. Since $\operatorname{Res}_{H' \cap H} f_H(t) = f_{H' \cap H}(t) = \operatorname{Res}_{H' \cap H} f_{H'}(t)$, $f_H(t) = f_{H'}(t)$. (I interpreted that "passage to subgroups" means that $H, H' \in X$ implies $H \cap H' \in X$.)
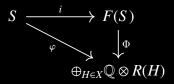
Since A is a subspace, so we can decompose $\oplus_{H \in X} C(H) = A \oplus A^\perp$. For fixed $\varphi \in C(G)$ and $n \in N$, we get

$$\sum_{H \in X} \langle n_H, \operatorname{Res}_H \varphi \rangle = \sum_{H \in X} \langle \operatorname{Ind}_H^G n_H, \varphi \rangle = 0. \tag{202}$$

It shows that $A \le N^\perp$.

Conversely, fix $(f_H) \in N^\perp$, then $(f_H) \in S^\perp$, and the above calculations (199), (200), and (201) show that $(f_H) \in A$. Therefore, $A = N^\perp$. It ends the proof.

S 9.7 Let $S = \{(H, \chi) : H \in X, \chi \in \mathbb{Q} \otimes R(H)\}$. Consier the free $\mathbb{Q}$-module $F(S)$, and i be the inclusion map from S to $F(S)$. A function $\varphi : S \to \oplus_{H \in X} \mathbb{Q} \otimes R(H)$ be a map of set defined as follows: $\varphi((H, \chi)) = \chi_H$. By the universal property of free module, there exists a well-defined $\mathbb{Q}$-module homomorphism Φ satisfying

$$S \xrightarrow{\quad i \quad} F(S)$$
$$\varphi \searrow \qquad \downarrow \Phi$$
$$\oplus_{H \in X} \mathbb{Q} \otimes R(H)$$

Let's check what is the kernel of Φ. It is clear that the relation (i) should be contained in the ker Φ. Taking quotient using relation (i), as $F(S)$ is $\mathbb{Q}$ vector space, the quotient is again $\mathbb{Q}$ vector space. Furthermore, it has dimension at most $\sum_{H \in X} \mathbb{Q} \otimes R(H)$: for fixed $H \in X$ and irreducible characters χ_i, (H, χ_i) spans $\{(H, \chi) : \chi \in \mathbb{Q} \otimes R(H)\}$ using the linear relation. However, we know that Φ is surjective map, which means that the dimension is same and Φ induces the $\mathbb{Q}$ module isomorphism between two module. Using ex. 9.6, finally, we get the relation (i), (ii), and (iii) for $F(S)$ makes it isomorphic to $\mathbb{Q} \otimes R(G)$ since the relation (ii) and (iii) for $\otimes_{H \in X} \mathbb{Q} \otimes R(H)$ makes it isomorphic to $\mathbb{Q} \otimes R(G)$.

S 9.8 I'll check the conditions in exercise 9.1. λ_A is real-valued function on A, and it is in $R(A)$ by proposition 28. Also, $\langle \varphi(a) r_A - \theta_A, 1_A \rangle = \frac{1}{a}(\varphi(a)a - \varphi(a)a) = 0$, so it is orthogonal to 1_A. Finally, $r_A(s) = 0$ for $s \neq 1$, so $\lambda_A(s) \le 0$ for $s \neq 1$. Therefore, λ_A is a character of A which is orthogonal to unit character 1_A. Using proposition 27,

$$\sum_{A \subset G} \operatorname{Ind}_A^G(\lambda_A) = \sum_{A \subset G} \operatorname{Ind}_A^G(\varphi(a) r_A - \theta_A) = \sum_{A \subset G} \varphi(a) \operatorname{Ind}_A^G(r_A) - g \tag{203}$$

Since 1 is itself a conjugacy class, $\operatorname{Ind}_A^G(r_A)(1) = \frac{1}{a} g a = g$ and 0 if $s \neq 1$. Finally, $\sum_{A \subset G} \varphi(a) = g$ since any element in G uniquely corresponds to a generator of a cyclic group in G. Therefore, we get

$$\sum_{A \subset G} \operatorname{Ind}_A^G(\lambda_A) = g(r_G - 1). \tag{204}$$

7 Chapter 10

S 10.1 For any $h = x^k p \in C \cdot P$, where $k \in \mathbb{Z}$, $hxh^{-1} = x^k p x p^{-1} x^{-k} = x$ since $xp = px$ in H having inner direct product structure. Therefore, $H \subset Z(x)$ and P should be contained in a Sylow p-subgroup of $Z(x)$ by the Sylow theorem. Choosing Sylow p-subgroup of $Z(x)$ containing H, we prove the statement.

S 10.2 If $|x| = p^k$ for $k \in \mathbb{Z}_{\geq 0}$, $(1 - x)^{p^k} = 1 - x^{p^k} = 0$, so $(1 - x)$ is nilpontent; cf. Frobenius endomorphism. Conversely, assume $1 - x$ is nilpotent, then there exists large enough $k \geq 1$ such that $(1 - x)^{p^k} = 0$. It means that $x^{p^k} = 1$, and $|x| \mid p^k$, which implies x is p-element. If x is p'-element, then $x^N = 1$ for $(N, p) = 1$. The minimum polynomial should divide $q(x) = x^N - 1$, which is separable as $(q'(x), q(x)) = (Nx^{N-1}, x^N - 1) = (Nx^{N-1}, -1) = 1$. It shows that the minimal polynomial is separable and x is diagonalizable in a finite extension of k. Conversely, assume x is diagonalizable in some finite extension of k having order p^k. By little Fermat's theorem, any non-zero element in the field have order dividing $p^k - 1$, which is coprime to p. Therefore, writing

$$x = V \Lambda V^{-1}, \tag{205}$$

where $V \in GL_n(k)$ and Λ is a diagonal matrix having eigenvalues in the diagonal part, we get the order of Λ coprime to p. Therefore, x have order coprime to p, and it is an p'-element.

10.3

Lemma 14. *Each class function on G with gA values is an A-linear combination of characters induced from characters of cyclic subgroups of G.*

Proof. Let f be such a function, and write it in the form $g\chi$, where χ is a class function with values in A. If C is a cyclic subgroup of G, let θ_C be the element of $R(C)$ defined in 9.4. We have

$$g = \sum_C \operatorname{Ind}_C^G(\theta_C), \tag{206}$$

whence

$$f = g\chi = \sum_C \operatorname{Ind}_C^G(\theta_C)\chi = \sum_C \operatorname{Ind}_C^G(\theta_C \operatorname{Res}_C^G \chi). \tag{207}$$

It remains to show that $\theta_C \operatorname{Res}_C \chi$ belongs to $A \otimes R(C)$ for each C. But the values of $\chi_C = \theta_C \cdot \operatorname{Res}_C \chi$ are values in A with multiple of the order of C, so if ψ is a character of C, we have $\langle \chi_C, \psi \rangle \in A$, which shows that χ_C is an A-linear combination of characters of C, whence $\chi_C \in A \otimes R(C)$. $\square$

10.4

I'll write a non-zero prime ideal in A by M since it is in fact a maximal ideal; note that krull dimension of A is 1, and it is integral domain. Choose $x \in G$ and take decomposition $x = x_r x_u$ where x_r is the p'-element and x_u is p-element. Set $H = \langle x_r \rangle \times \langle x_u \rangle$, then it is an elementary subgroup of G. Since H is an abelian group, its characters are all degree 1. For $H_1 = \langle x_r \rangle$ and $H_2 = \langle x_u \rangle$, choose degree 1 irreducible characters on each group and write χ_i and η_j. Extend both characters on G by setting $\chi_i(x_u) = \eta_j(x_r) = 1$; it is well-defined since each are degree 1 and

H is abelian. Finally, $\chi_i \eta_j$ spans all the irreducible characters of H, cf. chapter 3.2. Now, choose arbitrary $\xi \in A \otimes R(G)$, then we can write

$$\text{Res}_H \xi = \sum_{i,j} a_{ij} \chi_i \eta_j. \tag{208}$$

Also, choose large enough n such that $x_u^{p^n} = 1$, then

$$\xi(x)^q = (\text{Res}_H \xi(x))^q = \left(\sum_{i,j} a_{ij} \chi_i(x_r) \eta_j(x_u) \right)^{p_n} \equiv \sum_{i,j} a_{ij}^{p_n} \chi_i(x_r^{p_n}) \eta_j(1)$$

$$\equiv \sum_{i,j} a_{ij}^{p_n} \chi_i(x_r^{p_n}) \equiv \xi(x_r)^q \mod M. \tag{209}$$

It shows that $(\xi(x) - \xi(x_r))^q \in M$, so $\xi(x) \equiv \xi(x_r) \mod M$.

S 10.5

(a) From the assumption, there exists $r_{i,j} \in \mathbb{R}_+$ and degree 1 representations $(A_j, \chi_{i,j})$ where $A_j \leq G$ such that

$$\chi = \sum_j \sum_i r_{i,j} \text{Ind}_{A_j}^G \chi_{i,j}. \tag{210}$$

(I used i to express distinct irreducible characters in same A_j.) As χ is an irreducible character, we get

$$1_G = \langle \chi, \chi \rangle = \sum_j \sum_i r_{i,j} \langle \text{Ind}_{A_j}^G \chi_{i,j}, \chi \rangle, \tag{211}$$

and for the other irreducible representations χ',

$$0 = \langle \chi, \chi' \rangle = \sum_j \sum_i r_{i,j} \langle \text{Ind}_{A_j}^G \chi_{i,j}, \chi' \rangle. \tag{212}$$

Since $r_{i,j} > 0$ by deleting the terms with $r_{i,j} = 0$ and $\langle \text{Ind}_{A_j}^G \chi_{i,j}, \chi' \rangle \in \mathbb{Z}_{\geq 0}$ as both are characters, we get $\langle \text{Ind}_{A_j}^G \chi_{i,j}, \chi' \rangle = 0$ for all irreducible representations of G except χ. Choose one i, j and denote it i_0, j_0. Since the irreducible representations forms an orthonomal basis of class function, and $\text{Ind}_{A_{j_0}}^G \chi_{i_0,j_0} \in R^+(G)$, we get $\text{Ind}_{A_{j_0}}^G \chi_{i_0,j_0} = n\chi$ for some $n \in \mathbb{N}$. As a result, we conclude that $n\chi$ is a monomial.

(b) Before start, note that $\mathfrak{A}_5$ has elements

    (a) identity element;

    (b) 15 elements of type like (1 2)(3 4);

    (c) 20 elements of type like (1 2 3);

    (d) 24 elements of type like (1 2 3 4 5).

Let $G = \mathfrak{A}_5$. The permutation representation of $\mathfrak{A}_5$ on $\{e_i\}_{i=1}^5$ G action defined by by $\sigma \cdot e_i = e_{\sigma(i)}$ have character η. Note that the permutation representation have degree 1

subrepresentation for the basis $\sum_{i=1}^{5} e_i$ since any element in $\mathfrak{A}_5$ fix it, so trivial representation. Therefore, $\eta - 1_G$ is again an character of $\mathfrak{A}_5$, and

$$\langle \eta - 1_G, \eta - 1_G \rangle = \frac{1}{60} (4 * 4 + 0 * 15 + 1 * 20 + 1 * 24) = 1. \tag{213}$$

It shows that $\eta - 1_G$ is irreducible having degree 4. Set $\chi = \eta - 1_G$.

Now, assume there exists $m \geq 1$ such that $m\chi = \operatorname{Ind}_H^G \chi_H$ for some subgroup H such that the degree of χ_H is 1. Since it has degree $4m$, $[G : H] = 4m$, and $|H| = 15/m$; so the possible m is $1, 3, 5, 15$. Also,

$$\langle \operatorname{Res}_H \chi, \chi_H \rangle = \langle \chi, \operatorname{Ind}_H^G \chi_H \rangle = m. \tag{214}$$

As the degree of $\operatorname{Res}_H \chi$ is 4 and χ_H is irreducible, $m \leq 4$, so the possible m is 1 or 3. If m were 3, then $|H| = 5$ and it should be a cyclic group having element like (1 2 3 4 5) as the other element (except identity) have order coprime to 5. However, this is impossible: by the definition,

$$\operatorname{Ind}_H^G \chi_H((1\ 2\ 3)) = \frac{1}{5} \sum_{\substack{t \in G \\ t(1\ 2\ 3)t^{-1} \in H}} \chi_H(t(1\ 2\ 3)t^{-1}), \tag{215}$$

but the conjugacy class of (1 2 3) does not have intersection with H, so it is zero. However, $(\eta - 1_G)(1\ 2\ 3) = 2 - 1 = 1$.

The remainder is to show that $\mathfrak{A}_5$ does not have order 15 group. (To do this, I refered "https://math.stackexchange.com/questions/135654/why-a-5-has-no-subgroup-of-order-15") By the application of Sylow's theorem, cf. *Abstract Algebra*, Dummit and Foote, Chapter 4.5 p. 143, we know that order 15 group is cyclic group, but we know that $\mathfrak{A}_5$ does not have order 15 element. Since $m\chi$ can not be a monomial, it shows that χ cannot be a linear combination with positive real coefficients of monomial characters.

S 10.6

(a) In the previous homework, I showed that for any $E \leq H \leq G$, and $\chi \in R(E)$, we get $\operatorname{Ind}_E^G \chi = \operatorname{Ind}_H^G \operatorname{Ind}_E^H \chi$. Therefore, for $\operatorname{Ind}_E^H(\alpha - 1_E)$ having same notation as problem with $E \leq H$, we get

$$\operatorname{Ind}_H^G \operatorname{Ind}_E^H(\alpha - 1_E) = \operatorname{Ind}_E^G(\alpha - 1_E). \tag{216}$$

Also, note that E is again an elementary subgroup of G since writing $E \simeq \langle x \rangle \times P$ with p-group $P \leq Z_H(x)$, which is center in H, $P \leq Z_G(x)$ and again p-group in G.

(b) Let $\rho = \operatorname{Ind}_H^G(1_H)$. Set $\{\sigma_i\}$ be the representatives of G/H with $\sigma_1 = 1$. Since H is normal in G and $1_H(h) = 1$ for all $h \in H$, considering $\mathbb{C}[G]$ action on $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} \mathbb{C}$, for $g = \sigma_i h$,

$$g \cdot (\sigma \otimes c) = \sigma_j h \sigma \otimes c = \sigma_j \sigma \otimes (h' \cdot c) = \sigma_j \sigma \otimes c, \tag{217}$$

where $h\sigma = \sigma h'$. It shows that $\rho(h) = \operatorname{id}$ for $h \in H$, and the group homomorphism $\rho : G \to \operatorname{Ind}_H^G(\mathbb{C})$ induces a homomorphism $\tilde{\rho} : G/H \to \operatorname{Ind}_H^G(\mathbb{C})$ which factor through the canonical projection $\pi : G \to G/H$. Computing the character of $\tilde{\rho}$, we get $\tilde{\rho}(1) = (G : H)$ and zero elsewhere. It means that $\tilde{\rho}$ is isomorphic to the regular representation of G/H. Since G/H

is abelian, we know that the character $\tilde{\chi}$ of $\tilde{\rho}$ is the sum of degree 1 characters of G/H; let's denote the degree 1 characters $\tilde{\chi}_i$, then we can write

$$\tilde{\rho} = \sum_{i=1}^{(G:H)} \tilde{\chi}_i \tag{218}$$

Finally, set functions χ_i by $\chi_i = \tilde{\chi}_i \circ \pi$. These are character functions: for $g_1, g_2 \in G$,

$$\chi_i(g_1 g_2) = \tilde{\chi}_i(\pi(g_1 g_2)) = \tilde{\chi}_i(\pi(g_1)\pi(g_2)) = \tilde{\chi}_i(\pi(g_1))\tilde{\chi}_i(\pi(g_2)) = \chi_i(g_1)\chi_i(g_2), \tag{219}$$

and we can identify characters and representations since χ_i have codomain $\mathbb{C}^\times$. Note that χ_i all have degree 1, and $\chi_1 = 1_G$. Finally, we get

$$\mathrm{Ind}_H^G 1_H = \sum_{i=1}^{(G:H)} \chi_i, \tag{220}$$

Now, let's constructively show that $\mathrm{Ind}_H^G 1_H \in R'(G)$. First, using Brauer's theorem, we choose irreducible characters η_E^i and n_E^i for elementary subgroups E satisfying

$$1_G = \sum_E \sum_i n_E^i \, \mathrm{Ind}_E^G \eta_E^i. \tag{221}$$

Note that I used sup-script i to distinguish distinct irreducible characters in the same E. To go to next step, I need a lemma.

Lemma 15. *Any subgroup of p-elementary group is p-elementary group. More precisely, for $G \simeq C \times P$ where $C = \langle x \rangle$ is a cyclic subgroup having order prime to p and P a p-group of $Z(x)$, any subgroup of G is written as $H \simeq A \times B$ where $A \leq C$ and $B \leq P$.*

Proof. Let $G = \langle x \rangle \cdot P$ where $x \in G$ having order prime to p and P being a p-group in $Z(x)$. For a subgroup $H \leq G$, choose $y = (\alpha, \beta) \in H$ identifying $\langle x \rangle \cdot P \simeq \langle x \rangle \times P$. Since $(|\alpha|, |\beta|) = 1$, there exists n_1, n_2 in $\mathbb{Z}$ such that $n_1 |\alpha| + n_2 |\beta| = 1$. It shows that

$$\begin{aligned} y^{n_1 |\alpha|} &= (1, \beta^{1 - n_2 |\beta|}) = (1, \beta) \\ y^{n_2 |\beta|} &= (\alpha^{1 - n_1 |\alpha|}, 1) = (\alpha, 1), \end{aligned} \tag{222}$$

so $(\alpha, 1), (1, \beta) \in H$. Denote each α, β of y by α_y, β_y. Set A (resp. B) be the subgroup of $\langle x \rangle$ (resp. P) generated by α_y. (resp. β_y) Note that A is cyclic group since any subgroup of cyclic group is again cyclic group, and B is a p-subgroup of $Z(a)$ by the similar reason. I claim that $H \simeq A \times B$ with the same identification as G, then H is p-elementary subgroup of G.

By the construction of A, B, it is enough to show that $H \supset A \times B$, but any generator of $A \times 1$ and $1 \times B$ is in H, so $H \supset A \times B$. $\qquad \square$

Since E are super-solvable groups, η_E^i are induced by a representation of degree 1 of a subgroup of E, which is again elementary subgroup by the lemma. Abusing notation by setting η_E^i degree 1 character, we again write (221). From the basic property of induced representation, we know that

$$\mathrm{Ind}_E^G(\eta_E^i \, \mathrm{Res}_E(\chi_j - 1_G)) = (\mathrm{Ind}_E^G \eta_E^i)(\chi_j - 1_G), \tag{223}$$

so

$$\sum_{j=2}^{(G:H)} \sum_E \sum_i n_E^i \operatorname{Ind}_E^G(\eta_E^i \operatorname{Res}_E(\chi_j - 1_G)) = \sum_{j=2}^{(G:H)} \sum_E \sum_i n_E^i \operatorname{Ind}_E^G(\eta_E^i)(\chi_j - 1_G)$$

$$= \sum_{j=2}^{(G:H)} ((\chi_j - 1_G)1_G) \tag{224}$$

$$= \sum_{j=2}^{(G:H)} (\chi_j - 1_G).$$

Therefore,

$$\operatorname{Ind}_H^G 1_H = (G : H)1_G + \sum_{j=2}^{(G:H)} (\chi_j - 1_G)$$

$$= (G : H)1_G + \sum_{j=2}^{(G:H)} \sum_E \sum_i n_E^i \operatorname{Ind}_E^G(\eta_E^i \operatorname{Res}_E(\chi_j - 1_G))$$

$$= (G : H)1_G + \sum_{j=2}^{(G:H)} \sum_E \sum_i n_E^i \left(\operatorname{Ind}_E^G(\eta_E^i \operatorname{Res}_E \chi_j) - \operatorname{Ind}_E^G(\eta_E^i) \right) \tag{225}$$

$$= (G : H)1_G + \sum_{j=2}^{(G:H)} \sum_E \sum_i n_E^i \left(\operatorname{Ind}_E^G(\eta_E^i \operatorname{Res}_E \chi_j - 1_E) - \operatorname{Ind}_E^G(\eta_E^i - 1_E) \right).$$

Since multiplication of two degree 1 characters is again a degree 1 character, we get the result.

(c) Let's write $G \simeq C \times P$ where $C = \langle x \rangle$ is a cyclic subgroup having order prime to p and P a p-group of $Z(x)$. I'll first show a general lemma.

Lemma 16. *If G is nilpotent and $H < G$, then $H < N_G(H)$.*

Proof. Let's use the definition of nilpotent group given in the textbook. Given a sequence

$$\{1\} = G_0 \subsetneq G_1 \subsetneq \cdots G_{n-1} \subsetneq G_n = G \tag{226}$$

of subgroups of G satisfying $G_{i-1} \trianglelefteq G_i$ and $G_i/G_{i-1} \subset Z(G/G_{i-1})$, take quotient of G_1 in the sequence and get

$$\{1\} = G_1/G_1 \subsetneq G_2/G_1 \subsetneq \cdots G_{n-1}/G_1 \subsetneq G_n/G_1 = G/G_1. \tag{227}$$

I need to show that this is well-defined. First, G_1 is normal to $G_{i\geq 2}$ since $G_1/G_0 = G_1 \leq Z(G)$. Also, by the fourth isomorphism theorem, the normal property does not change. Finally, for $\varphi : G/G_1 \to G/G_{i-1}$ mapping $gG_1 \mapsto gG_{i-1}$, we get $\ker \varphi = G_{i-1}/G_1$ by the third isomorphism theorem for $i > 2$, and we know that $\varphi(G_i/G_1) = G_i/G_{i-1}$ with the same kernel by the same reason. Let $\bar{\varphi}$ be the induced isomorphism by taking quotient of G_{i-1}/G_1.

It shows that $G_i/G_{i-1} \leq Z(G/G_{i-1})$ implies $(G_i/G_1)/(G_{i-1}/G_1) \leq Z((G/G_1)/(G_{i-1}/G_1))$: for any $\bar{a} \in (G_i/G_1)/(G_{i-1}/G_1)$ and $\bar{b} \in (G/G_1)/(G_{i-1}/G_1)$ with $\bar{\varphi}(\bar{a}) = a$ and $\bar{\varphi}(\bar{b}) = b$,

$$\bar{\varphi}(\bar{a}\bar{b}) = \bar{\varphi}(\bar{a})\bar{\varphi}(\bar{b}) = ab = ba = \bar{\varphi}(\bar{b}\bar{a}), \tag{228}$$

so $\bar{a}\bar{b} = \bar{b}\bar{a}$ for all $\bar{b}$. It shows that G/G_1 is nilpotent.

Now, let's take induction on $|G|$ for the main result. If $G = 1$, it is trivial, so assume the statement is true for $|G| < n$ for some n. For $|G| = n$, take an proper subgroup H of G. Note that $Z(G)$ is non-trivial; unless, it is not nilpotent. If $G_1 \not\leq H$, then $N_G(H) \supset \langle H, G_1 \rangle$, which ends the proof, so we can assume $G_1 \leq H$. Consider $\bar{G} = G/G_1$, which is again nilpotent having smaller order, so $\bar{H} < N_{\bar{G}}(\bar{H})$. Again, by taking lattice isomorphism theorem, we know that the preimage of $N_{\bar{G}}(\bar{H})$ is $N_G(H)$: more precisely, for the canonical projection $\pi : G \to G/G_1 = \bar{G}$ and $g \in \pi^{-1}\left(N_{\bar{G}}(\bar{H})\right)$ with $h \in H$,

$$\pi(ghg^{-1}) = \bar{g}\bar{h}\bar{g}^{-1} \in \bar{H}, \tag{229}$$

so $ghg^{-1} \in \pi^{-1}(\bar{H}) = H$. Conversely, if $g \in N_G(H)$, then by the same reason, $\pi(ghg^{-1}) \in \bar{H}$, so $g \in \pi^{-1}\left(N_{\bar{G}}(\bar{H})\right)$. It shows that $H < N_G(H)$ and ends the proof. $\square$

If H is maximal subgroup of G, then $N_G(H) = G$ by the lemma, so H is normal in G. Also, using the lemma 1, let's write $H \simeq A \times B$ where $A \leq C$ and $B \leq P$. If $B \neq P$, then $A < C$ and $[C : A]$ should be prime applying the classification of finitely generated abelian group with the lattice theorem to C/A since $G/H \simeq C/A \times B/P$. If $C = A$, then $[P : B]$ should be prime since P/B is again a p group and any p group P have subgroup having order dividing $|P|$. If $C < A$ and $B < P$, then $C \times P$ is the bigger subgroup of G, so it is contradiction. As a result, $[G : H]$ is prime.

Using theorem 16 since G is super-solvable group, we can write each irreducible representation χ of G by

$$\chi = \sum_E \sum_i n_E^i \operatorname{Ind}_E^G \eta_E^i, \tag{230}$$

where E are subgroups of G, $n_E^i \in \mathbb{Z}$, and η_E^i are characters of degree 1 of E. Since any proper subgroup of G is contained in some maximal subgroup and by (a), we get

$$\begin{aligned}
\chi &= \sum_i n_G^i \eta_G^i + \sum_{E < G} \sum_i n_E^i \operatorname{Ind}_E^G \eta_E^i \\
&= \sum_i n_G^i \eta_G^i + \sum_{E < G} \sum_i n_E^i \operatorname{Ind}_{H_E}^G \left(\operatorname{Ind}_E^{H_E} \eta_E^i\right),
\end{aligned} \tag{231}$$

where H_E is the maximal subgroup containing E. It shows that $R(G)$ is generated by the characters of degree 1 of G together with the $\operatorname{Ind}_H^G(R(H))$, where H runs over Y.

Now, I'll prove a proposition

Proposition 17. *If G is an elementary group, then $R(G) = R'(G)$.*

Proof. Let's use induction on $|G|$. If $|G| = 1$, then it is trivial, so let's assume that the statement is true for $|G| < n$ for some $n \in \mathbb{N}_{\geq 2}$. It is enough to show that $R(G) \subset R'(G)$.

Since $[G : H]$ is prime order, it is abelian, cf. *Abstract Algebra*, Dummit and Foote, Section 4.3 theorem 8, so we can apply (b). By induction, we know that $R(H) = R'(H)$ since H are all proper elementary subgroup of G, so $\mathrm{Ind}_H^G(R(H)) \subset R'(G)$. Since G is an elementary subgroup, by setting $E = G$ in the generating element $\mathrm{Ind}_E^G(\alpha - 1_E)$ of $R_0'(G)$ with 1_G, we know that any degree 1 character of G is contained in $R'(G)$. Therefore, it shows that $R(G) \subset R'(G)$ and we get $R(G) = R'(G)$. □

(d) In (b), I already justified the argument to write

$$\varphi = \sum_{E \in X} \mathrm{Ind}_E^G(\varphi_E) \tag{232}$$

where $\varphi_E = f_E \cdot \mathrm{Res}_E(\varphi)$ following the notation in the problem. If $\varphi(1) = 0$, then $\varphi_E(1) = 0$ for all E since $\mathrm{Res}_E(\varphi)(1) = \varphi(1) = 0$. Since we already showed that $\varphi_E \in R(E) = R'(E)$, it means that $\varphi_E \in R_0'(E)$ as $\varphi_E(1) = 0$. By (a), it shows that $\varphi \in R_0'(G)$. Finally, for general $\varphi \in R(G)$, consider $\varphi - \varphi(1)1_G$, then it is again in $R_0'(G)$ and $\varphi \in R'(G)$. Therefore, $R(G) \subset R'(G)$. Conversely, $R'(G) \subset R(G)$ since it is generated by the element of $R(G)$. It shows that $R'(G) = R(G)$.

8 Chapter 11

S 11.1 Assume I showed the following proposition: P2: "Let f be a class function on cyclic group G with values in $\mathbb{Q}$ such that $f(x^m) = f(x)$ for all m primes to g, then $f \in \mathbb{Q} \otimes R(G)$". Let the original statement P1. It is trivial that P1 implies P2. Also, P2 implies P1: using th. 21' in the textbook, it is enough to show that for any cyclic subgroup $H \leq G$, $\mathrm{Res}_H f \in \mathbb{Q} \otimes R(H)$.

Since we assumed P2 is true, it is again enough to show that $f(x^m) = f(x)$ for all m prime to $|H|$ for $x \in H$. To show it, let's fix $x \in H$ and m such that $(m, |H|) = 1$. Note that $(m, |G|)$ need not to be 1. However, there always exists $k \in \mathbb{N}$ such that $(m + k|H|, |G|) = 1$ by the Dirichlet's theorem on arithmetic progressions: the original statment of the Dirichelt's theorem is that if $(m, |H|) = 1$, then $m + k|H|$ contains infinitely many primes, which means that there exists k_0 such that $(m + k_0|H|, |G|) = 1$. It means that

$$f(x^m) = f(x^{m+k_0|H|}) = f(x). \tag{233}$$

(The second equality is by the assumption of P1.) Therefore, the condition for P2 is satisfied and I showed that P2 implies P1. Now, I can safely reduce G to a cyclic group.

Let the generator of G by x and $g = |G|$. Choose any irreducible character χ_k from $0 \leq k \leq g-1$ such that $\chi_k(x) = \exp(2\pi ik/g)$ of G, then

$$\langle f, \chi_k \rangle = \sum_{m=1}^{g} f(x^m) \exp\left(\frac{-2\pi ikm}{g}\right). \tag{234}$$

Now, take partition of $\{1, \ldots, g\}$ such that $(a, g) = q$ for $1 \leq q \leq g$, for example,

$$A_q = \{a \in \{1, \ldots, g\} : (a, g) = q\}. \tag{235}$$

Since $(a/q, g/q) = 1$, we get

$$\sum_{m \in A_q} \exp\left(\frac{-2\pi ikm}{g}\right) = \sum_{m \in A_q} \exp\left(\frac{-2\pi ik(m/q)}{g/q}\right) = \sum_{m \in (\mathbb{Z}/(g/q)\mathbb{Z})^\times} \exp\left(\frac{-2\pi ikm}{g/q}\right) \in \mathbb{Z} \tag{236}$$

for each q since the nth cyclotomic polynomial is in $\mathbb{Z}[x]$ for any $n \geq 1$. Now, I'll show a proposition.

Proposition 18. *For any $a_1, a_2 \in \{1, \ldots, g\}$ such that $(a_1, g) = (a_2, g) = q$ for some $q \in \mathbb{Z}$, there exists $m \in \mathbb{N}$ such that $a_1 m \equiv a_2 \mod g$.*

Proof. Consider $a_1/q, a_2/q \in (\mathbb{Z}/(g/q)\mathbb{Z})^\times$, so take $m \in \mathbb{Z}$ such that $(m, g/q) = 1$ and $a_1 m/q - a_2/q \equiv 0 \mod g/q$. It shows that $a_1 m - a_2 \equiv 0 \mod g$. Also, $(m, g) = 1$ since $(a_1 m, g) = (a_1, g)(m, g) = (a_2, g)$. $\square$

The above proposition shows that $f(x^{a_1}) = f(x^{a_2})$. Therefore,

$$\begin{aligned}
\langle f, \chi \rangle &= \frac{1}{g} \sum_{m=1}^{g} f(x^m) \exp\left(\frac{-2\pi ikm}{g}\right) \\
&= \frac{1}{g} \sum_{q=1}^{g} \sum_{m \in A_q} f(x^m) \exp\left(\frac{-2\pi ikm}{g}\right) \\
&= \frac{1}{g} \sum_{q=1}^{g} \sum_{m \in A_q} f(x^q) \exp\left(\frac{-2\pi ikm}{g}\right) \\
&= \frac{1}{g} \sum_{q=1}^{g} f(x^q) \sum_{m \in A_q} \exp\left(\frac{-2\pi ikm}{g}\right) \in \mathbb{Q},
\end{aligned} \tag{237}$$

for any irreducible character χ and it shows that $f \in \mathbb{Q} \otimes R(G)$.

In problem 3, we showed that Ψ^n maps $R(G)$ to $R(G)$, so extending the scalar to $\mathbb{Q}$, we can treat that Ψ^n maps $\mathbb{Q} \otimes R(G)$ to $\mathbb{Q} \otimes R(G)$. Also, if $\operatorname{Im} f \subset \mathbb{Z}$, so $\operatorname{Im} \Psi^n f \subset \mathbb{Z} \subset A$, then $(g/(g,n))\Psi^n f \in A \otimes R(G)$ by theorem 23. It means that for any irreducible character χ of G,

$$g/(g,n)\langle \Psi^n f, \chi \rangle \in \mathbb{Q} \cap A = \mathbb{Z}. \tag{238}$$

Therefore, $(g/(g,n))\Psi^n f \in R(G)$.

For a class function $f(s) = \delta_{s=1}$, $\Psi^n f$ captures elements $s \in G$ such that $|s| \mid n$, i.e. $\Psi^n f = 1$ if $|s| \mid n$ and 0 elsewhere. The above result shows that $g/(g,n)1_{\{s:|s|\|n\}} \in R(G)$, which generalize the result $g\delta_{s=1}$ is the character of regular representation.

From now on, I refered some articles in the internet, stackexchange, and stackoverflow and write the link of those sites. Because of the length of the url, I shorten the links in this homework.

I'll write some useful theorems which will be used in this homework. For some theorems, it will supplement the talks in the class. Furthermore, our rings are commutative and have 1 if there is no mention.

Theorem 19. *If T is integral over R, then both have same krull dimension.*

Proof. See *Commutative Rings*, Kaplansky, Theorem 48, p. 32. □

Theorem 20. *Let $f : A \to B$ be an integral extension. For a maximal ideal M in B, $f^{-1}(B)$ is again a maximal ideal in A.*

Proof. See *Commutative Algebra*, Atiyah, corollary 5.8, p. 61. □

Theorem 21. *Let $f : A \to B$ be a ring homomorphism, then it induces the continuous map $f^* : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ by $f^*(p_B) = f^{-1}(p_B)$ for $p_B \in \operatorname{Spec}(B)$. If B is integral over A, then f^* is a surjective and a closed map.*

Proof. See *Commutative Algebra*, Atiyah, p. 13, p. 62, and p. 67. □

Theorem 22. $\operatorname{Spec}(A)$ *is irreducible if and only if the nilradical of A is prime ideal.*

Proof. See *Commutative Algebra*, Atiyah, p. 13. □

Remark 23. If the nilradical of A is prime ideal, then $\text{Spec}(A)$ is connected since there is no disjoint open set. It proves that "$\text{Spec}(A)$ is connected", where the A in the statement is defined in the textbook as A is integral domain.

Before solving the problems, let's define some global notation clarifying the notation in the textbook. Set $g = |G|$ and $\mu = \exp(2\pi i j/g)$. Let's write

$$\mathbb{Z} \xrightarrow{i_1} A \xrightarrow{i_2} A \otimes_{\mathbb{Z}} R(G) \xrightarrow{i_3} A^{\text{Cl}(G)}, \tag{239}$$

where

$$\begin{aligned}
A &:= \oplus_{j=0}^{g-1} \mathbb{Z}\mu^j \\
i_2(a) &= a \otimes 1_G \quad \text{and} \\
i_3(a \otimes f) &= af,
\end{aligned} \tag{240}$$

where $a \in A$ and $f \in R(G)$. Note that the maps are integral extensions, so it induces well-defined surjective closed map

$$\text{Spec}(A^{\text{Cl}(G)}) \xrightarrow{i_3^*} \text{Spec}(A \otimes_{\mathbb{Z}} R(G)) \xrightarrow{i_2^*} \text{Spec}(A) \xrightarrow{i_1^*} \text{Spec}(\mathbb{Z}) \tag{241}$$

by the theorem 21.

Now, I'll show a proposition in the textbook.

Proposition 24. *If M is a maximal ideal in A, then A/M is finite, in fact, $|A/M| = p^n$ for some prime p and n.*

Proof. Since M is maximal ideal, $i_1^*(M)$ is maximal ideal in $\mathbb{Z}$ by the theorem 21. Therefore, i_1 induces the map

$$\mathbb{Z}/(i_1^{-1}(M)) \xrightarrow{\bar{i}_1} A/M. \tag{242}$$

Note that this map is injective field homomorphism. Considering $\bar{i}_1$ as a $\mathbb{Z}$-module homomorphism, we get $\text{char}(A/M) = p$. It shows that for any roots of unity μ of g, $p\mu = 0$ in A/M, so A/M can be considered as a subring of $\sum_{i=1}^{g} \mathbb{F}_p \mu_i$, where $\{\mu_i\}$ is the set of roots of unity of g with $\mu_1 = 1$. It ends the proof. □

Proposition 25. $A^{\text{Cl}(G)}$ *is integral over $\mathbb{Z}$. It implies that $A \otimes R(G)$ is integral over $\mathbb{Z}$.*

Proof. Choose $a = (a_1, \ldots, a_h) \in A^{\text{Cl}(G)}$. For each a_i, it is integral over $\mathbb{Z}$, so there exists monic polynomial $p_i(x) \in \mathbb{Z}[x]$ such that $p_i(a_i) = 0$. In $A^{\text{Cl}(G)}$, it is

$$p_i((a_1, \ldots, a_h)) = (p_i(a_1), \ldots, p_i(a_h)), \tag{243}$$

and it definitely have 0 at ith position. Now, set $p(x) = \prod_{i=1}^{h} p_i(x)$, then each ith polynomial generate 0 at ith position, so $p(a) = 0$. Also, it is monic polynomial in $\mathbb{Z}[x]$ since each p_i are monic. Since $A \otimes R(G)$ is a subring of $A^{\text{Cl}(G)}$, it is integral over $\mathbb{Z}$. □

Let B be a A-algebra and let $\varphi : A \to B$ be the map sending A to the center of B. Now, we can consider $B \otimes_{\mathbb{Z}} R(G)$ by drawing commutative diagram

$$
\begin{array}{ccc}
B \times R(G) & \xrightarrow{\ i\ } & B \otimes R(G) \\
& \searrow{\scriptstyle f} & \downarrow{\scriptstyle \Phi} \\
& & B^{cl(G)}
\end{array}
$$

where i is the inclusion map and

$$ f : (b, \chi) \mapsto b(\varphi \circ \chi), \tag{244} $$

i.e. for $s \in G$, $f((b, \chi))(s) = b\varphi(\chi(s))$. Since f is $\mathbb{Z}$-bilinear, Φ is a well-defined $\mathbb{Z}$-module homomorphism. Also, B and $R(G)$ are $\mathbb{Z}$-algebra, so $B \otimes R(G)$ is again $\mathbb{Z}$-algebra.

Corollary 26. $B^{\mathrm{Cl}(G)}$ *is integral over* B. *This implies that* $B \otimes R(G)$ *is integral over* B

Proof. We can not say that B is integral over $\mathbb{Z}$, but we know that B is integral over itself, so by applying the proof of proposition 25, we get the first result. Since $B \otimes R(G)$ is a subring of $B^{\mathrm{Cl}(G)}$ by Φ, we get the second result. $\qquad\square$

From now on, I'll prove the main problems.

S 11.2 Let's take quotient on (239). Note that non-zero prime ideals in each ring is maximal by the theorem 19. Choose a maximal ideal M in A and choose a conjugacy class c in G. For the maximal ideal M_c in $\mathbb{A}^{\mathrm{Cl}(G)}$, we get the well-defined induced maps

$$ \mathbb{Z}/(i_1^{-1}(M)) \xrightarrow{\bar{i}_1} A/M \xrightarrow{\bar{i}_2} (A \otimes_{\mathbb{Z}} R(G))/P_{M,c} \xrightarrow{\bar{i}_3} A^{\mathrm{Cl}(G)}/M_c. \tag{245} $$

Note that all the field homomorphisms are non-trivial mapping 1 to 1, so those are injective. Also, by identifying $A^{\mathrm{Cl}(G)} \simeq \oplus_{i=1}^{h} A$ where $h = |\mathrm{Cl}(G)|$, $A^{\mathrm{Cl}(G)}/M_c \simeq A/M$ as a field by the projection $\pi_c : A^{\mathrm{Cl}(G)} \to A/M$ such that $\pi_c((a_1, \ldots, a_h)) = [a_c] \in A/M$: $\ker \pi_c = M_c$. If I show that $\bar{i}_3 \circ \bar{i}_2$ is surjective, then it ends the proof: if $\bar{i}_2$ is not surjective, then there exists $f \in (A \otimes R(G))/P_{M,c}$, and $\bar{i}_3(f)$ is not in the image of $\bar{i}_3 \circ \bar{i}_2$ as $\bar{i}_3$ is injective, which is contradiction. However, if I choose $[(a_1, \ldots, a_h)] \in A^{\mathrm{Cl}(G)}/M_c$, then I just choose $\pi_c((a_1, \ldots, a_h)) = [a_c]$ in A/M. Now, we get

$$ \bar{i}_3 \circ \bar{i}_2([a_c]) = [(a_c, a_c, \ldots, a_c)] = [(a_1, \ldots, a_h)]. \tag{246} $$

As $\bar{i}_2$ is bijective, the residue field of $P_{M,c}$ is isomorphic to A/M.

S 11.3 (Idea: We don't know what is B, but at least, we know that it contains some integer by the mapping $\varphi : 1_A \mapsto 1_B$. I'll use this property.)

Let's consider a sequence

$$ \mathbb{Z} \xrightarrow{i_1} A \xrightarrow{\varphi} B \xrightarrow{i_2} B \otimes_{\mathbb{Z}} R(G) \xrightarrow{i_3} B^{\mathrm{Cl}(G)}, \tag{247} $$

where $\varphi : A \to B$ is the ring homomorphism into the center of B with $1_A \mapsto 1_B$. By theorem 21, we know that the above sequence induces

$$ \mathrm{Spec}(B^{\mathrm{Cl}(G)}) \xrightarrow{i_3^*} \mathrm{Spec}(B \otimes_{\mathbb{Z}} R(G)) \xrightarrow{i_2^*} \mathrm{Spec}(B) \xrightarrow{\varphi^*} \mathrm{Spec}(A) \xrightarrow{i_1^*} \mathrm{Spec}(\mathbb{Z}). \tag{248} $$

55

Also, by the corollary 26, we know that i_3^* and i_2^* are surjective and closed. Now, let's choose a prime ideal M in B and a conjugacy class c in G. Let's consider the prime ideal M_c in $B^{\mathrm{Cl}(G)}$, then $P_{M,c} = i_3^{-1}(M_c)$ is a prime ideal in $B \otimes R(G)$ by the map i_3^*. Since i_3^* is surjective, any prime ideal $\mathfrak{m}$ in $B \otimes R(G)$ is of the form $P_{M,c}$, where M is a prime ideal of $B^{\mathrm{Cl}(G)}$ and c a conjugacy class.

Proposition 27. *Let M be a prime ideal in B and consider an integral domain B/M. Set $N = \operatorname{char} B/M$.*

1. *If $N = 0$, then $P_{M,c_1} = P_{M,c_2}$ if and only if $c_1 = c_2$.*

2. *If $0 < N$, N is some prime number $p \in \mathbb{Z}$. Also, $P_{M,c_1} = P_{M,c_2}$ if and only if $c_1' = c_2'$, which is p'-component of c_1 and c_2 defined in the proposition 30'.*

Proof. To prove (i), I need to show that $c_1 \neq c_2$ implies $P_{M,c_1} \neq P_{M,c_2}$. For element $x_1 \in c_1$ and $x_2 \in c_2$ in G, choose p such that $(p, |x_1\|x_2|) = 1$. Now, we can say that x_1 is p'-element. From lemma 8, there exists integer valued $\psi \in A \otimes R(G)$ such that $\psi(x_1) \neq 0$ and $\psi(c_2) = 0$. It shows that $\psi \in P_{M,c_2} \setminus P_{M,c_1}$, and we get $P_{M,c_1} \neq P_{M,c_2}$.

Now, assume $N > 0$. Since B/M is an integral domain, N should be a prime p. If $p \cdot 1_B \neq 0$, then $p \in M$, and if $p \cdot 1_B = 0$, then $p \in \ker \varphi$, so $p \in \varphi^{-1}(M) \cap \mathbb{Z}$. For any $\chi \in A \otimes R(G)$ and $x \in G$, let x_r be the p'-component of x. By the exercise 10.4, $\chi(x) \equiv \chi(x_r) \mod \varphi^{-1}(M)$, so $\varphi(\chi(x)) \equiv \varphi(\chi(x_r))$ mod M. It shows that $P_{M,c_1} \cap \operatorname{Im} \varphi(A \otimes R(G)) = P_{M,c_1'} \cap \operatorname{Im} \varphi(A \otimes R(G))$. However, if $c_1' \neq c_2'$, by the lemma 8, we know that $P_{M,c_1'} \cap \operatorname{Im} \varphi(A \otimes R(G)) \neq P_{M,c_2'} \cap \operatorname{Im} \varphi(A \otimes R(G))$: we can impose some integer $n \not\equiv 0 \mod p$ on c_1' and 0 on c_2', which shows that $\varphi(n) = \varphi(n \cdot 1_A) = (n\%p) \cdot 1_B \notin M$ by the definition of N. (% is remainder operator.) $\square$

S 11.4 Note that $R(G)$ contains $\mathbb{Z}$, so the inclusion $i : R(G) \to A \otimes R(G)$ an integral extension with same krull dimension 1. Using theorem 21, we know that $i^* : \operatorname{Spec}(A \otimes R(G)) \to \operatorname{Spec}(R(G))$ is a surjective closed map. More precisely, any prime ideal in $R(G)$ is of the form $P_{M,c} \cap R(G)$, where $P_{M,c}$ is the prime ideal in $A \otimes R(G)$ following the notation in the textbook. Now, I need to check the conditions on prime ideals in $A \otimes R(G)$ that i^* maps to the same prime ideal. I'll prove a proposition.

Proposition 28. *Let R be a ring, G a finite group of automorphisms of R, and R^G the subring of R which are invariant under G. Also, assume R is integral over R^G. (In fact, we don't have to assume it. See the reference in the last.) Let $p : \operatorname{Spec} R \to \operatorname{Spec} R^G$ denotee the morphism induced by the inclusion $i : R^G \to R$, then $p(x_1) = p(x_2)$ if and only if there exists a $\sigma \in G$ such that $\sigma(x_1) = x_2$.(This is the problem 3.20 in Chapter 2 in Algebraic geometry and arithmetic curves, Qing Liu.)*

Proof. If x is a prime ideal and $\sigma \in G$, $\sigma(x)$ is a prime ideal since $ab \in \sigma(x)$ means that $(\sigma^{-1}a)(\sigma^{-1}(b)) \in x$, so a or b is in $\sigma(x)$. It shows that G acts on $\operatorname{Spec} R$.

Assume $\sigma(x_1) = x_2$. Since i is injective, $i^{-1}(a) = a$ if $\sigma(a) = a$ for all $\sigma \in G$ and $\emptyset$ otherwise by identifying $R^G \subset R$. Therefore,

$$p(x_1) = i^{-1}(x_1) = i^{-1}\left(\cap_{\sigma \in G} \sigma(x_1)\right) = i^{-1}(x_2) = p(x_2). \tag{249}$$

Conversely, assume $p(x_1) = p(x_2)$. Now, for some non-zero $a \in x_1$,

$$\prod_{\sigma \in G} \sigma(a) \in p(x_1) = p(x_2) \subset x_2, \tag{250}$$

so there exists $\sigma \in G$ such that $\sigma(a) \in x_2$, i.e. $a \in \sigma(x_2)$ abusing notation since x_2 is prime. It shows that

$$x_1 \subset \cup_{\sigma \in G} \sigma(x_2). \tag{251}$$

Using prime avoidance lemma, cf. *Commutative algebra*, Atiyah, proposition 1.11, p. 8, we know that $x_1 \subset \sigma(x_2)$ for some $\sigma \in G$. Finally, using incomparable condition for the integral extension, cf. *Commutative algebra*, Kaplansky, theorem 44, p. 29, we get $p_1 = \sigma(p_2)$. It ends the proof. (This is the proof from "https://bit.ly/2SH8wcp".) □

Note that our problem perfectly fits with the proposition by applying the automorphism group Γ, $R = A \otimes R(G)$, and $R^{\Gamma} = R(G)$. Checking what is Γ, we easily see that $K = \mathbb{Q}(\mu_g)$, where μ_g is the primitive gth root of unity: as $\mu_g \in A$, $\mu_g \in K$ and $\mathbb{Q} \in K$, so $\mathbb{Q}(\mu_g) \subset K$. Conversely, K is the smallest field containing A, so $K \subset \mathbb{Q}(\mu_g)$. Therefore, it is a cyclotomic extension and the Galois group of $K/\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/g\mathbb{Z})^{\times}$.

Let $\sigma_k \in \Gamma$ by setting $\sigma(\mu_g) = \mu_g^k$ for $(k, g) = 1$, then we get

$$\sigma_k \left(\sum_{i=1}^{h} a_i \otimes \chi_i \right) = \sum_{i=1}^{h} \sigma_k(a_i) \otimes \chi_i \tag{252}$$

where χ_i are the irreducible characters of G.

Using the above proposition, we know that $i^*(x_1) = i^*(x_2)$ for $x_1, x_2 \in \text{Spec}(A \otimes R(G))$ if and only if there exists $\sigma \in \text{Gal}(\mathbb{Q}(\mu_g)/\mathbb{Q})$ such that $x_1 = \sigma(x_2)$. Finally, we combine the condition with the proposition 30', then we exactly get the condition when the primes of the form $P_{M,c}$ in $A \otimes R(G)$ maps to the same prime ideal in $R(G)$.

Addition: I tried to figure out what is the explicit form of the prime. There were some hard points, however, figuring out the explicit form: First, the Galois action only acts on the coefficient of irreducible characters, so we can not know how the $P_{M,c}$ moves: even I can not know whether c moves to another class. Second, The prime ideal in cyclotomic integer is not easy to describe. See "https://bit.ly/3c77Zr5".

S 11.5 In the problem 3.3, we already shows that there exists the canonical isomorphism φ between G and $\hat{\hat{G}}$ by mapping $\varphi(g)(\chi) = \chi(g)$ for irreducible representation χ of G. This isomorphism extends to the ring isomorphism $\bar{\varphi}$ between $\mathbb{Z}[G]$ and $R(\hat{G})$, and again $1 \otimes \bar{\varphi}$ between $A \otimes \mathbb{Z}[G] \simeq A[G]$ and $A \otimes R(\hat{G})$. Abusing notation, let the final isomorphism φ. Since it is a ring isomorphism, it is enough to determine $\text{Spec}(A \otimes R(\hat{G}))$ to check $\text{Spec}(A[G])$.

Now, I prove a proposition.

Proposition 29. *Let G be a finite abelian group with primary cyclic group decomposition*

$$G \simeq \mathbb{Z}/q_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/q_t\mathbb{Z}, \tag{253}$$

where q_i are powers of primes which are not necessarily distinct. Then we again get

$$\hat{G} \simeq \mathbb{Z}/q_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/q_t\mathbb{Z}. \tag{254}$$

(Warning: this is not canonical isomorphism.)

Proof. Let the generator of each $\mathbb{Z}/q_i\mathbb{Z}$ part by x_i. For a cyclic group $\mathbb{Z}/q_i\mathbb{Z}$, we know that it has irreducible character χ_k^i such that for the generator x_i of $\mathbb{Z}/q_i\mathbb{Z}$,

$$\chi_k^i(x_i^m) = \exp\left(\frac{2\pi i k m}{q_i}\right). \tag{255}$$

Extend this character to G by setting

$$\chi_k^i(x_j) = 1 \tag{256}$$

if $i \neq j$. We can easily check that each χ_k^i defined on G are irreducible and disjoint to each other for k and i by computing $\langle \cdot, \cdot \rangle$. Also,

$$(\chi_1^i)^k(x_i) = \left(\exp\left(\frac{2\pi i}{q_i}\right)\right)^k = \chi_k^i(x_i), \tag{257}$$

so χ_1^i is a generator of cyclic subgroup of order q_i in G. Let the subgroup C_i for each i. Finally, we know that $C_i C_j = C_j C_i$ for each i, j since $\hat{G}$ is abelian and $\oplus_{i=1}^{m-1} C_i \cap C_m = \{1\}$ for all $1 < m \leq t$ since each C_i have non-zero function value only on x_i. It shows that

$$\oplus_{i=1}^{t} \mathbb{Z}/q_i\mathbb{Z} \simeq \oplus_{i=1}^{t} C_i = \hat{G} \tag{258}$$

$\square$

Using this group isomorphism, we know that $A \otimes R(G)$ and $A \otimes R(\hat{G})$ are isomorphic: we can easily see this using the property of the tensor product: apply tensor product on the exact sequence

$$0 \to R(G) \to R(\hat{G}) \to 0. \tag{259}$$

Let the ring isomorphism $\varphi : A[G] \to A \otimes R(G)$. Since we already know what is the prime ideals in $A \otimes R(G)$, by pulling back the prime ideals using φ, we get $\text{Spec}(A[G])$.

S 11.6 Note that A has krull dimension 1 and is integral domain, so any non-zero prime ideal in A is maximal ideal. Fix a maximal ideal M with character p. By the exercise 10.4, we get $f(c) \equiv f(c') \mod M$ for any conjugacy class c with p-regular class c' of c for any $f \in A \otimes R(G)$. Therefore, $A \otimes R(G) \subset B$.

Note that $A \otimes R(G) \subset B \subset A^{\text{Cl}(G)}$ and each are integral extension. Therefore, it is enough to show that for any prime M_c in $A^{\text{Cl}(G)}$, $M_c \cap B = P'_{M,c}$ satisfies the same condition in proposition 30': for prime ideal $\mathfrak{p} = P'_{M,c}$ in B, $\mathfrak{p} \cap A$ is a prime ideal. It shows that $\mathfrak{p}$ determines M uniquely.

Assume $M = 0$. From theorem 23', we know that $g1_c \in A \otimes R(G)$ for any class c in G, so if $c_1 \neq c_2$, then $P'_{M,c_1} \neq P'_{M,c_2}$. Now, assume $M \neq 0$ with residue character p with the same notation in proposition 30' (ii). By the definition of B, if $f \in P'_{M,c_1}$, then $f \in P'_{M,c_1'}$ as $f(c_1) \in M$ implies $f(c_1') \in M$ for any p-regular class c_1'. The converse is also true, so we get $P'_{M,c_1} = P'_{M,c_1'}$. Finally, the lemma 8 shows that there exists integer valued $f \in A \otimes R(G)$ for fixed $x \in c_1'$ such that $f(x) \notin p\mathbb{Z}$ and $f(s) = 0$ for each p'-element s not conjugate to x, which shows that $f \notin M_{c_1'}$ as $M_{c_1'} \cap \mathbb{Z} = p\mathbb{Z}$. Since $f(c_2') = 0 \in M$, it shows that $P'_{M,c_1} = P'_{M,c_1'} = P'_{M,c_2'} = P'_{M,c_2}$ if and only if $c_1' = c_2'$. It shows that two rings have the same spectrum of form $P_{M,c}$ (resp. $P'_{M,c}$).

Let $G = \mathbb{Z}_4$ with generator t. Every class in G have 2-regular component class 1. $A = \mathbb{Z}[i]$, which is Gaussian integer. The Gaussian integer Euclidean domain, so prime ideals are principal

ideal and maximal ideal. Define a function $f \in A^{\text{Cl}(G)}$ by setting $f(1) = 1$, $f(t) = 2+i$, $f(t^2) = 4-i$, and $f(t^3) = 6 - i$. For any maximal ideal M with residue class $p > 2$, p-regular class of t^i is t^i, so it automatically satisfies the condition for B. For $p = 2$, we know that $M = \langle 1 - i \rangle = \langle 1 + i \rangle$; since $i(1 - i)^2 = (1 - i)(1 + i) = 2$ and $1 \pm i$ are Gaussian primes. The $2'$ component for any elements in G is 1, so $f \in B$. Let's claim that

$$f = \sum_{i=0}^{3} a_j \chi_j, \tag{260}$$

where $a_j \in \mathbb{C}$ and $\chi_j(t) = \mu = \exp(2\pi i j / 4)$. The above condition shows that

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 + i \\ 4 - i \\ 6 - i \end{pmatrix}. \tag{261}$$

The solution is

$$(a_0, a_1, a_2, a_3) = \left(-\frac{1}{4} + \frac{5i}{4}, -\frac{3}{4} - \frac{i}{4}, -\frac{5}{4} - \frac{3i}{4}, \frac{13}{4} - \frac{i}{4} \right) \notin A^4. \tag{262}$$

It shows that B is strictly larger than $A \otimes R(G)$.

6-8(S 11.7**)**

(a) If $H \cap c = \emptyset$, then for any $f \in R(H)$ and $x \in c$,

$$\text{Ind}_H^G f(x) = \sum_{\substack{s \in G \\ sxs^{-1} \in H}} f(sxs^{-1}) = 0, \tag{263}$$

so $f \in P_{0,c}$ and $\text{Im}(A \otimes \text{Ind}_H^G) \subset P_{0,c}$. Conversely, if $x \in H \cap c$ for some $x \in G$, let $c' = \{sxs^{-1} : s \in H\}$. This is a class in H containing x, so $h1_{c'} \in A \otimes R(H)$. Since

$$h \, \text{Ind}_H^G 1_{c'}(x) = \sum_{\substack{s \in G \\ sxs^{-1} \in c'}} 1_{c'}(sxs^{-1}) > 0, \tag{264}$$

we get $\text{Im}(A \otimes \text{Ind}_H^G) \not\subset P_{0,c}$.

(b) Since $p \in A$, M has residue characteristic p.

Assume H contains no p-elementary subgroup associated with an element of c. If $f \in A \otimes R(H)$, then $\text{Im } f \subset A$. Therefore, by the lemma 11, we know that $\text{Ind}_H^G f(c) \in pA$, and $pA \subset M$. It shows that $I_H \subset P_{M,c}$.

Conversely, assume H contains a p-elementary subgroup associated with an element $x \in c$. By the lemma 8, there exists an integer valued $f \in A \otimes R(H)$ such that $f' = \text{Ind}_H^G f$ satisfies $f'(x) \in \mathbb{Z}$, but $f'(x) \not\equiv 0 \mod p$, which means that $f' \notin P_{M,c}$. It shows that $I_H \not\subset P_{M,c}$.

(c)

Theorem 30. *theorem 18*

Proof. To prove theorem 18, it is enough to show that $A \otimes V_p$ has finite index in $A \otimes R(G)$ and the index is prime to p. First, assume that the index finite, later I'll check this condition.

Let $X(p)$ be the family of p-elementary subgroups of G. Consider an ideal I generated by I_H for each $H \in X(p)$. If $I = A \otimes R(G)$, then it ends the proof, so we can safely set I be a proper ideal. Note that it is contained in some maximal ideal of the form $P_{M,c}$ where M is a maximal ideal in A and a class c in G. If A/M has characteristic different from p, it ends the proof since $p \notin I$, so assume $p \in M$. Let's write p-regular class of c by c'. Choose a p-elementary subgroup H associated with an element of c' By (b), we know that $I_H \not\subset P_{M,c'} = P_{M,c}$, which is contradiction since $H \in X(p)$. Therefore, its conclusion is that $M \cap \mathbb{Z}$ have prime different problem p, so the index of V_p in $R(G)$ is prime to p; in this step, I use the finite index assumption.

Now, let's show that V_p has finite index in $R(G)$. It is equivalent to say that there exists $l \in \mathbb{N}$ such that $l \cdot 1_G \in V_p$. Now, we use Artin's theorem. Artin's theorem says that for the set of cyclic groups Y in G, there exists $l \in \mathbb{N}$ and $\chi_H \in R(H)$ such that

$$l1_G = \sum_{H \in Y} \mathrm{Ind}_H^G \chi_H. \tag{265}$$

For each cyclic group H, there exists a generator t_H, and consider the p-elementary subgroup P_H associated to $(t_H)_r$. Since $(t_H)_u \in Z((t_H)_r)$, $H \leq P_H$. Therefore,

$$l1_G = \sum_{H \in Y} \mathrm{Ind}_H^G \chi_H = \sum_{H \in Y} \mathrm{Ind}_{P_H}^G \left(\mathrm{Ind}_H^{P_H} \chi_H \right), \tag{266}$$

which shows that $l1_G \in V_p$. It ends the proof. $\square$

Theorem 31. *Theorem 23'''*

Proof. Assume there exists $H \in I$ such that H does not contains any elementary subgroups of G. For $g = 1, 2$ such H does not exist, so assume $g > 2$. It means that I_H is contained in $P_{M,c}$ for all maximal ideal M in A and conjugacy class c: for any maximal ideal M having residue class p and conjugacy class c, we know that $P_{M,c} = P_{M,c'}$ where c' is p-regular class associated with c, so by (b), $I_H \subset P_{M,c'} = P_{M,c}$. Since all the maximal ideals in $A \otimes R(G)$ is of the form $P_{M,c}$ with non-zero prime ideals M, we get I_H is contained in the Jacobson ideal of $A \otimes R(G)$.

Now, we know that $\mathrm{Ind}_H^G r_H = r_G$, so $r_G \in I_H$. By the property of Jacobson radical, cf. *Commutative Algebra*, Atiyah, p. 6, we get $1 - f r_G$ is a unit in $A \otimes R(G)$ for all $f \in A \otimes R(G)$. However, for $f = 1_G$, $\chi = 1_g - r_G$ is not unit: note that $\chi(1) = 1 - g$ and $\chi(s) = 1$ for $s \neq 1$. If $g = 1$, then χ is not unit since $\chi(1) = 1$, so assume $g > 2$. If It was unit, there exists $\eta \in A \otimes R(G)$ such that $\eta(1) = \frac{1}{1-g}$ and $\eta(s) = 1$ for $s \neq 1$. However, $\eta(1) \in A$, so if $g > 2$, $\eta(1) \in A \cap \mathbb{Q} = \mathbb{Z}$, which is not possible. It ends the proof. $\square$

Supplement:
Thm 23 From the class, what I need to show is the following:

Proposition 32. *For each conjugacy class c of p-group G, and each irreducible character χ of G, we have $1/(g,n) \sum_{x^n \in c} \chi(x) \in A$.*

and what we actually proved is the following

Proposition 33. *Let c be a conjugacy class of a p-group G, let χ be a character of degree 1 of G, and let $a_c \sum_{x^n \in c} \chi(x)$. Then $a_c \in (g,n)A$.*

To end the proof, I need to show that proposition 33 implies 32.
Before start, I'll prove some propositions.

Proposition 34. *For a conjugacy class c of G, set $c^{-1} = \{s^{-1} : s \in c\}$, then c^{-1} is again a conjugacy class.*

Proof. If $a_1, a_2 \in c^{-1}$, then $a_1^{-1}, a_2^{-1} \in c$, so there exists $s \in G$ such that $sa_1^{-1}s^{-1} = a_2^{-1}$. It shows that $sa_1s^{-1} = a_2$. Conversely, for fixed $a_1 \in c^{-1}$, $sa_1s^{-1} \in c^{-1}$ by the same reason. $\square$

Proposition 35. *For a conjugacy class c of G and a subgroup $H \leq G$, $c \cap H$ is a disjoint union of the conjugacy classes in H if $c \cap H \neq \emptyset$.*

Proof. Assume $a \in c \cap H$, then for any $s \in H$, $sas^{-1} \in c \cap H$. It ends the proof. $\square$

From the fact that any irreducible character of p-group is induced by a character of degree 1, for an irreducible character χ of G, choose degree 1 character η of H such that $H \leq G$ satisfying $\chi = \mathrm{Ind}_H^G \eta$. Note that any subgroup of p-group is again p-group, so H is p-group. Now,

$$\langle \chi, \Psi^n f_{c^{-1}} \rangle = \frac{1}{g} \sum_{x^n \in c} \chi(x). \tag{267}$$

On the other hands,

$$\langle \chi, \Psi^n f_{c^{-1}} \rangle = \langle \eta, \mathrm{Res}_H \Psi^n f_{c^{-1}} \rangle = \frac{1}{h} \sum_{x \in H} \eta(x) f_{c^{-1}}(x^{-n}) = \frac{1}{h} \sum_{x \in H, x^n \in c \cap H} \eta(x). \tag{268}$$

By the proposition 35, $c \cap H$ is a disjoint union of c_H^i, where these are conjugacy classes of H, so

$$\frac{1}{h} \sum_{x \in H, x^n \in c \cap H} \eta(x) = \frac{1}{h} \sum_i \sum_{x \in H, x^n \in c_H^i} \eta(x) \in (h, n)A \tag{269}$$

by the 33. Finally, it implies

$$\langle \chi, \Psi^n f_{c^{-1}} \rangle \in (h, n)A \subset (g, n)A, \tag{270}$$

and we get

$$\frac{1}{(g,n)} \sum_{x^n \in c} \chi(x) \in A. \tag{271}$$

It ends the proof.