FINAL

박성빈, 수학과, 20202120

Notation: I'll reserve $g = |G|$ and $h = |H|$ if there is no additional mention.

1 The induced character from H to G is written by

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

for $s \in G$. Let's prove that this is the valid formula. Let $R = \{1 = g_1, \ldots, g_n\} \subset G$ be the representatives of the left cosets G/H and choose $s \in G$. For $\theta : H \to GL(V)$, choose a basis of V by $\{v_j\}_{j=1}^m$. Now, choose a basis of $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$ by

$$\{g_1 \otimes v_1, g_1 \otimes v_2, \ldots, g_1 \otimes v_m, g_2 \otimes v_1, \ldots, g_n \otimes v_m\}. \tag{2}$$

Let's consider the matrix $\text{Ind}_H^G \theta(s)$ by the action onto $g_i \otimes V$ blocks, then the diagonal block part survives if and only if s maps $g_i \otimes V$ block to $g_i \otimes V$ block, in other words, $g_i^{-1}sg_i \in H$, so

$$s \cdot (g_i \otimes v_j) = g_i \otimes ((g_i^{-1}sg_i) \cdot v_j). \tag{3}$$

Also, if s succeed to make map $g_i \otimes V$ to $g_i \otimes V$, the action to V part is $\theta(g_i^{-1}sg_i)$, so tracing the $\text{Ind}_H^G \theta(s)$ is of the form

$$\text{Ind}_H^G f(s) = \sum_{\substack{i \\ g_i^{-1}sg_i \in H}} f(g_i^{-1}sg_i). \tag{4}$$

Finally, f is the class function in H, so for any $h \in H$,

$$f(g_i^{-1}sg_i) = f(h^{-1}g_i^{-1}sg_ih) = f((g_ih)^{-1}s(g_ih)). \tag{5}$$

It shows that

$$\text{Ind}_H^G f(s) = \frac{1}{h} \sum_{\substack{t \in G \\ t^{-1}st \in H}} f(t^{-1}st). \tag{6}$$

2

(a) Let $\{1 = g_1, \ldots, g_n\}$ be the representatives of the left cosets G/H; note that $n = g/h$. For $s \in G$, $\chi(s)$ counts the elements in the representatives satisfying $g_i^{-1}sg_i \in H$. On the other hand,

$$\text{Ind}_H^G(1)(s) = \frac{1}{h} \sum_{\substack{t \in G \\ t^{-1}st \in H}} 1. \tag{7}$$

For any $s' \in H$, $(g_is')^{-1}s(g_is') \in H$ is equivalent to saying that $g_i^{-1}sg_i \in H$, so the above sum is equivalent to

$$\text{Ind}_H^G(1)(s) = \frac{1}{h} \sum_{\substack{t \in G \\ t^{-1}st \in H}} 1 = \sum_{i : g_i^{-1}sg_i \in H} 1, \tag{8}$$

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

(b) As χ is a character, we get

$$
\begin{aligned}
\langle \chi, 1_G \rangle &= \langle \mathrm{Ind}_H^G(1_H), 1_G \rangle \\
&= \langle 1_H, \mathrm{Res}_H 1_G \rangle \text{ (By the Frobenius reciprocity)} \qquad (9) \\
&= \langle 1_H, 1_H \rangle = 1,
\end{aligned}
$$

and χ contains one irreducible character component 1_H. It shows that $\psi = \chi - 1_H$ is again a character.

(c) Since
$$
\langle \chi - 1, \chi - 1 \rangle = \langle \chi, \chi \rangle - 2\langle \chi, 1 \rangle + \langle 1, 1 \rangle = \langle \chi, \chi \rangle - 1, \qquad (10)
$$

ψ is an irreducible character if and only if $\langle \chi, \chi \rangle = 2$. Furthermore, from the exercise 2.6, $\chi - 1$ is irreducible if and only if G acts on G/H doubly transitively, equivalently saying that $\langle \chi, \chi \rangle = \langle \chi^2, 1 \rangle = 2$; note that $\chi(s)$ is real-valued for all s as it is induced from the real-valued class function. The doubly transitive condition comes the property that the permutation action on $X \times X$ have characteristic χ^2 and $\langle \chi^2, 1 \rangle = 2$ if and only if there is only two distinct orbits under the action of G. Definitely, H is not a normal subgroup of G if it is doubly transitive on G/H.

3 너무 길어서 뒤로 빼겠습니다.

4 The first condition is translated as follows:
$$
\sum_{s \in G} \varphi(s) = 0. \qquad (11)
$$

In the problem 6.7 in the textbook, which I remember that we solved in the midterm, we showed that $|\chi(s)| \leq \chi(1)$ for irreducible character χ. For each irreducible representation χ,

$$
\begin{aligned}
\mathrm{Re}\left(\langle \varphi, \chi \rangle\right) = \sum_{s \in G} \varphi(s^{-1}) \,\mathrm{Re}\left(\chi(s)\right) &= \chi(1)\varphi(1) + \sum_{s \neq 1} \varphi(s^{-1}) \,\mathrm{Re}(\chi(s)) \\
&\geq \chi(1)\varphi(1) + \chi(1) \sum_{s \neq 1} \varphi(s^{-1}) = \chi(1) \sum_{s \in G} \varphi(s^{-1}) = 0
\end{aligned}
\qquad (12)
$$

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.

5

Theorem 1. *(Artin's theorem) Let G be a finite group, and X be the set of all the cyclic subgroups of G. For any virtual character $\chi \in R(G)$, there exists $\eta_C \in R(C)$ for each $C \in X$ and $k \in \mathbb{N}$ satisfying*
$$
k\chi = \sum_{C \in X} \mathrm{Ind}_C^G \eta_C. \qquad (13)
$$

Definition 2. Let G be a finite group. For a prime $p \in \mathbb{N}$, $x \in G$ is a p-element if its order is of the power of p. We say $x \in G$ is a p'-element if its order is coprime to p. A group H is called p-elementary group if it is the direct product of a cyclic group C of order coprime to p and a p-group P, i.e. $H = C \times P$.

Remark 3. Let G be a finite group. To consider elementary subgroup H of G, we impose that $H = C \cdot P \simeq$ with the same notation above with the condition that any element in C and P are commutes. This condition says that for x be the generator of C, $P \leq Z(x)$. By imposing the commutativity, we can identifying internal direct product of C and P with direct product $C \times P$.

Theorem 4. *(Brauer's theorem) Let G be a finite group, and X' be the set of all the elementary subgroups of G. For any virtual character $\chi \in R(G)$, there exists $\eta_H \in R(H)$ for each $H \in X'$ satisfying*

$$\chi = \sum_{H \in X'} \mathrm{Ind}_H^G \eta_H. \tag{14}$$

Remark 5. First remark is that $X \subset X'$: for any cyclic subgroup C, choose an prime p such that the order of C is coprime to p. By writing $C = C \cdot 1$, we know that C is p-elementary subgroup. The second remark is that Brauer's theorem can exactly write any $\chi \in R(G)$ into the sum of the induced virtual characters of elementary subgroups, while Artin's theorem only can say that it can write by the sum of the induced virtual characters of cyclic subgroups with coefficient in $\mathbb{Q}$. This difference comes from that X' have larger collection of the subgroups of G than X.

6 I'll show the following proposition.

Proposition 6. *(Ex. 10.2 in the textbook) Let $G = GL_n(k)$, where k is a finite field of characteristic p. Show that an element $x \in G$ is a p-element if and only if its eigenvalues are all equal to 1, i.e., $1 - x$ is nilpotent; it is a p'-elemen if and only if it is semisimple, i.e., diagonalizable in a finite extension of k.*

Proof. 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. Since the extended field k' have characteristic p, it again have order p^m for some $m \in \mathbb{N}$. By little Fermat's theorem, any non-zero element in the field have order dividing $p^m - 1$, which is coprime to p. Therefore, writing

$$x = V \Lambda V^{-1}, \tag{15}$$

where $V \in GL_n(k')$ and $\Lambda \in GL_n(k')$ 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. $\square$

If x is p-element, $(1 - x)$ is nilpotent by the proposition. Since $(1 - x)$ is irreducible polynomial in $F[x]$, it means that each minimal polynomial and characteristic polynomial are of the form $(1 - x)^m$ for some $m \in \mathbb{N}$, cf. *Abstract Algebra*, Dummit and Foote, proposition 20 in Section 12.2.

Now, let x be p'-element. As in the proof of the proposition, the minimal polynomial of x is separable and divides $x^N - 1$ where $N = |x|$. Since the minimal polynomial divides the characteristic polynomial, and characteristic polynomial of x divides some power of the minimal polynomial,

3

the characteristic polynomial completely splits in the finite splitting field extension of k about the minimal polynomial of x.

Example: for p-element, which is not p'-element, choose

$$A = \begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \dots & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{16}$$

as

$$A^n = \begin{pmatrix} 1 & n & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \dots & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \tag{17}$$

so $|A| = p$.

For p'-element which is not p-element, choose

$$B = \begin{pmatrix} \delta & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \dots & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \tag{18}$$

where $\delta = 2$ if $p > 2$, non-zero and not 1 element in k if $p = 2$, but $k \neq \mathbb{F}_2$, and a root of $x^2 + x + 1$ if $k \simeq \mathbb{F}_2$. For $p > 2$ case, as $|\delta| \mid p - 1$, B is p'-element. For $k \simeq \mathbb{F}_2$, note that $|\delta| = 3$, so it is again p'-element.

7

(a) Using Brauer's theorem, theorem 4, we can write

$$\chi = \sum_{H \in X'} \operatorname{Ind}_H^G \eta_H. \tag{19}$$

For each $H \in X'$, let's write $\eta_H = \sum_{i=1}^{m_H} n_{H,i} \eta_{H,i}$, where $\eta_{H,i}$ are irreducible characters of H and $n_{H,i} \in \mathbb{Z}$. Using the fact that any irreducible character of H, which is supersolvable, are monomials, we know that η_H is the sum of monomial characters with integer coefficients. It shows that χ is the sum of monomial characters with integer coefficients.

(b) 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

$$\chi = \sum_j \sum_i r_{i,j} \operatorname{Ind}_{A_j}^G \chi_{i,j}. \tag{20}$$

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

$$1 = \langle \chi, \chi \rangle = \sum_j \sum_i r_{i,j} \langle \operatorname{Ind}_{A_j}^G \chi_{i,j}, \chi \rangle, \tag{21}$$

and for the other irreducible representations χ' of G,

$$0 = \langle \chi, \chi' \rangle = \sum_j \sum_i r_{i,j} \langle \operatorname{Ind}_{A_j}^G \chi_{i,j}, \chi' \rangle. \tag{22}$$

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

8 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 $H \leq G$, $\operatorname{Res}_H f \in \mathbb{Q} \otimes R(H)$.

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

$$f(x^m) = f(x^{m+k_0|H|}) = f(x). \tag{23}$$

(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 $\chi_k(x) = \exp(2\pi i k/g)$ of G, then

$$\langle f, \chi_k \rangle = \sum_{m=1}^g f(x^m) \exp\left(\frac{-2\pi i k m}{g}\right). \tag{24}$$

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

$$A_q = \{a \in \{1, \ldots, g\} : (a, g) = q\}. \tag{25}$$

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

$$\sum_{m \in A_q} \exp\left(\frac{-2\pi i k m}{g}\right) = \sum_{m \in A_q} \exp\left(\frac{-2\pi i k (m/q)}{g/q}\right) = \sum_{m \in (\mathbb{Z}/(g/q)\mathbb{Z})^\times} \exp\left(\frac{-2\pi i k m}{g/q}\right) \in \mathbb{Z} \tag{26}$$

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 7. *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 $(m, g) = 1$ and $a_1 m \equiv a_2 \mod g$.*

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 $(a_1 m, g) = (a_1, g)(m, g) = (a_2, g)$. $\qquad\qquad\square$

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

$$
\begin{aligned}
\langle f, \chi \rangle &= \frac{1}{g} \sum_{m=1}^{g} f(x^m) \exp\left(\frac{-2\pi i k m}{g}\right) \\
&= \frac{1}{g} \sum_{q=1}^{g} \sum_{m \in A_q} f(x^m) \exp\left(\frac{-2\pi i k m}{g}\right) \\
&= \frac{1}{g} \sum_{q=1}^{g} \sum_{m \in A_q} f(x^q) \exp\left(\frac{-2\pi i k m}{g}\right) \\
&= \frac{1}{g} \sum_{q=1}^{g} f(x^q) \sum_{m \in A_q} \exp\left(\frac{-2\pi i k m}{g}\right) \in \mathbb{Q},
\end{aligned}
\tag{27}
$$

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

In problem 9.3 (b) in the textbook, we showed that Ψ^n maps $R(G)$ to $R(G)$, so extending the scalar to $\mathbb{Q}$ with the map $1 \otimes \Psi^n$, we can treat that Ψ^n maps $\mathbb{Q} \otimes R(G)$ to $\mathbb{Q} \otimes R(G)$ abusing notation. 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 in the textbook. It means that for any irreducible character χ of G,

$$
g/(g, n)\langle \Psi^n f, \chi \rangle \in \mathbb{Q} \cap A = \mathbb{Z}.
\tag{28}
$$

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. $\Psi^n f(s) = 1$ if $|s| \mid n$ and 0 elsewhere. The above result shows that $g/(g, n)1_{\{s:|s|\mid n\}} \in R(G)$, which generalize the result $g\delta_{s=1} \in R(G)$ for regular representation with $n = 1$ case and $1_G \in R(G)$ for $n = g$ case.

9 In the problem 3.3 in the textbook, we already shows that there exists the canonical isomorphism φ between G and $\hat{\hat{G}}$ by mapping $\varphi(s)(\chi) = \chi(s)$ for irreducible representation χ of G. For $\sum_{s \in G} n_s s \in \mathbb{Z}[G]$, let's define $\bar{\varphi}$ by

$$
\bar{\varphi}\left(\sum_{s \in G} n_s s\right) := \sum_{s \in G} n_s \varphi(s).
\tag{29}
$$

This is a ring isomorphism $\bar{\varphi}$ between $\mathbb{Z}[G]$ and $R(\hat{G})$: it preserves addition, multiplication as

$$
\bar{\varphi}\left(\left(\sum_{s \in G} n_s s\right)\left(\sum_{s' \in G} n'_{s'} s'\right)\right) = \sum_{s \in G} \sum_{s' \in G} n_s n'_{s'} \varphi(s s') = \bar{\varphi}\left(\sum_{s \in G} n_s s\right) \bar{\varphi}\left(\sum_{s' \in G} n'_{s'} s'\right),
\tag{30}
$$

and identity since

$$
\bar{\varphi}(1)(\chi) = \chi(1) = 1,
\tag{31}
$$

so $\bar{\varphi}(1) = 1_{\hat{G}}$.

Secondary, I'll show that $A \otimes_{\mathbb{Z}} \mathbb{Z}[G] \simeq A[G]$. Consider the following universal property diagram

$$A \times \mathbb{Z}[G] \xrightarrow{\ i\ } A \otimes \mathbb{Z}[G]$$
$$\varphi \searrow \quad \downarrow \Phi$$
$$A[G]$$

by setting

$$\varphi : (a, \sum_{s \in G} n_s s) \mapsto \sum_{s \in G} a n_s s. \tag{32}$$

As φ is a $\mathbb{Z}$ bilinear map, it indues well-defined $\mathbb{Z}$-module homomorphism Φ. As φ is surjective, Φ is surjective. Finally, it is injective: any element in $A \otimes \mathbb{Z}[G]$ can be simplified by the form

$$\sum_{s \in G} a_s \otimes s \tag{33}$$

by sending the coefficient of $\mathbb{Z}[G]$ part to A. Since $\Phi : \sum_{s \in G} a_s \otimes s \mapsto \sum_{s \in G} a_s s$, if two element in $A \otimes \mathbb{Z}[G]$ maps to the same element in $A[G]$, it means two element are in fact same in $A \otimes \mathbb{Z}[G]$. Therefore, Φ is $\mathbb{Z}$-module isomorphism.

Since A and $\mathbb{Z}[G]$ are $\mathbb{Z}$-algebras, $A \otimes \mathbb{Z}[G]$ have $\mathbb{Z}$-algebra structure. Furthermore, the multiplication structure of two $\mathbb{Z}$-algebras are same. It shows that $A \otimes \mathbb{Z}[G]$ and $A[G]$ are in fact $\mathbb{Z}$-algebra isomorphism.

Now, let's again define $\bar{\bar{\varphi}}$ by $1 \otimes \bar{\varphi}$ between $A \otimes \mathbb{Z}[G] \simeq A[G]$ and $A \otimes R(\hat{G})$: as $\mathbb{Z}[G]$ and $R(\hat{G})$ are ring isomorphic, by the elementary property of the tensor product, both are again ring isomorphic. Abusing notation, let's write the final isomorphism φ. Since it is a ring isomorphism, it is enough to determine $\mathrm{Spec}(A \otimes R(\hat{G}))$ to check $\mathrm{Spec}(A[G])$.

Now, I prove a proposition.

Proposition 8. *Let G be a finite abelian group with primary cyclic group decomposition*

$$G \simeq \mathbb{Z}/q_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/q_t\mathbb{Z}, \tag{34}$$

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

$$\hat{G} \simeq \mathbb{Z}/q_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/q_t\mathbb{Z}. \tag{35}$$

(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 $\mathbb{Z}/q_i\mathbb{Z}$,

$$\chi_k^i(x_i^m) = \exp\left(\frac{2\pi i k m}{q_i}\right). \tag{36}$$

Extend this character to G by setting

$$\chi_k^i(x_j) = 1 \tag{37}$$

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,

$$(\chi_1^i)^k(x_i) = \left(\exp\left(\frac{2\pi i}{q_i}\right)\right)^k = \chi_k^i(x_i), \tag{38}$$

7

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 $C_iC_j = C_jC_i$ 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

$$\oplus_{i=1}^t \mathbb{Z}/q_i\mathbb{Z} \simeq \oplus_{i=1}^t C_i = \hat{G} \tag{39}$$

$\square$

Using this group isomorphism, we can extend it to group ring isomorphism between $R(G)$ and $R(\hat{G})$. Also, 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 by applying tensor product on the exact sequence

$$0 \rightarrow R(G) \rightarrow R(\hat{G}) \rightarrow 0. \tag{40}$$

Let the final ring isomorphism $\psi : A[G] \rightarrow A \otimes R(G)$. Since we already know what is the prime ideals in $A \otimes R(G)$ in the class, by pulling back the prime ideals using ψ, we get $\mathrm{Spec}(A[G])$.

10 (I'll write in Korean.) 여러 수학 과목을 들으면서 느낀 점이 있다면 예전에 많은 이들이 해 놓아서 잘 정립된 분야를 공부할 때 보통 non-trivial한 property들이 중심을 꽉 잡고 있고, 그 외의 정리들은 그 non-trivial한 property들의 따름 정리로써 따라온다고 생각합니다. 저 같은 경우 이 과목을 들으면서 non-trivial하다고 느낀 성질들이 1. character를 보면 representation을 classification할 수 있다. 와 2. Artin and Brauer's theorem이라고 생각합니다. Tool로써 tricky 하다고 생각하는 것은 Frobenius reciprocity formula와 (이름은 모르겠지만)

$$\mathrm{Ind}(\psi \cdot \mathrm{Res}\,\varphi) = (\mathrm{Ind}\,\psi) \cdot \varphi \tag{41}$$

라고 생각합니다. The most favorite을 하나 고르라고 하셨으니 이 중에서 하나를 고르면 (41)를 고를 것 같습니다. 다른 tool들이나 증명에서 사용하는 것들은 뭔가 열심히 생각하면 그래도 어떻게든 생각해낼 수 있겠다 생각은 들지만 저 tool은 뭔가 안 될 것 같은 statement를 풀어낼 때 약방의 감초와 같은 역할로 들어가기 때문입니다. 예를 들어 저를 아주 골치아프게 하였 던 Exercise 10.6과 같은 문제를 풀 때 저 식이 얼마나 강력하고 직관과 어긋나는지를 배울 수 있었습니다. 사실 식을 봐도 말이 안 된다고 생각하는 것이, Ind를 취하면 normal subgroup에 대해서 취하는 게 아닌 이상 보통 character가 배배 꼬일 것이라고 예상을 하지만, Res 붙인 것 하나를 free pass하듯이 그대로 끌고 나오기 때문입니다. 저 식 때문에 문제 풀면서 머리도 많이 아팠지만 그 만큼 과목을 재밌게 들을 수 있었기 때문에 The most favorite one in this class로 저 식을 고르겠습니다.

3 I'll assume the fact from the exercise 9.2 and 9.3 (b) in the textbook. I could put it in this paper, but it will make this solution too long. (In fact, this solution is from my homework for 9.4)

(a) I'll first show a proposition.

Proposition 9. *Let's define $\varphi : G \rightarrow G$ 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 10. *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 $c_1' = \operatorname{Im}\varphi(c_1)$, 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 $s \in G$, $\varphi(ss_1 s^{-1}) = ss_1^n s^{-1}$, 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. $\qquad\square$

Corollary 11. *Let $\{c_1, \ldots, c_h\}$ be the set of conjugacy classes in G. Let's define*

$$\Phi : \{c_1, \ldots, c_h\} \to \{c_1, \ldots, c_h\} \tag{42}$$

by $\Phi(c_i) = \operatorname{Im}\varphi(c_i)$. 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. $\qquad\square$

Using the proposition, we get

$$\langle \Psi^n(\chi), \Psi^n(\chi) \rangle = \frac{1}{g}\sum_{s \in G} \chi(s^n)\chi(s^{-n}) = \frac{1}{g}\sum_{s \in G}\chi(s)\chi(s^{-1}) = \langle \chi, \chi \rangle = 1. \tag{43}$$

Also, $\Psi^n(\chi)(1) = \chi(1) > 0$. By the problem 9.2, we know that $\Psi^n\chi$ 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 12. *For two conjugacy classes c_1, c_2 in G, we get*

$$\sum_{s \in c_1}\sum_{s' \in c_2} s^n (s')^n = \sum_{s \in c_1}\sum_{s' \in c_2}(ss')^n. \tag{44}$$

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 $\sum_{s \in G} u(s)s \in \operatorname{Cent}.\mathbb{C}[G]$ to $\mathbb{C}$ by

$$\omega_i\left(\sum_{s \in G} u(s)s\right) = \frac{1}{n_i}\sum_{s \in G} u(s)\chi_i(s), \tag{45}$$

where χ_i is the irreducible character corresponding to ω_i and $n_i = \deg\chi_i$. (For detailed explanation, see Chapter 6.3 in the textbook.) 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

$$\omega_i\left(\sum_{s \in c_1}\sum_{s' \in c_2} s^n (s')^n\right) = \omega_i\left(\sum_{s \in c_1}\sum_{s' \in c_2}(ss')^n\right). \tag{46}$$

for all i.

Now, let's use corollary 10. Let's set $c'_1 = \mathrm{Im}\,\varphi(c_1)$ and $c'_2 = \mathrm{Im}\,\varphi(c_2)$, then we get

$$
\begin{aligned}
\sum_{s\in c_1} s^n &= \sum_{s\in c'_1} s \\
\sum_{s'\in c_2} (s')^n &= \sum_{s'\in c'_2} s',
\end{aligned}
\tag{47}
$$

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

$$
\begin{aligned}
\omega_i\left(\sum_{s\in c_1}\sum_{s'\in c_2} s^n(s')^n\right) &= \omega_i\left(\left(\sum_{s\in c_1} s^n\right)\left(\sum_{s'\in c_2}(s')^n\right)\right) \\
&= \omega_i\left(\sum_{s\in c_1} s^n\right)\omega_i\left(\sum_{s'\in c_2}(s')^n\right) \\
&= \frac{1}{n_i^2}\sum_{s\in c_1}\Psi^n\chi_i(s)\sum_{s'\in c_2}\Psi^n\chi_i(s').
\end{aligned}
\tag{48}
$$

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

$$
\begin{aligned}
\omega_i\left(\sum_{s\in c_1}\sum_{s'\in c_2} s^n(s')^n\right) &= \frac{1}{n_i^2}\sum_{s\in c_1}\Psi^n\chi_i(s)\sum_{s'\in c_2}\Psi^n\chi_i(s') \\
&= \frac{1}{n_j^2}\sum_{s\in c_1}\chi_j(s)\sum_{s'\in c_2}\chi_j(s') \\
&= \omega_j\left(\sum_{s\in c_1} s\right)\omega_j\left(\sum_{s'\in c_2} s'\right) \\
&= \omega_j\left(\sum_{s\in c_1}\sum_{s'\in c_2} ss'\right).
\end{aligned}
\tag{49}
$$

Also,

$$
\begin{aligned}
\omega_i\left(\sum_{s\in c_1}\sum_{s'\in c_2}(ss')^n.\right) &= \frac{1}{n_i}\sum_{s\in c_1, s'\in c_2}\Psi^n\chi_i(ss') \\
&= \frac{1}{n_j}\sum_{s\in c_1, s'\in c_2}\chi_j(ss') \\
&= \omega_j\left(\sum_{s\in c_1, s'\in c_2} ss'\right).
\end{aligned}
\tag{50}
$$

Therefore, (46) 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

$$
\psi_n(e_{c_1})\psi_n(e_{c_2}) = \psi_n(e_{c_1}e_{c_2})
\tag{51}
$$

for any conjugacy classes c_1 and c_2 in G. By the corollary 11, we know that $\mathrm{Im}\,\psi_n$ 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 $\mathbb{C}[G]$.