HW11

박성빈, 수학과, 20202120

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

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

Theorem 2. *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 3. *Let $f : A \to B$ be a ring homomorphism, then it induces the continuous map $f^* :$ $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ by $f^*(p_B) = f^{-1}(p_B)$ for $p_B \in \mathrm{Spec}(B)$. 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 4. $\mathrm{Spec}(A)$ *is irreducible if and only if the nilradical of A is prime ideal.*

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

Remark 5. If the nilradical of A is prime ideal, then $\mathrm{Spec}(A)$ is connected since there is no disjoint open set. It proves that "$\mathrm{Spec}(A)$ 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

$$\mathbb{Z} \xrightarrow{i_1} A \xrightarrow{i_2} A \otimes_{\mathbb{Z}} R(G) \xrightarrow{i_3} A^{\mathrm{Cl}(G)}, \tag{1}$$

where

$$\begin{aligned}
A &:= \oplus_{j=0}^{g-1} \mathbb{Z}\mu^j \\
i_2(a) &= a \otimes 1_G \;\; \text{and} \\
i_3(a \otimes f) &= af,
\end{aligned} \tag{2}$$

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

$$\mathrm{Spec}(A^{\mathrm{Cl}(G)}) \xrightarrow{i_3^*} \mathrm{Spec}(A \otimes_{\mathbb{Z}} R(G)) \xrightarrow{i_2^*} \mathrm{Spec}(A) \xrightarrow{i_1^*} \mathrm{Spec}(\mathbb{Z}) \tag{3}$$

by the theorem 3.

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

Proposition 6. *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 3. Therefore, i_1 induces the map

$$\mathbb{Z}/(i_1^{-1}(M)) \xrightarrow{\bar{i}_1} A/M. \tag{4}$$

Note that this map is injective field homomorphism. Considering $\bar{i}_1$ as a $\mathbb{Z}$-module homomorphism, we get $\mathrm{char}(A/M) = p$. 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. $\qquad\square$

Proposition 7. *$A^{\mathrm{Cl}(G)}$ is integral over $\mathbb{Z}$. It implies that $A \otimes R(G)$ is integral over $\mathbb{Z}$.*

Proof. Choose $a = (a_1, \ldots, a_h) \in A^{\mathrm{Cl}(G)}$. 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 $A^{\mathrm{Cl}(G)}$, it is

$$p_i((a_1, \ldots, a_h)) = (p_i(a_1), \ldots, p_i(a_h)), \tag{5}$$

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 $A^{\mathrm{Cl}(G)}$, it is integral over $\mathbb{Z}$. $\qquad\square$

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

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

where i is the inclusion map and

$$f : (b, \chi) \mapsto b(\varphi \circ \chi), \tag{6}$$

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 8. *$B^{\mathrm{Cl}(G)}$ 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 7, 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. $\qquad\square$

Proposition 9. *Ex. 10.4 (Discussed with Jeong Dasol.)*

Proof. 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

$$\mathrm{Res}_H \xi = \sum_{i,j} a_{ij} \chi_i \eta_j. \tag{7}$$

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

$$
\begin{aligned}
\xi(x)^q = (\mathrm{Res}_H \xi(x))^q &= \left(\sum_{i,j} a_{ij} \chi_i(x_r) \eta_j(x_u) \right)^{p_n} \equiv \sum_{i,j} a_{ij}^{p_n} \chi_i(x_r^{p_n}) \eta_j(1) \\
&\equiv \sum_{i,j} a_{ij}^{p_n} \chi_i(x_r^{p_n}) \equiv \xi(x_r)^q \quad \mathrm{mod}\ M.
\end{aligned}
\tag{8}
$$

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

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

1(S 11.2) Let's take quotient on (1). Note that non-zero prime ideals in each ring is maximal by the theorem 1. 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

$$\mathbb{Z}/(i_1^{-1}(M)) \xrightarrow{\bar{i}_1} A/M \xrightarrow{\bar{i}_2} (A \otimes_{\mathbb{Z}} R(G))/P_{M,c} \xrightarrow{\bar{i}_3} A^{\mathrm{Cl}(G)}/M_c. \tag{9}$$

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

$$\bar{i}_3 \circ \bar{i}_2([a_c]) = [(a_c, a_c, \ldots, a_c)] = [(a_1, \ldots, a_h)]. \tag{10}$$

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

2(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

$$\mathbb{Z} \xrightarrow{i_1} A \xrightarrow{\varphi} B \xrightarrow{i_2} B \otimes_{\mathbb{Z}} R(G) \xrightarrow{i_3} B^{\mathrm{Cl}(G)}, \tag{11}$$

where $\varphi : A \to B$ is the ring homomorphism into the center of B with $1_A \mapsto 1_B$. By theorem 3, we know that the above sequence induces

$$\mathrm{Spec}(B^{\mathrm{Cl}(G)}) \xrightarrow{i_3^*} \mathrm{Spec}(B \otimes_{\mathbb{Z}} R(G)) \xrightarrow{i_2^*} \mathrm{Spec}(B) \xrightarrow{\varphi^*} \mathrm{Spec}(A) \xrightarrow{i_1^*} \mathrm{Spec}(\mathbb{Z}). \tag{12}$$

Also, by the corollary 8, 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.

3

Proposition 10. *Let M be a prime ideal in B and consider an integral domain B/M. Set $N =$ 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.) $\quad\square$

3(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 3, 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 11. *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,

$$p(x_1) = i^{-1}(x_1) = i^{-1}\left(\cap_{\sigma \in G}\sigma(x_1)\right) = i^{-1}(x_2) = p(x_2). \tag{13}$$

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

$$\prod_{\sigma \in G} \sigma(a) \in p(x_1) = p(x_2) \subset x_2, \tag{14}$$

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

$$x_1 \subset \cup_{\sigma \in G}\sigma(x_2). \tag{15}$$

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

$$\sigma_k \left(\sum_{i=1}^{h} a_i \otimes \chi_i \right) = \sum_{i=1}^{h} \sigma_k(a_i) \otimes \chi_i \tag{16}$$

where χ_i are the irreducible characters of G.

Using the above proposition, we know that $i^*(x_1) = i^*(x_2)$ for $x_1, x_2 \in \operatorname{Spec}(A \otimes R(G))$ if and only if there exists $\sigma \in \operatorname{Gal}(\mathbb{Q}(\mu_g)/\mathbb{Q})$ 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".

4(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 $\operatorname{Spec}(A \otimes R(\hat{G}))$ to check $\operatorname{Spec}(A[G])$.

Now, I prove a proposition.

Proposition 12. *Let G be a finite abelian group with primary cyclic group decomposition*

$$G \simeq \mathbb{Z}/q_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/q_t\mathbb{Z}, \tag{17}$$

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

$$\hat{G} \simeq \mathbb{Z}/q_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/q_t\mathbb{Z}. \tag{18}$$

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

$$\chi_k^i(x_i^m) = \exp\left(\frac{2\pi i k m}{q_i}\right). \tag{19}$$

Extend this character to G by setting

$$\chi_k^i(x_j) = 1 \tag{20}$$

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,

$$(\chi_1^i)^k(x_i) = \left(\exp\left(\frac{2\pi i}{q_i}\right)\right)^k = \chi_k^i(x_i), \tag{21}$$

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

$$\oplus_{i=1}^t \mathbb{Z}/q_i\mathbb{Z} \simeq \oplus_{i=1}^t C_i = \hat{G} \tag{22}$$

$$\square$$

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

$$0 \to R(G) \to R(\hat{G}) \to 0. \tag{23}$$

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 $\text{Spec}(A[G])$.

5(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

$$f = \sum_{i=0}^{3} a_j \chi_j, \tag{24}$$

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

$$
\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 2+i \\ 4-i \\ 6-i \end{pmatrix}. \tag{25}
$$

The solution is

$$
(a_0, a_1, a_2, a_3) = \left(-\frac{1}{4} + \frac{5i}{4}, -\frac{3}{4} - \frac{i}{4}, -\frac{5}{4} - \frac{3i}{4}, \frac{13}{4} - \frac{i}{4} \right) \notin A^4. \tag{26}
$$

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 $x \in c$,

$$
\mathrm{Ind}_H^G f(x) = \sum_{\substack{s \in G \\ sxs^{-1} \in H}} f(sxs^{-1}) = 0, \tag{27}
$$

so $f \in P_{0,c}$ and $\mathrm{Im}(A \otimes \mathrm{Ind}_H^G) \subset P_{0,c}$. 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 $h 1_{c'} \in A \otimes R(H)$. Since

$$
h \, \mathrm{Ind}_H^G 1_{c'}(x) = \sum_{\substack{s \in G \\ sxs^{-1} \in c'}} 1_{c'}(sxs^{-1}) > 0, \tag{28}
$$

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

(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 $\mathrm{Im} f \subset A$. Therefore, by the lemma 11, we know that $\mathrm{Ind}_H^G f(c) \in pA$, 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 $f' = \mathrm{Ind}_H^G f$ 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 13. *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

$$l1_G = \sum_{H \in Y} \operatorname{Ind}_H^G \chi_H. \tag{29}$$

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,

$$l1_G = \sum_{H \in Y} \operatorname{Ind}_H^G \chi_H = \sum_{H \in Y} \operatorname{Ind}_{P_H}^G \left(\operatorname{Ind}_H^{P_H} \chi_H \right), \tag{30}$$

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

Theorem 14. *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 $\operatorname{Ind}_H^G r_H = r_G$, 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. $\qquad\square$