國立臺灣大學理學院數學系

碩士論文

Department of Mathematics
College of Science
National Taiwan University
Master Thesis

表現理論初探

A Glimpse of Representation Theory

許乃珩
Nai-Heng Sheu

指導教授：余家富 博士
Advisor: Chia-Fu Yu, Ph.D.

中華民國 107 年 1 月
January, 2018

doi:10.6342/NTU201800167

致謝

感謝余家富老師，溫和且有耐心的指導，同時給予了很多數學上的幫助，並爲了此篇論文的完整性而撰寫了第五章，以及對於論文內容給了很多洞見，有老師的幫忙，我才能夠完成這篇論文。感謝康明昌老師、謝銘倫老師以及林惠雯老師，撥時間來當口試委員，並給予珍貴的建議。感謝郭家瑋學長，常常讓我問問題。感謝系上的同學陳奎佑、黃子豪及王國鑫的幫忙，讓脫線的我足以使口試順利進行。感謝台大數學系和那架鋼琴給予了舒適且自由的環境，讓人待在裡面感到舒服自在。也感謝系上的同學，認眞且開放的討論風氣讓人收穫良多。感謝玩味咖啡的美味餐點及飲料，讓一天的開始是如此的令人期待。最後感謝賴奕甫給予的陪伴與各種支持。

doi:10.6342/NTU201800167

摘要

在這篇論文中，我們趁著這次機會整理了一些關於有限群表現理論基本而重要的結果，例如：判定給定的群他的不可分解 (indecomposable) 表現及不可分解的整數表現 (integral representations)，是否只有有限多種。因爲分裂的代數圓圈 (split algebraic tori) 會與有限群的整數表現產生對應，所以在此論文的最後一章，我們也介紹了代數圓圈的可分離分裂體 (separable splitting fields) 定理。在第二章中，我們探討模表現 (modular representations)，尤其是體 (field) 的特徵值 (characteristic) 整除群的元素總個數時。我們介紹了格林對應 (Green's correspondence)，在格林對應之後，我們有了相對投射性 (relative projectivity) 的概念，進而能夠判斷給定的群的不可分解的表現是否有無限多種，同時在模系統 (modular system) 下我們介紹了格羅滕迪克群 (Grothendieck group) 及 cde 三角形。第三章簡單的介紹了整數表現理論以及判斷不可分解的整數表現的有限性的方式。在第四章，我們整理了一些特定有限群的不可分解整數表現，例如元素個數爲質數 p 的循環群，以及元素個數爲 2p 的二面體群。在最後一章，我們整理了很多代數圓圈會在他的有限可分離體擴張 (finite separable field extension) 分裂的不同證明，並且推廣了 Chow 的定理，最後則是給了對於一個代數圓圈，他的分裂體的上限。

關鍵字：模表現、整數表現、有限表現類型、代數圓圈、分裂體

doi:10.6342/NTU201800167

Abstract

In the present thesis, we take the opportunity to discuss several basic and important results in representation theory. More precisely we mainly investigate the criterion of finite groups G that are of finite representation type for both kG-modules or for $\mathbb{Z}G$-lattices, as well as separable splitting fields of algebraic tori.

In Chapter 2, we consider the theory of representations of finite groups over a field k. We focus mainly on the case where the characteristic of k divides the order of the group G. This chapter include Green's correspondence and its the connection to the criterion of kG that is of finite representation. We also discuss the structure and relation of Grothendieck groups R_kG and R_KG in a modular system setting, namely the cde triangle.

In Chapter 3, we give an overview of integral representations based on classical results of Heller and Reiner, which would be useful for further studies. In Chapter 4, we give a description of classification of indecomposable integral representations of cyclic groups of prime order p and dihedral groups of order $2p$, based on works of Reiner and of Lee.

In the last chapter, we give a connection between algebraic tori and integral representations of finite groups. We give several different proofs of the theorem that any algebraic tori over a field splits over a finite field extension. Besides, we also generalize Chow's theorem to semi-abelian varieties, and give a sharp bound for the splitting fields of algebraic tori.

Keywords: modular representations, integral representations, finite representation type, algebraic tori, splitting fields

doi:10.6342/NTU201800167

Contents

doi:10.6342/NTU201800167

doi:10.6342/NTU201800167

List of Tables

doi:10.6342/NTU201800167

Chapter 1

Introduction

This paper is the author's attempt to organize some well-known and important results in representation theory. It includes topics on representations of finite groups over fields of characteristic $p \neq 0$, integral representations of finite groups, as well as some results on algebraic tori which are connected to integral representations.

In Chapter 2, we deal with representations of finite groups over a field k of characteristic $p \neq 0$. The content of this chapter is mainly followed from [36] and [43]. We exhibit some notions and general results concerning kG-modules. For example, we discuss Green's correspondence, numbers of irreducible representations up to isomorphism, properties of projective covers, the cde triangle, and a criteria of groups that are of finite representation type. We include the adorable construction in [43] of infinitely many indecomposable non-isomorphic representations of the group $C_p \times C_p$. Based on general results we learned, we make a detailed study on indecomposable representations of the symmetric group S_3. This finite group S_3 will also appear as an example in successive chapters.

In the next two chapters, we introduce integral representations of finite groups. Chapter 3 concerns mainly the finiteness criteria for finite groups. For definitions and basic theorems, we follow mainly the exposition of Curtis and Reiner [10]. Then we are de-

doi:10.6342/NTU201800167

voted to discussing results toward the main theorems of Heller and Reiner ([17] and [18]) on a criterion of G which is of finite representation type. Chapter 4 deals with the classification problem of indecomposable integral representations of special finite groups, namely $G = C_p$ a cyclic group of prime order p, and $G = D_p$ a dihedral group of order $2p$. The examples in this chapter illustrate an interesting connection between integral representations and algebraic number theory.

The last chapter, Chapter 5, deals with separable splitting fields of algebraic tori. We explain how integral representations of finite groups are related to classification of algebraic tori. This is based on a well-known theorem that any algebraic torus splits over a finite separable field extension. The main part of this chapter provides several different proofs of this well-known theorem from different points of view. We also establish Chow's theorem for semi-abelian varieties and give a sharp bound for the degrees of the splitting fields. The latter uses a classical theorem of Chevalley on invariants of finite reflection groups, results on finite subgroups of $GL_d(\mathbb{Q})$ and Hilbert's irreducibility.

doi:10.6342/NTU201800167

Chapter 2

The group ring kG

In this chapter, our group G is a finite group. Let A be a complete discrete valuation ring with quotient field K. Assume that K is of characteristic 0 and the residue field k is of characteristic $p > 0$. Assume that k sufficiently large i.e. k contains a $|G|$-th root of unity. Let kG denote the group ring of G over k. All kG-modules M considered are finitely generated, unless specifically stated otherwise.

The ring structure of the group ring kG and its representations are known when char $k \nmid |G|$ and k is sufficiently large. In the following, we shall focus on the situation where char $k = p \mid |G|$. We try to understand kG in three ways: studying indecomposable kG-modules through Green's correspondence, the (modular) character theory and ring structure of kG itself.

We will first introduce relative projectiveness, vertices and sources. Using these notions, we can describe Green's Correspondence, and obtain information on the number of isomorphism classes of indecomposable kG-modules under suitable conditions of G. Later, we will give an example of G for which there are infinitely many isomorphism classes indecomposable kG-modules. After that, we will give a criterion for G that there are only finitely many indecomposable kG-modules up to isomorphism, i.e. kG is of finite representation type.

doi:10.6342/NTU201800167

For the second approach, we exhibit some general results like the cde triangle, projective covers, numbers of irreducible representations over k.

At the end, we use results we have discussed about, and obtain more explicit information in the case $G = S_3$ and $p = 2$ or 3.

2.1 Green's correspondence

For the moment, let k be a field of any arbitrary field. Suppose U is a kG-module, H a subgroup of G and V is a kH-module. In the following, let $V \uparrow_H^G$ denote the induced representation of V from H to G. Let $U \downarrow_H^G$ denote the restriction of U to kH-module. If U' is a direct summand of U, then we write $U' \mid U$.

We first state different definitions of H-projectiveness. These three definitions are actually equivalent by [43] Corollary 11.3.4.

Definition 1. A kG-module U is said to be *H-projective* if U is a direct summand of $T \uparrow_H^G$ for some kH-module T.

Definition 2. We say a kG-module U *H-projective* if for a given exact sequence $0 \xrightarrow{f} E_1 \xrightarrow{g} E_2 \to U \to 0$ of kG-modules, it splits if and only if it splits as kH-modules.

Definition 3. We say a kG-module U *H-projective* if $U | U \downarrow_H^G \uparrow_H^G$.

Example 4. Every kG-module U is G-projective.

Example 5. Since every projective kG-module is a direct summand of $(kG)^n$, a kG-module P is projective if and only if it is 1_G-projective.

Proposition 6. *Suppose U is a Q-projective kG-module with Q a minimal subgroup satisfying this condition. Then this minimal subgroup Q is unique up to conjugacy.*

Proof. Suppose there exists a minimal subgroup Q' of G such that U is Q'-projective. Since U is both Q- and Q'-projective, we have $U | U \downarrow_Q^G \uparrow_Q^G \downarrow_{Q'}^G \uparrow_{Q'}^G$. From Mackay's formula (ref. [36] Proposition 22),

$$U \downarrow^G_Q \uparrow^G_Q \downarrow^G_{Q'} \uparrow^G_{Q'} = (U \downarrow^G_Q \uparrow^G_Q \downarrow^G_{Q'}) \uparrow^G_{Q'} = \Big(\bigoplus_{s\in Q'\backslash G/Q} ((U \downarrow^G_Q)_s \downarrow^{{}^sQ}_{{}^sQ\cap Q'}) \uparrow^{Q'}_{{}^sQ\cap Q'}\Big) \uparrow^G_{Q'}$$

$$= \bigoplus_{s\in Q'\backslash G/Q} ((U \downarrow^G_Q)_s \downarrow^{{}^sQ}_{{}^sQ\cap Q'}) \uparrow^G_{{}^sQ\cap Q'}, \text{ where } {}^sQ = sQs^{-1}$$

Since U is indecomposable, U must be a direct summand of $((U \downarrow^G_Q)_s \downarrow^{{}^sQ}_{{}^sQ\cap Q'}) \uparrow^G_{{}^sQ\cap Q'}$ for some s. Since Q' is minimal, we have ${}^sQ \cap Q' = Q'$. This means that Q' is conjugate to a subgroup of Q. Similarly, Q is conjugate to a subgroup of Q'. Hence Q is conjugate to Q'

Definition 7. Let U be a kG-module, and Q a subgroup of G as in Proposition 6. We say Q is a *vertex* of U.

Proposition 8. *Suppose H is a subgroup of G such that $|G/H|$ is invertible in k. Then every kG-module M is H-projective.*

Proof. See [43] Proposition 11.3.5.

Corollary 9. *Suppose U is an indecomposable kG-module, $\operatorname{char} k = p$, with a vertex Q. This Q must be a p-subgroup of G.*

Proof. Let H be a Sylow p-subgroup P of G, then by Proposition 8, M is P-projective. Hence a vertex of M is a p-group.

Proposition 10. *Let U be an indecomposable kG-module. Suppose U has a vertex Q, and one has $U|T \uparrow^G_Q$ for some kQ-module T. If we choose such kQ-module T indecomposable, then T is unique up to conjugacy by an element belongs to $N_G(Q)$.*

Proof. At first, we choose our T specifically. Observe that since $U|U \downarrow^G_Q \uparrow^G_Q$ and U is indecomposable, we can choose some indecomposable kQ-module T with $T|U \downarrow^G_Q$ such that $U|T\uparrow_Q^G$. Now suppose there exists an indecomposable kQ-module T' such that $U|T'\uparrow_Q^G$. Since $U|T\uparrow_Q^G$, we have

$$T|U\downarrow_Q^G|T'\uparrow_Q^G\downarrow_Q^G, \text{ and } T'\uparrow_Q^G\downarrow_Q^G=\bigoplus_{s\in Q\backslash G/Q}(T'\downarrow^Q_{{}^sQ\cap Q})_s\uparrow^Q_{{}^sQ\cap Q}.$$

Hence $T|(T'\downarrow^Q_{{}^{s'}Q\cap Q})_{s'}\uparrow^Q_{{}^{s'}Q\cap Q})$ for some s'. Since Q is a vertex, it is minimal. Therefore, ${}^{s'}Q=Q$. We must have $s'\in N_G(Q)$.

Definition 11. Let Q,T,U be as in Proposition 10, we say T is a *source* of U.

The following proposition is not directly related to the content of this section. However, this property looks similar to Definition 3, and will be used later.

Proposition 12. *For any kH-module V, we have $V|V\uparrow_H^G\downarrow_H^G$.*

Proof. From Mackay's formula, we have

$$V\uparrow_H^G\downarrow_H^G=\bigoplus_{s\in H\backslash G/H}(V\downarrow^H_{{}^sH\cap H})_s\uparrow^H_{{}^sH\cap H}.$$

When $s\in[e]$, we have $V=(V\downarrow^H_{{}^sH\cap H})_s\uparrow^H_{{}^sH\cap H}$. Therefore, $V|V\uparrow_H^G\downarrow_H^G$.

Theorem 13 (Krull-Schmidt-Azumaya)**.** *Let R be a complete discrete valuation ring or a field. If Λ is an R-algebra and finitely generated as R-module, then every finitely generated Λ-module M can be written as $\bigoplus_{i=1}^n M_i$ with M_i indecomposable R-modules, and the set counting with the multiplicity $\{M_i\}$ is uniquely determined by M.*

Proof. See [10] Theorem 6.12.

Theorem 14 (Green's Correspondence)**.** *Let k be a field of characteristic p. Let Q be a p-subgroup of G and L a subgroup of G containing the normalizer of Q in G.*

(1). Suppose U is an indecomposable kG-module with vertex Q, then there exists a unique indecomposable kL-module $f(U)$ with vertex Q, such that $f(U)|U\downarrow_L^G$. Also if $X|U\downarrow_L^G$ and $X\ncong f(U)$, then X is H-projective, for some $H={}^xQ\cap L$ and $x\in G\setminus L$.

(2). Suppose V is an indecomposable kL-module with vertex Q, then there exists a unique indecomposable kG-module $g(V)$ with vertex Q, such that $g(V)|V \uparrow_L^G$.And if $Y|V \uparrow_L^G$ and$Y \ncong g(V)$, then Y is H-projective for some $H = {}^yQ \cap Q$, and $y \in G \setminus L$.

(3). Moreover, we have $gf(U) \cong U$, and $fg(V) \cong V$.

Proof. Step 0 : At first, suppose H is the subgroup in (2), then $|H|$ is strictly smaller than $|Q|$. This is because if $|H|$ is equals to $|Q|$, we have $H = {}^yQ \cap Q = Q$ for some $y \in G \setminus L$. Therefore, we have $y \in N_G(Q) \subset L$, which can not happen. Also, the subgroup H in (1) can not be conjugate to Q under L. If so, we have ${}^yQ \cap L = {}^xQ$ for some $x \in L$. Consequently, ${}^{yx^{-1}}Q$ equals to Q, hence $yx^{-1} \in N_G(Q)$. Therefore, y belongs to $xN_G(Q) \subset L$, and we get a contradiction.

Now we prove (2) first.

Step 1 : Suppose V has source T, then we write $T \uparrow_Q^L = V \oplus Z$. By Proposition 12, we have

$$V \uparrow_L^G \downarrow_L^G = V \oplus V', Z \uparrow_L^G \downarrow_L^G = Z \oplus Z'.$$

Now, we look at T more carefully to understand V. We have

$$T \uparrow_Q^G \downarrow_L^G = \bigoplus_{s \in L \backslash G/Q} T_s \downarrow^{sQ}_{L \cap {}^sQ} \uparrow^L_{{}^sL \cap Q} = V \oplus V' \oplus Z \oplus Z'.$$

Since V has a vertex Q, we have

$$V \oplus Z = T \uparrow_Q^L = T_s \downarrow^{sQ}_{L \cap {}^sQ} \uparrow^L_{{}^sL \cap Q}, \ s \in L.$$

For indecomposable summands of V', Z', they must be ${}^sL \cap Q$-projective, $s \notin L$. However, $L \cap {}^sQ$ is not conjugate to Q under L by the first paragraph. Hence $V \uparrow_L^G \downarrow_L^G$ has the unique summand V with vertex Q.

Step 2 : (Existence) Now consider $V \uparrow_L^G$, write $V \uparrow_L^G$ as direct sum of indecomposable

kG-modules. We can pick an indecomposable one, say U, such that $U\downarrow_L^G$ contains V and such U must have a vertex Q. We have that U is Q-projective. Suppose it has a vertex Q' proper subgroup of Q and a source T'. $V|U\downarrow_L^G|T'\uparrow_{Q'}^G\downarrow_L^G$, similar to step 1, V must has a vertex strictly smaller than Q, contradiction to the minimality of the vertex Q.

Step 3 : (Uniqueness) Suppose $U'|V\uparrow_L^G$, and U' has a vertex $Q' < Q < L$. Since $U'|U'\downarrow_L^G\uparrow_L^G$, one of indecomposable summands of $U'\downarrow_L^G$ must contain a source of U', when we restrict this summand to Q'. We denote this indecomposable summand by X. This X must has vertex a Q', otherwise it will contradict with U' has a vertex Q'. Also $X|U'\downarrow_L^G|V\uparrow_L^G\downarrow_L^G$, by step 1, we have that X is $L\cap {}^sQ$-projective. But since X is an indecomposable kL-module, we have that Q' must be L-conjugate to a subgroup of $L\cap {}^sQ$ for some $s\notin L$. Also ${}^lQ' < L\cap {}^sQ$ implies $Q' < L\cap {}^{sl^{-1}}Q$. Since $Q' < Q$, we have $Q' < Q\cap {}^{s'}Q$ for $s'\notin L$, since $s\notin L$, and we have $Q' < Q$. By step 0, we have that $|Q'|\neq|Q|$, hence Q' is a proper subgroup of Q.

For proof of (1): Now suppose U is an indecomposable kG-module with a vertex Q. Since U is also L-projective, $U|U\downarrow_L^G\uparrow_L^G$. Hence $U\downarrow_L^G$ contains an indecomposable kL-module V such that $U|V\uparrow_L^G$. And such a kL-module V must have a vertex Q and source T since U has. Now suppose $V'\ncong V$ is another indecomposable summand of $U\downarrow_L^G \mid T\uparrow_Q^G\downarrow_L^G$. By Step 1 of proof (2), V' must be ${}^xQ\cap L$-projective for some $x\in L-Q$. By Step 0, we know that ${}^xQ\cap L$ is not L-conjugate to Q, hence V' is not an indecomposable kL-module with a vertex Q.

For proof of (3): This follows from

$$U|U\downarrow_L^G\uparrow_L^G,\ V|V\uparrow_L^G\downarrow_L^G,$$

and the uniqueness of (1), (2).

Theorem 15 (Schur—Zassenhaus)**.** *Suppose G is a finite group, and N is a normal*

doi:10.6342/NTU201800167

subgroup of G such that the order of G/N is coprime to the order of N. Then G is a semidirect product of N and G/N.

Proof. See [11] Theorem 17.4.39.

Definition 16. We let $S_k(G)$ denote the set of all non-isomorphic simple kG-modules.

Proposition 17. *Suppose G is a finite group with the (unique) normal Sylow p-subgroup P cyclic of order p^n. Hence G is a semi-direct product of P and a subgroup K with $|K|$ coprime to p. Then the number of isomorphism classes of indecomposable kG-modules is $p^n \cdot |S_k(K)|$.*

Proof. See [43], Corollary 11.2.2.

Corollary 18. *Suppose G has a Sylow p-group P of order p, then there are*

$$(p-1) \cdot |S_k(N_G(P))| + |S_k(G)|$$

indecomposable kG-modules.

Proof. By the Schur-Zassenhaus Theorem, we have $N_G(P) = P \rtimes K$. And we have $|S_k(N_G(P))| = |S_k(K))|$(cf. [43], Corollary 6.2.2). By Proposition 17, there are $p \cdot |S_k(N_G(P))|$ non-isomorphic classes of $kN_G(P)$-modules. Since there are $|S_k(N_G(P))|$ indecomposable projective kG-modules (up to isomorphism), i.e. 1-projective, $p \cdot |S_k(N_G(P))| - |S_k(N_G(P))|$ of them must be P-projective. By Green's correspondence, there are $p|S_k(N_G(P))| - |S_k(N_G(P))|$ indecomposable and not projective kG-modules with a vertex P, and $|S_k(G)|$ indecomposable projective kG-modules.

Definition 19. A ring R is said to be of *finite representation type*, if there are only finitely many isomorphism classes of indecomposable R-modules.

Proposition 20. *Let k be a field of characteristic p and P be a Sylow p-subgroup of G. Then kG is of finite representation type if and only if kP is of finite representation type.*

Proof. $(\Rightarrow)$: For an indecomposable kP-module V, we have $V|V\uparrow_P^G\downarrow_P^G$. Since V is kP-indecomposable, $V|\ U\downarrow_P^G$ for some indecomposable kG-summand U of $V\uparrow_P^G$. Since kG is of finite representation type and by Theorem 13 for any indecomposable kG-module U, we have that $U\downarrow_P^G$ has only finitely many indecomposable kP-summands. Our kP can only be of finite representation type.

$(\Leftarrow)$: By Proposition 8, we know that every indecomposable kG-module U must be P-projective, and $U|V\uparrow_P^G$ for some indecomposable kP-module V. Again, by Theorem 13 and finiteness of kP, kG can only be of finite representation type.

If we assume the following Example in Section 2.2 and using the proposition above, we get a criterion of G that kG is of finite representation type.

Proposition 21. *Let P be a cyclic p-group of order $q = p^n$, k be a field of characteristic p, then kP is of finite representation type.*

Proof. Suppose M is an indecomposable kP-module with the representation $\rho : P \to \mathrm{GL}(M)$, and P is generated by g. Clearly, $\rho(g)^q = id$. Since characteristic of $k = p$, $(\rho(g) - id)^q = 0$. Since M is indecomposable, there are only one Jordan block of $\rho(g)$, and the size of Jordan block is not bigger than q. Particularly, $\dim_k M \leq q$. Hence there are only finitely many indecomposable kP-modules up to isomorphism.

Theorem 22. *Let k be a field of characteristic p. Then kG is of finite representation type if and only if any of its Sylow p-subgroup is cyclic.*

Proof. By Proposition 20, it is equivalent to prove that kP has finite representation type if and only if it is cyclic. By Proposition 21, we know that if P is cyclic then kP is of finite representation type. Now suppose P is not cyclic. Considering the Frattini subgroup $\Phi(P)$ of P (cf. [11] p. 199), we have that $P/\Phi(P) \cong {C_p}^d$. Since P is not cyclic, we have $d \geq 2$. Therefore, $C_p \times C_p$ is a homomorphic image of P. In Section 2.2 we will show that $kC_p \times C_p$ is not of finite representation type. Since any indecomposable

doi:10.6342/NTU201800167

$kC_p \times C_p$-module can be also viewed as an indecomposable kP-module, kP is not of finite representation type.

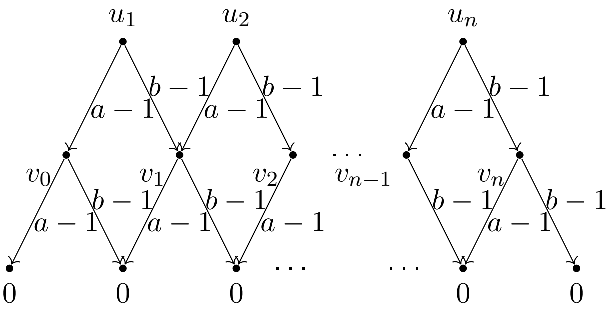
2.2 Infinitely many indecomposable representations

Suppose our G is $C_p \times C_p = \langle a \rangle \times \langle b \rangle$ and k is a field of characteristic p. Consider M_{2n+1} a kG-module of dimension $2n+1$ with basis $\{u_n, u_{n-1}, \cdots, u_1, v_0, v_1, \cdots, v_n\}$, and define the action of G on M_{2n+1} by

$$(a-1) \cdot u_i = v_{i-1},\ (b-1) \cdot u_i = v_i,$$

$$(a-1) \cdot v_i = 0,\ (b-1) \cdot v_i = 0.$$

Here 1 above is the identity element $(1,1)$ of G.



To see this is really an action of G on M_{2n+1}, we need to check $s(t \cdot x) = (st) \cdot x$. So we need to check that $(a-1)(b-1)x = (b-1)(a-1)x = 0 = (ab - b - a + 1)x$ and $0x = (a^p - 1^p)x = (a-1)^p x = (b-1)^p x = 0x = 0$. These can be computed directly.

Since n is arbitrary, once we prove that each M_{2n+1} is indecomposable, we have infinitely many indecomposable kG-modules. We prove this in two ways.

The first one is to prove that the endomorphism ring $E = \mathrm{End}_{kG}(M_{2n+1})$ is a local ring, then by [10] Proposition 6.10, M_{2n+1} is indecomposable kG-module. We can use the similar argument to prove that $\mathbb{Z}[X]/(p^2, X^2, pX)$ is a ring not of finite representation type. In the second proof, we use the relation of dimensions of kG-submodules to get a contradiction.

Proposition 23. *The kG-module M_{2n+1} is indecomposable.*

Proof. First, we choose an ordered basis $\mathscr{B} = \{v_0, v_1, \ldots, v_n, u_1, \ldots, u_n\}$ and let $S = a - 1$ and $R = b - 1$. Suppose $T \in E$, $T(v_j) = \sum_{i=0}^{n} a_{i,j} v_i + \sum_{i=1}^{n} b_{i,j} u_i$ and $T(u_j) = \sum_{i=0}^{n} a'_{i,j} v_i + \sum_{i=1}^{n} b'_{i,j} u_i$.

Since

$$\begin{aligned} ST(v_j) = S(\sum_{i=0}^{n} a_{i,j} v_i + \sum_{i=1}^{n} b_{i,j} u_i) = \sum_{i=1}^{n} b_{i,j} v_{i-1} \\ TS(v_j) = T(0), \end{aligned}$$

we have $b_{i,j} = 0$ for $0 \leq j \leq n,\ 1 \leq i \leq n$.

Since

$$\begin{aligned} ST(u_j) = S(\sum_{i=0}^{n} a'_{i,j} v_i + \sum_{i=1}^{n} b'_{i,j} u_i) = \sum_{i=1}^{n} b'_{i,j} v_{i-1} \\ TS(u_j) = T(v_{j-1}) = \sum_{i=0}^{n} a_{i,j-1} v_i, \end{aligned}$$

we have

$$a_{n,j} = 0,\ 0 \leq j \leq n-1,$$

and

$$b'_{i,j} = a_{i-1,j-1},\ 1 \leq i, j \leq n.$$

Using $TR(u_j) = RT(u_j)$, we have

$$TR(u_j) = T(v_j) = \sum_{i=0}^{n} a_{i,j} v_i$$
$$RT(u_j) = R(\sum_{i=0}^{n} a'_{i,j} v_i + \sum_{i=1}^{n} b'_{i,j} u_i) = \sum_{i=1}^{n} b'_{i,j} v_i,$$

hence we have

$$a_{0,j} = 0,\ 1 \leq j \leq n$$

and

$$a_{i,j} = b'_{i,j} = a_{i-1,j-1},\ 1 \leq i, j \leq n.$$

Using these equations, we have:

$$\left[T\right]_{\mathscr{B}} = \left[\begin{array}{cccc|cccc} a_{0,0} & 0 & \cdots & 0 & & & & \\ 0 & \ddots & \ddots & \vdots & & & & \\ \vdots & \ddots & \ddots & 0 & & & * & \\ 0 & \cdots & 0 & a_{0,0} & & & & \\ \hline & & & & a_{0,0} & 0 & \cdots & 0 \\ & & & & 0 & \ddots & \ddots & \vdots \\ & 0_{n,n+1} & & & \vdots & \ddots & \ddots & 0 \\ & & & & 0 & \cdots & 0 & a_{0,0} \end{array}\right] \text{, the left upper block is of size } n+1 \times n+1.$$

If the diagonal entries of $\left[T\right]_{\mathscr{B}}$ are zero, then T is nilpotent, hence T belongs to $\operatorname{Rad}(E)$. Also $cI \notin \operatorname{Rad}(E)$, for $c \neq 0$, and hence we have $E/\operatorname{Rad}(E) \cong k$. Therefore, E is a local ring and by [10] Proposition 6.10, M_{2n+1} is an indecomposable kG-module.

Now we give the second proof. We have $M_{2n+1} = U \oplus V$ as k-modules, where $U =$

$\langle u_0, \cdots, u_n\rangle_k$ and $V = \langle v_1, \cdots, v_n\rangle_k$. Suppose that M_{2n+1} is a decomposable kG-module. Then $M_{2n+1} = M_1 \oplus M_2$. We have $V = RM_{2n+1} + SM_{2n+1} = V_1 \oplus V_2$, where $V_1 := RM_1 + SM_1 \subset M_1$ and $V_2 := RM_2 + SM_2 \subset M_2$. We have $M_1/V_1 \xrightarrow{\sim} U_1 := M_1 \cap U$ and $M_2/V_2 \xrightarrow{\sim} U_2 := M_2 \cap U$. Since $M = M_1 \oplus M_2$ and $M/V \xrightarrow{\sim} U$, we have $U = U_1 \oplus U_2$. Then we have a decomposition $M_{2n+1} = U_1 \oplus U_2 \oplus V_1 \oplus V_2$ of vector spaces, and the dimension of $V_1 \oplus V_2$ is $n+1$.

Suppose we can prove that

$$\dim(V_i) = \dim(S(U_i) + R(U_i)) > \dim(U_i),$$

then we have $\dim(V_1 + V_2) = n + 1 \geq \dim(U_1 + U_2) + 2 = n + 2$, which can not happen. Then we have done.

Note that for a vector space V and any two arbitrary subspaces W_1, W_2, we have $\dim(W_1) + \dim(W_2) - \dim(W_1 \cap W_2) = \dim(W_1 + W_2)$.

Let $W = U_1$, $W_1 = S(W)$ and $W_2 = R(W)$. Since the maps S and R are injective from $U \to V$, we have $\dim(W) = \dim(W_1) = \dim(W_2)$. Since $\dim(W_1 + W_2) = \dim(V_1)$ and $\dim(U_1) = \dim(W)$, it is easy to show that the condition $\dim(V_1) > \dim(U_1) \Leftrightarrow \dim(W) > \dim(W_1 \cap W_2)$. The latter is equivalent to $W_1 \neq W_2$.

Suppose that W is contained in a subspace $\langle u_i, u_{i+1}, \ldots, u_j\rangle$, where $[i, j]$ is the minimal internal with this condition; that is possible since M_{2n+1} is finite-dimensional. Then

$$W_1 := S(W) \subset \langle v_{i-1}, \ldots, v_{j-1}\rangle, \quad W_2 := T(W) \subset \langle v_i, \ldots, v_j\rangle.$$

Suppose $W_1 = W_2$, we have

$$W_1 = W_2 = W_1 \cap W_2 \subset \langle v_i, \ldots, v_{j-1}\rangle, W \subset \langle u_{i+1}, \ldots, u_j\rangle.$$

doi:10.6342/NTU201800167

However, the result that $W \subset \langle u_{i+1}, \ldots, v_j \rangle$ contradicts with the minimality of $[i, j]$. Therefore, we prove that $\dim(V_1) > \dim(U_1)$, and similarly that $\dim(V_2) > \dim(U_2)$. This follows that M_{2n+1} is an indecomposable kG-module.

Since M_{2n+1} is indecomposable and n can be chosen arbitrary, the ring $kG = kC_p \times C_p$ is not of finite representation type.

2.3 Another example of infinitely many indecomposable modules

In this section, the algebra we consider is not a group ring. Let $B := \mathbb{Z}/(p^2)$ and $R := B[X]/(pX, X^2) = \mathbb{Z}[X]/(p^2,\ pX,\ X^2)$. Consider a free B-module F of rank $2n+1$ with basis $\mathscr{B} = \{v_0, v_1, \ldots, v_n,\ u_1, \ldots\ u_n\}$. Let M_{2n+1} be the R-module which is the quotient of F by the following relations:

$$pu_i = v_i,\ Xu_i = v_{i-1},$$
$$pv_i = 0,\ Xv_i = 0.$$

doi:10.6342/NTU201800167

Suppose $T \in \operatorname{End}_R(M_{2n+1})$, similar to the first proof of Proposition 23, we have

$$\Big[T\Big]_{\mathscr{B}} = \left[\begin{array}{cccc|cccc} a_{0,0} & 0 & \cdots & 0 & & & & \\ 0 & \ddots & \ddots & \vdots & & & & \\ \vdots & \ddots & \ddots & 0 & & \multicolumn{2}{c}{*} & \\ 0 & \cdots & 0 & a_{0,0} & & & & \\ \hline & & & & a_{0,0} & 0 & \cdots & 0 \\ & & & & 0 & \ddots & \ddots & \vdots \\ & \multicolumn{2}{c}{0_{n,n+1}} & & \vdots & \ddots & \ddots & 0 \\ & & & & 0 & \cdots & 0 & a_{0,0} \end{array}\right].$$

Since v_i is annihilated by p, we have $a_{0,0} \in \mathbb{F}_p$. Therefore, we have $\operatorname{End}_R(M_{2n+1})/\operatorname{Rad}(\operatorname{End}_R(M_{2n+1})) \cong \mathbb{F}_p$. Consequently, M_{2n+1} is R-indecomposable. This shows that the Artinian ring $R = \mathbb{Z}[X]/(p^2,\ pX,\ X^2)$ is not of finite representation type.

2.4 General results of kG

In this section, we study the cde triangle and projective covers for kG-modules. Our reference is [36]. Recall that we assume A is a complete discrete valuation ring with quotient field K. The characteristic of residue field k is p dividing the order of G, and the characteristic of K is 0. Let $F_k(G)$ be a free abelian group generated by all isomorphism classes of kG-modules, and $F_k^+(G)$ be the subset of $F_k(G)$ generated by all isomorphism classes of kG-modules with coefficients in $\mathbb{Z}_{\geq 0}$. Let $Q_k(G)$ be the subgroup of $F_k(G)$, generated by $E - E' - E''$ if there is a kG-exact sequence $0 \to E' \to E \to E'' \to 0$. Let $R_k(G)$ denote the Grothendieck group of finitely generated kG-modules, i.e. $R_k(G) := F_k(G)/Q_k(G)$. We denote by $[E]$ the image of an element $E \in F_k(G)$ in $R_k(G)$. Let $R_k^+(G)$ be the image of $F_k^+(G)$ in $R_k(G)$, i.e. the element of $F_k^+(G)$ is $[E]$ for some kG-module E.

Example 24. Let G be $C_2 = \langle a \rangle$, and $k = \mathbb{F}_2$. Consider the regular representation $\mathbb{F}_2G$, the trivial representation U is inside $\mathbb{F}_2G$. The trivial representation is the only one representation of dimension 1. If U is a direct summand of $\mathbb{F}_2G$, then we can decompose $\mathbb{F}_2G$ as $U \oplus V$, and $V = \operatorname{Span}\{a\}$, or $\operatorname{Span}\{e\}$ by observing the elements of $\mathbb{F}_2G$. However, either case contains U, which is impossible. We have that $0 \to U \to \mathbb{F}_2G \to U \to 0$, so $[\mathbb{F}_2G] = 2[U]$, however $\mathbb{F}_2G \ncong U \oplus U$.

We use the similar way to define $R_K(G)$ for a field K of characteristic zero. Since KG is semisimple, any short KG-exact sequence $0 \to E' \to E \to E'' \to 0$ splits. This means that $[E] = [E'] + [E'']$ if and only if $E = E' \oplus E''$. Hence the Grothendieck group $R_K(G)$ is isomorphic to the free abelian group generated by characters defined over K. Denote the image of all finitely generated KG-modules in $R_K(G)$ by $R_K^+(G)$.

For $P_k(G)$, we use the same way but only consider projective kG-modules. Using the projectivity, any projective kG-module is a direct sum of indecomposable ones. Thus the subgroup $P_k(G)$ is just the free abelian group generated by isomorphism classes of indecomposable projective kG-modules. Let $P_k^+(G)$ be the semi-subgroup of $P_k(G)$ generated by isomorphism classes of indecomposable projective kG-modules with coefficients in $\mathbb{Z}_{\geq 0}$.

Once we have defined the abelian groups $R_k(G), R_K(G), P_k(G)$, we can draw a triangle, which is described as follows.

For any element of $P_k^+(G)$, we can consider its image in $R_k^+(G)$. Hence we get an additive map from $P_k^+(G) \to R_k^+(G)$, and extend it to a homomorphism $c : P_k(G) \to R_k(G)$.

Here is a way to obtain a kG-module from a KG-module. Suppose V is a KG-module. Choose an arbitrary lattice L_1 of V, i.e. L_1 is finitely generated A-module in V, and L_1 spans V with K coefficient. We can get an AG-module $L_2 = \sum_{g \in G} gL_1$. Consider the quotient module $L_2/\mathfrak{m}L_2 = \bar{L}_2$, and then it is a kG-module we get from V, called the reduction mod $\mathfrak{m}$ of L_2.

Proposition 25. *For all kG-modules of reduction from the same KG-module, their images in $R_k(G)$ are the same.*

Proof. See [36], Theorem 32.

Therefore, we have an additive map from $R_K^+(G) \to R_k^+(G)$ and extend it to a homomorphism $d : R_K(G) \to R_k(G)$.

The assumption at the beginning of this chapter that A is a complete discrete valuation ring with residue field k leads to the following proposition.

Proposition 26. *For any projective kG-module E, there is a unique projective AG-module such that its reduction is isomorphic to E. Moreover, for any projective AG-module, its reduction is a projective kG-module.*

Proof. See [36], Proposition 42.

By this proposition, we can identify $P_k(G)$ and $P_A(G)$. Given a projective AG-module, after tensoring K over A, we get a KG-module. After identifying $P_k(G)$ and $P_A(G)$, we have the last homomorphism $e : P_k(G) \to R_K(G)$.

At the end, we have a cde triangle with homomorphisms c, d, e. Further, this diagram commutes by the definition of d.

$$\begin{tikzcd}
P_k(G) \arrow[r, "c"] \arrow[dr, "e"] & R_k(G) \\
& R_K(G) \arrow[u, "d"]
\end{tikzcd}.$$

Definition 27. Let M be a kG-module and P be a projective kG-module. We call P a *projective cover (envelope)* of M if there exists a surjective homomorphism $\phi : P \to M$ such that for any proper submodule Q of P, $\phi(Q) \neq M$.

Proposition 28. *(1) Every kG-module M has a projective cover unique up to isomorphism.*

(2) Suppose P_i is the projective cover of E_i, then $\bigoplus P_i$ is the projective cover of $\bigoplus E_i$.

(3) Every projective kG-module P is the projective cover of its maximal semisimple quotient E, i.e. every semisimple quotient of P will factor thrugh E.

Proof. See [36], Proposition 41.

Remark 29. Proposition 28 says that for every M, it has a unique projective cover, but the converse is not true. More precisely, non isomorphic kG-modules may have the isomorphic projective covers. For example, given a non semisimple kG-module M, by (3), we know its projective cover P can also be the projective cover of the maximal semisimple quotient of P.

Remark 30. Let $\mathfrak{r}$ be the radical of kG, the maximal semisimple quotient in (3) is $P/\mathfrak{r}P$.

By (3) and (2) of Proposition 28, every indecomposable projective module is the projective cover of a simple module. Conversely, the projective cover of a simple module is an indecomposable projective module by (3) and the definition of projective covers.

Suppose E, and E' are two non-isomorphic simple kG-modules, and we denote their projective covers by P_E, and $P_{E'}$, respectively. By Remark 30, P_E, and $P_{E'}$ are not isomorphic.

From the discussion above, we have a one-one correspondence between indecomposable projective kG-modules and simple kG-modules. As mentioned before, $P_k(G)$ is a free abelian group with basis of indecomposable projective kG-modules. Combining these two results, we have the following proposition.

Proposition 31. *The set $\{[P_E]\}$, for $E \in S_k(G)$, forms a basis of $P_k(G)$.*

Definition 32. Let p be a prime number. An element $g \in G$ is said to be *p-regular* if its order is prime to p. Conjugacy classes of p-regular elements are called *p-regular conjugacy classes*.

doi:10.6342/NTU201800167

Recall that if K is a field of characteristic 0 and it is sufficiently large, then the number of irreducible representations of G over K is the number of conjugacy classes of G (cf. [36], Theorem 7). Now, we also have a description of the number of irreducible representations of G over k of characteristic p.

Theorem 33. *If k is a sufficiently large field and of characteristic p, then the number of irreducible representations of G over k is the same as the number of p-regular conjugacy classes of G.*

Proof. See [36], Theorem 42.

2.5 The example $G = S_3$

Now we use what we have known to look at the modular representations of symmetric group S_3 more closely.

Case $k = \mathbb{F}_2$:

There are two 2-regular conjugacy classes of S_3. By Theorem 33, we know that there are at most two simple-$\mathbb{F}_2S_3$-modules up to isomorphism. We denote the trivial representation by U and denote by V the 2 dimensional representation over $\mathbb{F}_2$ generated by $\{e_1 - e_2,\ e_2 - e_3\}$ in the standard representation, i.e. S_3 permutes the basis $\{e_1,\ e_2,\ e_3\}$ of the standard representation. We know U is the only representation of S_3 over $\mathbb{F}_2$ of degree 1. Also we can compute directly that there does not exist a subrepresentation M of V such that $M \cong U$. Therefore, V is an irreducible representation of S_3.

Since indecomposable projective modules are direct summands of $\mathbb{F}_2S_3$, we can find all indecomposable projective kG-modules by finding the idempotents of $\mathbb{F}_2S_3$.

We know that the Sylow 2-subgroup of S_3 is cyclic , hence by Theorem 22, $\mathbb{F}_2S_3$ is of finite representation type. By Corollary 18, we can know that there are $(2 -$

$1)|S_k(N_G(P))| + |S_k(S_3)| = (2-1)|S_k(C_2)| + |S_k(S_3)| = 1+2 = 3$ isomorphism classes of indecomposable $\mathbb{F}_2S_3$ modules. It might be weird that there are two simple $\mathbb{F}_2S_3$-modules and two indecomposable projective $\mathbb{F}_2S_3$-modules, but only three indecomposable $\mathbb{F}_2S_3$-modules. Actually, one of the simple modules is projective.

Suppose $\tau, \sigma \in S_3$, $\tau = (123), \sigma = (12)$. Let $e_1 = 1 + \sigma + \tau + \sigma^2\tau \in \mathbb{F}_2S_3$. We have $e_1^2 = e_1$, hence it is an idempotent of $\mathbb{F}_2S_3$. Let W be the $\mathbb{F}_2S_3$-module $\mathbb{F}_2S_3e_1$. We have

$$v_1 := 1e_1 = \tau e_1,\ v_2 := \sigma^2 e_1 = \tau\sigma e_1,\ v_3 := \sigma e_1 = \tau\sigma^2 e_1 = v_1 + v_2,$$

and then we find out $W \cong V$ as $\mathbb{F}_2S_3$-modules. Since W is projective and simple, W is the projective cover of itself.

Let $e_2 = 1+\tau+\tau^2$. It is easy to compute that $e_2^2 = e_2$ and e_2 is a *primitive* idempotent. We have that $\mathbb{F}_2S_3e_2$ is a projective *indecomposable* $\mathbb{F}_2S_3$-module. Since $e_2 + \sigma e_2$ is fixed by S_3, the module $\mathbb{F}_2S_3e_2$ has a submodule isomorphic to U, and the quotient by U is isomorphic to U. Therefore, $\mathbb{F}_2S_3e_2$ is the projective cover of U.

Case $k = \mathbb{F}_3$:

There are two 3-regular conjugacy classes. The trivial representation and sign representation are irreducible representations of S_3 over $\mathbb{F}_3$, because they are of degree 1 and non-isomorphic. We still denote the subrepresentation generated by $\{e_1 - e_2,\ e_2 - e_3\}$ in the standard representation by V. Since $e_1 + e_2 + e_3 = (e_1 - e_2) - (e_2 - e_3) \in V$ and it is fixed by S_3, V is not an irreducible representation.

The Sylow 3-subgroup of S_3 is cyclic, and it is a normal subgroup of S_3. Therefore, we know that $\mathbb{F}_3S_3$ is of finite representation type. By Corollary 18, there are

$$(3-1)|S_k(N_{S_3}(C_3))| + |S_k(C_3)| = 2 \times 2 + 2 = 6$$

doi:10.6342/NTU201800167

isomorphism classes of indecomposable $\mathbb{F}_3 S_3$-modules.

Proposition 34. *Let N be a nilpotent ideal of any ring A, and ε an idempotent in A/N. Then there exists an idempotent e of A mapping to ε. Moreover, if ε is primitive, then so is any lift e.*

Proof. See [43], Theorem 7.3.5.

To compute the idempotents of $\mathbb{F}_3 S_3$, we first consider a map $f : \mathbb{F}_3 S_3 \to \mathbb{F}_3 C_2$, by $\sigma \mapsto 1$. Then the kernel of f is $\mathrm{Rad}\mathbb{F}_3 S_3 = (\sigma - 1)$. By Proposition 34, we compute the idempotents of $\mathbb{F}_3 C_2$ first. Since

$$(\bar{1} + \bar{\tau})^2 = (\bar{1} + 2\bar{\tau} + \bar{\tau}^2) = 2(\bar{1} + \bar{\tau}),$$

we have $\bar{e_1} := \frac{1}{2}(\bar{1} + \bar{\tau}) = 2(\bar{1} + \bar{\tau})$ is a primitive idempotent of $\mathbb{F}_3[C_2]$. Similarly, we get another primitive element $\bar{e_2} := 2(\bar{1} - \bar{\tau})$, and they are all. Therefore, the candidates of the primitive idempotents of $\mathbb{F}_3 S_3$ are known. Fortunately, their liftings are $2 + 2\tau, 2 - 2\tau$ and we denote them as e_1, e_2, respectively.

Definition 35. Let R be a commutative ring and G a finite group acting on R with $\rho : G \to \mathrm{Aut}_{ring}(R)$. The *twisted group ring of G over R relative to ρ* is defined by

$$R \circ G = \{\sum_{g \in G} a_g g : \ a_g \in R\},$$

$$a_g g \cdot a_h h = a_g(\rho(g) a_h) gh.$$

We will omit ρ and write $r_1 \rho(g_1)(r_2) g_1 g_2$ as $r_1 g_1(r_2) g_1 g_2$ for short.

If we let $t = \sigma - 1$, then we have $t^3 = 0$ and $\tau t \tau^{-1} = \tau\sigma\tau^{-1} - 1 = \sigma^2 - 1 = (\sigma + 1)(\sigma - 1) = (t + 2)t$. Consider a twisted group ring $\mathbb{F}_3[t]/(t^3) \circ C_2$, where $C_2 = \langle \tau \rangle$ of order 2 and τ acts on t by $\tau(t) = (t + 2)t$. We have $1\tau \cdot t1 = 1\tau(t)(\tau 1) = (t + 2)t\tau$.

doi:10.6342/NTU201800167

Consider $\phi : \mathbb{F}_3[t]/(t^3) \circ C_2 \to \mathbb{F}_3S_3$ via $\alpha x \mapsto \alpha x$ and identifying $t,\ \tau$ in both sides, we have a ring isomorphism ϕ.

Since $\tau e_1 = 2\tau(1+\tau) = 2(\tau+1) = e_1$, we have that $\mathbb{F}_3S_3e_1 \cong \mathbb{F}_3[t]/t^3[1,\tau]e_1 = \mathbb{F}_3[t]/t^3e_1$. Moreover, $\tau \cdot t = (t+2)t \in (t)$, and hence $t^i\mathbb{F}_3[t]/t^3e_1$ are $\mathbb{F}_3S_3$-modules. Similarly, we have the other three $\mathbb{F}_3S_3$-modules $t^i\mathbb{F}_3[t]/t^3e_2$ and $\tau e_2 = \tau 2(1-\tau) = 2\tau - 2 = -e_2$. Since $t^i\mathbb{F}_3[t]/t^3e_j$, for $i = 0,1,2$, and $j = 1,2$, are homomorphic images of indecomposable modules $\mathbb{F}_3[t]/t^3e_j,\ j = 1,\ 2$, all of these 6 are indecomposable $\mathbb{F}_3S_3$-modules. Note that the annihilators of $t^i\mathbb{F}_3[t]/t^3e_j$ and $t^{i'}\mathbb{F}_3[t]/t^3e_{j'}$ are different if $i' \neq i$. From the actions of τ on e_1 and e_2, we see that these 6 indecomposable $\mathbb{F}_3S_3$-modules are mutually non-isomorphic.

We can also see this result using Green's correspondence. By Proposition 8, all indecomposable $\mathbb{F}_3S_3$-module are C_3-projective. Two of them are projective and have vertices $\{1\}$. The others are all have vertices C_3. By the same argument of the proof of Proposition 21, all indecomposable $\mathbb{F}_3C_3$-modules are $t^i\mathbb{F}_3[t]/t^3$, for $i = 0,1,2$. Any indecomposable $\mathbb{F}_3S_3$-module appears as a direct summand of $t^i\mathbb{F}_3[t]/t^3 \uparrow_{C_3}^{S_3}$ for some i by Green's correspondence. When $i = 0, \mathbb{F}_3[t]/t^3 = 1 \uparrow_1^{C_3}$, and we have 2 isomorphism classes of indecomposable $\mathbb{F}_3S_3$-modules from

$$t^i\mathbb{F}_3[t]/t^3 \uparrow_{C_3}^{S_3} = t^i(\mathbb{F}_3[t]/t^3 \uparrow_{C_3}^{S_3}) = t^i(1 \uparrow_1^{S_3}) = t^i\mathbb{F}_3S_3 = t^i(\mathbb{F}_3S_3e_1 \oplus \mathbb{F}_3S_3e_2).$$

Similarly for $i = 1$ or 2, we have the other 4 isomorphism classes of indecomposable $\mathbb{F}_3S_3$-modules.

doi:10.6342/NTU201800167

Chapter 3

Integral representations

In this chapter, we focus on some general results about the group ring $A = \mathbb{Z}G$, where G is a finite group. We shall consider only finitely generated $\mathbb{Z}G$-modules which are $\mathbb{Z}$-torsion free. These modules are called A-lattices. Indeed, if we do not require this condition, then it is easy to construct many A-modules even generated by one element. For example, any $\mathbb{Z}/p^kG$ can be viewed as an A-module.

3.1 Introduction

Definition 36. Let R be an integral domain with fraction field K. An R-module M is said to be of *R-rank n*, if $\dim_K M \otimes_R K$ is n.

Example 37. Let R be a Dedekind domain and K its fraction field. Then K is an R-module of R-rank one.

Let R be a Dedekind domain, and let Λ be an R-algebra. Let M be a left Λ-module which is *R-projective and R-finitely generated*. Let I be the annihilator of M in Λ. Then M is a Λ/I-module. We denote Λ/I by $\bar{\Lambda}$. Then we can consider $\bar{\Lambda}$-structure of M. The following explains that $\bar{\Lambda}$ is actually an R-algebra, *R-projective and R-finitely generated.* This motivates us to looking at *R-lattice* and *R-order*.

doi:10.6342/NTU201800167

Since the annihilator of M in Λ is I, M is a faithful $\bar{\Lambda}$-representation. Since Λ is an R-algebra, so is $\bar{\Lambda}$. Hence we have $\bar{\Lambda} \to \mathrm{End}_R(M)$. Since M is $\bar{\Lambda}$-faithful, we can regard $\bar{\Lambda}$ as a subring of $\mathrm{End}_R(M)$. Since M is an R-projective, we have $M \oplus M' = R^{(k)}$ for some R-module M' and integer k. Since $\mathrm{End}_R(M)$ is a direct summand of $\mathrm{End}_R(R^{(k)}) = M_k(R)$, we have $\mathrm{End}_R(M)$ is R-projective. Since R is a Dedekind domain, it is a Noetherian ring. Hence any submodule of a finitely generated R-module is also finitely generated. Moreover, any submodule of a projective R-module is also projective, because it is torsion free and R is Dedekind. Thus, $\bar{\Lambda}$ is also *R-projective and R-finitely generated.*

In the following, R denotes a Dedekind domain with fraction field K.

Definition 38. An R-module M is said to be an R-lattice if it is R-projective and R-finitely generated.

Definition 39. An R-algebra is said to be an *R-order* if it is also an R-lattice.

Definition 40. Let A be a finitely dimensional K-algebra. An R-subalgebra Λ in A is said to be an R-order *in* A if Λ is an R-order and $K\Lambda = A$. If an R-order Λ in A can not be strictly contained in an R-order Γ in A, then Λ is said to be a *maximal order* in A.

Definition 41. Let Λ be an R-order in a K-algebra A. A Λ-module is said to be a Λ-lattice if it is R-lattice.

Theorem 42 (Jordan-Zassenhaus Theorem)**.** *Let R be a Dedekind domain with fraction field K. Assume K is a global field. Suppose A is a finite-dimensional semisimple K-algebra, and Λ is an R-order in A. Given an arbitrary finitely generated A-module M, there exist only finitely many non-isomorphic Λ-lattices $X_1, \cdots, X_m$ such that $K \otimes X_i \cong M$ as A-modules, $\forall\, i = 1, \ldots, m$.*

Proof. See [10] Jordan-Zassenhaus Theorem 24.1.

doi:10.6342/NTU201800167

Theorem 43. *Let R be a discrete valuation ring with maximal ideal $\mathfrak{m}$. Let $R_{\mathfrak{m}}$ be the completion of R. Suppose Λ is an R-order. We write $\Lambda_{\mathfrak{m}} = R_{\mathfrak{m}} \otimes_R \Lambda$. Suppose M, N are Λ-modules and finitely generated R-modules, then*

$$M \cong N \text{ as } \Lambda\text{-modules if and only if } M_{\mathfrak{m}} \cong N_{\mathfrak{m}} \text{ as } \Lambda_{\mathfrak{m}}\text{-modules.}$$

Proof. See [10] Proposition 30.17.

Note that this theorem does not tell us whether any $\Lambda_{\mathfrak{m}}$-module arises from a Λ-module.

Let G be a finite group, $A = KG$ the group algebra and $\Lambda = RG$ the group ring. For any prime $\mathfrak{p}$ of R, denote by $R_{(\mathfrak{p})}$ the localization of R at $\mathfrak{p}$, and by $R_{\mathfrak{p}}$ the completion of R with valuation $v_{\mathfrak{p}}$. For any Λ-module M, write $M_{(\mathfrak{p})} = R_{(\mathfrak{p})} \otimes_R M$ and $M_{\mathfrak{p}} = R_{\mathfrak{p}} \otimes_R M$. If M is a Λ-lattice and one may regard M as a Λ-submodule of $M_{(\mathfrak{p})}$ or of $M_{\mathfrak{p}}$. When M is R-free, we call M an integral representation of G over R. Some authors call M so if M is required only R-torsion free.

Proposition 44. *For any prime ideal $\mathfrak{p}$ of R and a $\Lambda_{(\mathfrak{p})}$-lattice M, there exists a Λ-lattice X such that $R_{(\mathfrak{p})} \otimes_R X \cong M$.*

Proof. See [10] Corollary 23.14.

Definition 45. We say two RG-lattices M and N are in the same *genus* if $M_{(\mathfrak{p})} \cong N_{(\mathfrak{p})}$ for any prime ideal $\mathfrak{p}$ of R.

In Propositions 46 and 47, we assume that R is the ring of integers in a number field K. Set $S = \{\mathfrak{p} : \text{prime ideal of R: } \mathfrak{p} \mid |G|\}$. Let $R_{(S)} = \bigcap_{\mathfrak{p} \in S} R_{(\mathfrak{p})}$.

Proposition 46. *An RG-lattice M is RG-indecomposable if and only if $R_{(S)} \otimes_R M$ is $R_{(S)}G$-indecomposable.*

Proof. See [34] Theorem 1.2.

Proposition 47. *Two RG-lattices M and N are in the same genus if and only if $R_{(S)} \otimes M \cong R_{(S)} \otimes N$.*

Proof. See [10] Proposition 31.15.

Proposition 48. *Let G be a finite group of order n. Suppose K is a field of characteristic not dividing n. Let Λ be an R-order in KG containing RG. Then we have $nRG \subset n\Lambda \subset RG$. Moreover, RG is a maximal R-order of KG if and only if n is a unit of R.*

Proof. See [10] Proposition 27.1.

Proposition 49. *Suppose Λ is a maximal R-order in a finite-dimensional separable algebra A over K. A left Λ-lattice M is indecomposable if and only if KM is a simple A-module.*

Proof. See [10] Theorem 26.12.

Remark 50. Suppose that R is a discrete valuation ring with residue field of characteristic not dividing $|G|$. Then combining Propositions 48, 49, and Theorem 42, there are only finitely many non-isomorphic indecomposable RG-lattices.

3.2 An example and reduction mod p

We keep the notations in Section 2.5 but let the ground field k be $\mathbb{Q}$. Let $\sigma = (1\ 2) \in S_3$ and $\tau = (1\ 2\ 3) \in S_3$. Let U (respectively U', V) be the trivial (respectively sign, standard) representation of S_3 over $\mathbb{Q}$. After choosing ordered basis $\mathscr{B} = \{v_1 = e_1 - e_2, v_2 = e_2 - e_3\}$ of V we have an isomorphism ϕ from $\mathbb{Q}S_3$ to $\mathbb{Q} \times \mathbb{Q} \times M_2(\mathbb{Q})$. We compute the image and find out that $\mathbb{Z}S_3 \ncong \mathbb{Z} \times \mathbb{Z} \times M_2(\mathbb{Z})$. We write $\mathcal{O} = \mathbb{Z} \times \mathbb{Z} \times M_2(\mathbb{Z})$, a maximal $\mathbb{Z}$-order in $\mathbb{Q}S_3$. Using this ϕ, we have

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

$$(1\ 2\ 3) \mapsto (1,\ 1,\ \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}).$$

Let

$$E_1 = (1,\ 0, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}),\ E_2 = (0,\ 1, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}),\ E_3 = (0,\ 0, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}),$$

$$E_4 = (0,\ 0, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}),\ E_5 = (1,\ 0, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}),\ E_6 = (1,\ 0, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}),$$

we have $\mathcal{O} = \langle E_1,\ E_2,\ E_3,\ E_4,\ E_5,\ E_6 \rangle_{\mathbb{Z}}$. If we choose an ordered basis $\mathscr{A} = \{\sigma, \tau\sigma,\ \tau^2\sigma,\ \tau,\ \tau^2,\ e = \tau^3\}$ of $\mathbb{Q}S_3$, we have

$$\begin{bmatrix} \phi \end{bmatrix}_{\mathscr{A},\ \mathscr{B}} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & 1 & 1 & 1 \\ -1 & 0 & 1 & 0 & -1 & 1 \\ 0 & -1 & 1 & 1 & -1 & 0 \\ 1 & -1 & 0 & -1 & 1 & 0 \\ 1 & 0 & -1 & -1 & 0 & 1 \end{bmatrix}.$$

By changing the ordered basis $\mathscr{A}$ of $\mathbb{Z}S_3$ (i.e. only use elementary column operations like interchanging two columns and adding any *integer* multiple of a column to another),

doi:10.6342/NTU201800167

we have

$$\Big[\phi\Big]_{\mathscr{A},\ \mathscr{B}} = HU,\ H = \begin{bmatrix} 6 & 3 & 3 & -1 & 1 & 1 \\ 0 & -3 & 3 & -3 & 1 & 1 \\ 0 & 0 & 3 & -1 & -1 & 1 \\ 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},\ U = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 \\ 1 & -2 & 1 & 0 & 0 & 0 \\ 1 & -1 & 0 & -1 & 1 & 0 \\ 1 & 0 & 1 & -1 & 0 & 1 \end{bmatrix}.$$

From the matrix H, we see that $\mathbb{Z}S_3$ contains $6\mathcal{O}$ (cf. Proposition 48). Localizing at $p = 2, 3$, we see that $\mathbb{Z}_2S_3$ contains $2\mathcal{O}_2$ and $\mathbb{Z}_3S_3$ contains $3\mathcal{O}_3$. Thus, we can describe $\mathbb{Z}_pS_3$ by its image $\mathbb{Z}_pS_3/p\mathcal{O}_p$ in $\mathcal{O}_p/p\mathcal{O}_p = \mathbb{F}_p \times \mathbb{F}_p \times M_2(\mathbb{F}_p)$. The map $\mathbb{Z}_pS_3 \to \mathbb{Z}_pS_3/(p\mathcal{O}_p) \subset \mathbb{F}_p \times \mathbb{F}_p \times M_2(\mathbb{F}_p)$ induces a map $\rho : \mathbb{F}_pS_3 \to \mathbb{F}_p \times \mathbb{F}_p \times M_2(\mathbb{F}_p)$.

Since $\mathbb{F}_pS_3$ is not semisimple for $p = 2,\ 3$, we know that its image $\rho(\mathbb{F}_pS_3)$ is not equal to $\mathbb{F}_p \times \mathbb{F}_p \times M_2(\mathbb{F}_p)$. Looking at H (modulo 2 or 3), we have $\rho(\mathbb{F}_2S_3) \cong \{(x, -x, M_2(\mathbb{F}_2))|x \in \mathbb{F}_2\}$. Thus its semisimple quotient is $\mathbb{F}_2 \times M_2(\mathbb{F}_2)$. This is compatible with the fact that all non-isomorphic simple $\mathbb{F}_2S_3$-modules class are U and V (over $\mathbb{F}_2$). For $p = 3$ we see that $\rho(\mathbb{F}_3S_3)$ is isomorphic to an $\mathbb{F}_3$-subalgebra of $M_2(\mathbb{F}_3)$ of dimension 3. This is a Borel subgroup of $M_2(\mathbb{F}_3)$, so we can choose a basis such that the image $\rho(\mathbb{F}_3S_3) \cong \left\{\begin{pmatrix} \star & \star \\ 0 & \star \end{pmatrix}\right\}$. Its semisimple quotient is $\mathbb{F}_3 \times \mathbb{F}_3$.

3.3 Finiteness of the group ring $\mathbb{Z}G$

Let G be a finite group. For the rest of this chapter and Chapter 4, an R-module will mean an R-lattice unless specifically stated otherwise. In this section, we will state a criterion of G that $\mathbb{Z}G$ is of finite representation type (for R-lattices). We follow mainly Heller and Reiner [17] and [18].

Let p be a prime number. For a $\mathbb{Z}G$-module M, and recall that we denote $\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} M$ by $M_{(p)}$ and $\mathbb{Z}_p \otimes_{\mathbb{Z}} M$ by M_p, respectively. Let K be a number field, and R the ring of integers in K. Suppose P is a prime ideal of R containing integer p, and then we denote localization of R at P by $R_{(P)}$ and the completion of $R_{(P)}$ by R_P. Let K_P be the completion of K at P.

Definition 51. Let K, P and G be as above. We call K is a *splitting field for G relative to K_P*[1] if for any simple KG-module M, its completion M_P is also a simple K_PG module.

If we write $KG = \prod_{i=1}^{r} M_{n_i}(D_i)$ into a product of simple K-algebras, where D_i are division K-algebras. Any simple G-module then is of the form $M = D_i^{n_i}$ of column D_i-vectors. It is easy to compute that $\mathrm{End}_{KG}(M) \simeq D_i^{\mathrm{opp}}$. Since taking centralizer commutes with base change, we have $\mathrm{End}_{K_PG}(M_P) \simeq D_i^{\mathrm{opp}} \otimes_K K_P$. Therefore, the module M_P is G-simple if and only if $D_i \otimes_K K_P$ remains a division algebra. Thus, that K is a splitting field of G relative to K_P means that the number r of simple factors in KG and the numbers n_i of sizes of simple factors remain the same after the completion at P.

Theorem 52. *If K is a splitting field for G relative to K_P, then given an $R_{(P)}G$-module M, the map $M \mapsto R_PM$ induces a one-one correspondence between the set of isomorphism classes of $R_{(P)}G$-modules and those of R_PG-modules.*

Proof. See [10], Theorem 30.18.

Corollary 53. *Suppose K is a splitting field for G relative to K_P. An $R_{(P)}G$-module M is indecomposable if and only if the R_PG-module R_PM is indecomposable.*

[1] This terminology is due to Heller [19]. However, it is not taken in Curtis and Reiner [10]. We illustrate the idea as follows. For a field extension L/K of characteristic 0, we may call K is a relatively splitting field of G with respect to L if the number r of simple factors and the numbers n_i of size in its Wedderburn decomposition remain the same after tensoring L over K. Recall that K is a splitting field of G if KG is a product of matrix algebras over K, or equivalently, any simple KG-module is absolutely simple. In other words, K is a relatively splitting field of G with respect to $\overline{K}$ precisely when K is a splitting field of G.

doi:10.6342/NTU201800167

Proposition 54. *Suppose G is an abelian p-group of exponent p^e, and K and v_P are as above. Let L be the field extension of K by adjoining a primitive p^e-th root of unity ξ. If v_P has only one extension on L, then K is a splitting field of G relative to K_P.*

Proof. This is originally proved in the case where G is a cyclic p-group; see [17], Theorem 1.4. Write $C = C_{p^{e_1}} \times \cdots \times C_{p^{e_r}}$ with $e_1 \le e_2 \le \cdots \le e_r = e$. Then $KG = \otimes_{i=1}^{r} KC_{p^{e_i}}$. We first show that the K-algebra KG is a product of finite field extensions of the form $K(\xi_j)$ with $j \le e$, where ξ_j is a primitive p^j-th root of unity. We prove this by induction on r. The case $r = 1$ is clear. When $r > 1$, one has

$$KG = (\bigotimes_{i=1}^{r-1} \otimes_K KC_{p^{e_i}}) \otimes_K KC_{p^{e_r}}$$

Using the induction hypothesis, both $\otimes_{i=1}^{r-1} KC_{p^{e_i}}$ and $KC_{p^{e_r}}$ are products of field extensions of the form $K(\xi_j)$ with $j \le e$. Thus, KG is a product of field extensions $K(\xi_i) \otimes_K K(\xi_j)$ for some integers $0 \le i \le j \le e$. Since $K(\xi_i)/K$ is Galois and $K(\xi_i) \subset K(\xi_j)$, the tensor is the product of $[K(\xi_i) : K]$-copies of $K(\xi_j)$. This proves our assertion.

Since every irreducible KG-module is a factor $K(\xi_j)$ of KG, its completion $K_P \otimes_K K(\xi_j)$ is a simple K_PG-module if it is a field. Since there is only one prime of L over P, there is only one prime in its subfield $K(\xi_j)$. Therefore, $K_P \otimes K(\xi_j)$ is a field and hence a simple K_PG-module.

Lemma 55. *Let $\mathbb{Q}(\xi)$ be the p^e-th cyclotomic field. There exists a number field K and a prime P of K over p which is linearly disjoint from $\mathbb{Q}(\xi)$ but K_P is isomorphic to $\mathbb{Q}_p(\xi)$. In particular, the prime P splits completely in the Galois extension $K(\xi)$ of K.*

Proof. Let $\mathbb{Q}(\xi) = \mathbb{Q}[t]/(f(t))$, where f is a monic irreducible polynomial over $\mathbb{Q}$ of degree $d = \varphi(p^e)$. Consider the $\mathbb{Q}[x] = \mathbb{Q}[x_1, \dots, x_d]$-algebra $\mathbb{Q}(\xi)[x,t]/(F(x,t))$, where $x = (x_1, \dots, x_d)$ and $F(x,t) = t^d + x_1 t^{d-1} + \cdots + x_d$. Using the weak approximation and the Hilbert irreducibility, there is a specialization $x_0 \in \mathbb{Q}^d$, such that $F(x_0, t)$ is sufficiently close to $f(t)$ in the p-adic topology and $\mathbb{Q}(\xi)[t]/(F(x_0, t))$ is a field. Put $K := \mathbb{Q}[t]/(F(x_0, t))$. By Krasner's Lemma $K \otimes \mathbb{Q}_p \simeq \mathbb{Q}_p(\xi)$ and hence there is only prime P of K over p, particularly $K_P \simeq \mathbb{Q}_p(\xi)$. Also K is linearly disjoint from $\mathbb{Q}(\xi)$ over $\mathbb{Q}$, because $\mathbb{Q}(\xi)[t]/(F(x_0, t)) = \mathbb{Q}(\xi) \otimes_{\mathbb{Q}} K$.

Remark 56. (1) The reader may find a more general statement of Theorem 52 and Corollary 53 due to Heller in [10], Theorem 30.18. In loc. cit., $R_{(P)}$ is replaced by any DVR R, KG is replaced by any semisimple K-algebra, and $R_{(P)}G$ is replaced by any R-order.

(2) It is clear from the proof of Proposition 54 that the condition v_P extending uniquely to L is necessary, otherwise some simple KG-module would split after the completion at P. This necessary condition holds for some number field, for example $K = \mathbb{Q}$, because p is totally ramified in $\mathbb{Q}(\xi)$. On the other hand, this necessary condition may not hold for some number fields; see Lemma 55.

(3) It would be interesting to know whether Proposition 54 remains true if G is replaced by any finite p-group.

Proposition 57. *Let G be as in Proposition 54. A $\mathbb{Z}G$-module M is indecomposable if and only if the corresponding $\mathbb{Z}_pG$-module M_p is indecomposable.*

Proof. By Corollary 53, Propositions 46 and 54, we only need to show v_P has only one extension on $\mathbb{Q}(\xi)$, where ξ is a primitive p^e-th root of unity. This follows from the fact that (p) is totally ramified in $\mathbb{Q}(\xi)$.

Definition 58. Let $n(G)$ (resp. $n_{(p)}(G)$, $n_p(G)$) be the number of isomorphism classes of indecomposable $\mathbb{Z}G$ (resp. $\mathbb{Z}_{(p)}G$, $\mathbb{Z}_pG$)-modules.

Theorem 59. *Let G be as in Proposition 54. Suppose there are only finitely many isomorphism classes of indecomposable of $\mathbb{Z}_pG$-modules. Then there are only finitely many isomorphism classes of indecomposable of $\mathbb{Z}G$-modules.*

doi:10.6342/NTU201800167

Proof. Since v_p has only one extension of $\mathbb{Q}(\xi)$, $\mathbb{Q}$ is a splitting field for G relative to $\mathbb{Q}_p$ by Proposition 54. If $n_p(G)$ finite, then $n_{(p)}(G)$ is finite, by Theorem 52. Then we deduce from Theorem 42 that $n(G)$ is finite.

Theorem 60. *Let G be a cyclic group of order p^2. There are only finitely many isomorphism classes of indecomposable $\mathbb{Z}_pG$-modules. There are only finitely many isomorphism classes of indecomposable $\mathbb{Z}G$-modules.*

Proof. For the first statement, see [17] Theorem 3.1. The second statement follows from the first one and Theorem 59.

Theorem 61. *Let G be a cyclic p-group and $|G| \geq p^3$. There are infinitely many isomorphism classes of indecomposable $\mathbb{Z}_pG$-modules.*

Proof. See [18], Theorem, p. 327.

Remark 62. One can see Theorem 61 by Proposition 57 and Dade's Theorem (cf. [10] Theorem 33.8).

Theorem 63. *If G is a finite group such that a Sylow p-subgroup is not cyclic for some prime p, then $n(G)$ is infinite.*

Proof. See [17] Theorem 6.1.

Theorem 64. *Let G be a finite p-group. Then $n(G)$ is finite if and only if G is cyclic of order p^e for $e \leq 2$.*

Proof. This follows from Theorems 60, 61 and 63.

Theorem 65. *Let G be a finite p-group. Then $n_p(G)$ is finite if and only if G is cyclic of order p^e for $e \leq 2$.*

Proof. This follows from Theorems 60, 61 and Remark 73.

Suppose R is a commutative ring. We introduce relative projectivity in Section 2.1 for kG-modules. This notion can be defined for RG-modules in the same way, and Proposition 8 remains true. Namely, we have

Proposition 66. *Suppose H is a subgroup of G such that $|G/H|$ is invertible in R. Then every RG-module M is H-projective.*

Proof. See [43] Proposition 11.3.5.

For the following proposition one needs to assume that R is a complete discrete valuation ring as we need to apply the Krull-Schmidt-Azuyama Theorem in the proof.

Proposition 67. *Let R be a complete discrete valuation ring with the residue field of characteristic p. Let P be a Sylow p-subgroup of G. Then RG has finite representation type if and only if RP has finite representation type.*

Proof. ($\Rightarrow$): For an indecomposable RP-module V, we have $V|V \uparrow_P^G\downarrow_P^G$. Since RG has finite representation type and using Theorem 13 for any indecomposable RG-module U, the RP-module $U \downarrow_P^G$ has only finitely many indecomposable RP-summands. We have the ring RP must be of finite representation type.

($\Leftarrow$): By Proposition 66 we know every indecomposable RG-module is P-projective. Therefore, we have $U|V \uparrow_P^G$ for some indecomposable RP-module V. Again, by Theorem 13 and that there are only finitely many indecomposable RP-modules, RG is of finite representation type.

Lemma 68. *Let G be a finite group, and P a Sylow p-subgroup of G. Suppose there are infinitely many non-isomorphic indecomposable $\mathbb{Z}P$-modules $\{M_i\}$ such that their completions $(M_i)_p$ are all indecomposable $\mathbb{Z}_pP$-modules. Then $\mathbb{Z}G$ is not of finite representation type.*

Proof. The idea of proof follows from [17] Theorem 6.1. We prove by contradiction. By Theorem 42, the $\mathbb{Z}$-ranks of $\{M_i\}$ are unbounded. Suppose $n(G)$ is finite. Let $Y_1, \cdots, Y_m$

be full non-isomorphic indecomposable $\mathbb{Z}G$-modules and we have $\mathbb{Z}$-ranks of $\{Y_i\}$ are bounded. Write $M_i \uparrow_P^G = \oplus Y_j^{a_j}$. Then we have $M_i | \ M_i \uparrow_p^G \downarrow_P^G$. Passing to the completion, we have $(M_i)_p | \ \oplus_j (Y_j)_p^{a_j} \downarrow_P^G$. Since $(M_i)_p$ is indecomposable and $\mathbb{Z}_p$ is a complete discrete valuation ring , by Theorem 13, we have $(M_i)_p | \ (Y_j)_p \downarrow_P^G$ for some j. However, since the $\mathbb{Z}_p$-rank of $(M_i)_p$ is unbounded, $\mathbb{Z}$-ranks of $\{Y_i\}$ are unbounded. This contradicts with that $\mathbb{Z}$-ranks of $\{Y_i\}$ are bounded. Therefore, $n(G)$ is infinite.

Theorem 69. *Suppose G is a finite group, then $n(G)$ is finite if and only if $n_p(G)$ is finite for each prime number p such that $p \mid |G|$.*

Proof. For the implication ($\Leftarrow$), see [21] Theorem 8. For the other implication ($\Rightarrow$), by Proposition 67, $n_p(G)$ is finite if and only if $n_p(P)$ is finite, where P is a p-Sylow subgroup of G. Assume $n_p(P)$ is not finite, proving by contradiction, and then we need to show $n(G)$ is finite. By Lemma 68, it suffices to construct a family $\{M_i\}$ of non-isomorphic indecomposable non-isomorphic $\mathbb{Z}P$-modules such that $(M_i)_p$ remains $\mathbb{Z}_pP$-indecomposable for all M_i. By Theorem 65, P divides into two cases: P non-cyclic and P cyclic of order p^e with $e \geq 3$. If P is non-cyclic, $C_p \times C_p$ is a homomorphic image of P (cf. Theorem 22). Therefore, any indecomposable $\mathbb{Z}C_p \times C_p$-module is also an indecomposable $\mathbb{Z}P$-module. We reduce non-cyclic P to $C_p \times C_p$.

For P a cyclic group of order p^e with $e \geq 3$, by Theorem 61, we have $\{M_i\}$, a set of non-isomorphic indecomposable $\mathbb{Z}P$-modules. By Proposition 57, each M_i remains indecomposable after completion.

For $P = C_p \times C_p$, by Proposition 72, we have $\{M'_{2n+1}\}$, a set of non-isomorphic $\mathbb{Z}P$-indecomposable modules. By Remark 73, $(M'_{2n+1})_p$ is an indecomposable $\mathbb{Z}_pP$-module.

We also give another proof for $P = C_p \times C_p$ when $p \geq 5$. Let θ be a p-primitive root of unity, and $\mathfrak{p}$ be the prime ideal of $\mathbb{Z}[\theta]$ lying over (p). Since (p) is totally ramified, we have $\mathbb{Z}_p[\theta] = \mathbb{Z}[\theta]_{\mathfrak{p}}$. Besides, $\mathbb{Z}[\theta]C_p$ is a homomorphic image of $\mathbb{Z}C_p \times C_p$. Since $\mathbb{Q}(\theta)C_p \cong \mathbb{Q}(\theta)^p$ and $p \geq 5$, by Dade's Theorem (see [10] Theorem 33.8), we have $\{M_i\}$, a family of non-isomorphic indecomposable $\mathbb{Z}[\theta]C_p$-modules, therefore, non-isomorphic indecomposable $\mathbb{Z}C_p \times C_p$-modules. Moreover, by Proposition 54, $\mathbb{Q}(\theta)$ is a splitting field for C_p relative to $\mathbb{Q}(\theta)_{\mathfrak{p}}$. By Proposition 46 and Corollary 53, $\mathbb{Z}[\theta]_{\mathfrak{p}} \otimes M_i$ is $\mathbb{Z}[\theta]_{\mathfrak{p}}C_p$-indecomposable, therefore, $\mathbb{Z}_p[\theta]C_p$-indecomposable. Consequently, we have a family of non-isomorphic indecomposable $\mathbb{Z}C_p \times C_p$-modules such that the completions of them are still $\mathbb{Z}_pC_p \times C_p$-indecomposable.

Remark 70. By Theorem 65, Proposition 67 and Theorem 69, we have that given a finite group G, $n(G)$ is finite if and only if for each prime $p \mid |G|$, a Sylow p-subgroup of G is cyclic of order p or p^2.

3.4 Infinitely many indecomposable lattices

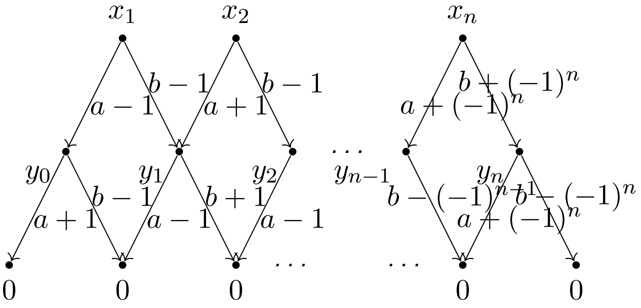
Let $G = C_p \times C_p = \langle a \rangle \times \langle b \rangle$. In this section we construct infinitely many indecomposable $\mathbb{Z}G$-modules. We follow [17] when $p = 2$, and modify it for other prime numbers.

Proposition 71. *Let $p = 2$. Let M'_{2n+1} be a free $\mathbb{Z}$-module with basis $\{x_1, \cdots, x_n, y_0, y_1, \cdots, y_n\}$. Define the action of $G = C_p \times C_p$ by*

$$(a + (-1)^i)x_i = y_{i-1}, \ (b + (-1)^i)x_i = y_i,$$
$$(a + (-1)^i)y_i = (b - (-1)^i))y_i = 0.$$

Or more explicitly,

$$\begin{aligned}
&(a-1)x_i = y_{i-1}, \quad \textit{for } i \textit{ is odd}, \; (a+1)x_i = y_{i-1}, \; \textit{for } i \textit{ is even},\\
&(b-1)x_i = y_i, \qquad \textit{for } i \textit{ is odd}, \; (b+1)x_i = y_i, \; \textit{for } i \textit{ is even},\\
&(a-1)y_i = 0, \qquad \textit{for } i \textit{ is odd}, \; (a+1)y_i = 0, \; \textit{for } i \textit{ is even},\\
&(b-1)y_i = 0, \qquad \textit{for } i \textit{ is even}, \; (b+1)y_i = 0, \; \textit{for } i \textit{ is odd}.
\end{aligned}$$



Then M'_{2n+1} is an indecomposable $\mathbb{Z}G$-module.

Proof. We need to check the action defined above is well defined. Therefore, we need to check M'_{2n+1} is annihilated by (a^2-1) and (b^2-1), and this is clear. Also we need to check $abx = bax$, for $x \in M'_{2n+1}$. This can be seen from $(a+(-1)^i)(b-(-1)^i)x_i = (b-(-1)^i)(a+(-1)^i)x_i$, so $abx_i = bax_i$. Also, $aby_i = bay_i$ is clear. Hence M'_{2n+1} is a $\mathbb{Z}G$-module.

Observe that $M'_{2n+1}/2M'_{2n+1}$ is the same as the $\mathbb{F}_2G$-module M_{2n+1} defined in Section 2.2. If M'_{2n+1} decomposes into $N_1 \oplus N_2$ as $\mathbb{Z}G$-modules, then $M_{2n+1} = M'_{2n+1} \otimes \mathbb{F}_2 = N_1 \otimes \mathbb{F}_2 \oplus N_2 \otimes \mathbb{F}_2$ as $\mathbb{F}_2G$-modules. Then M'_{2n+1} is an indecomposable $\mathbb{Z}G$-module.

Now we want to construct indecomposable $\mathbb{Z}G$-modules for $p \geq 3$. Let θ be a primitive p-th root of unity, and let $G = C_p \times C_p = \langle a \rangle \times \langle b \rangle$. Let M'_{2n+1} be a free $\mathbb{Z}[\theta]$-module with basis $\{x_1, \cdots, x_n, y_0, y_1, \cdots, y_n\}$. Define the action of G on M'_{2n+1} by

$$
\begin{aligned}
(a-\theta^2)x_i &= y_{i-1},\ \textit{for } i \textit{ is odd},\\
(b-\theta^2)x_i &= y_i,\ \textit{for } i \textit{ is odd},\\
(a-\theta)x_i &= y_{i-1},\ \textit{for } i \textit{ is even},\\
(b-\theta)x_i &= y_i,\ \textit{for } i \textit{ is even, and}\\
ay_i &= \begin{cases} \theta y_i, & \textit{for } i \textit{ is even},\\ \theta^2 y_i, & \textit{for } i \textit{ is odd}, \end{cases}\\
by_i &= \begin{cases} \theta^2 y_i, & \textit{for } i \textit{ is even},\\ \theta y_i, & \textit{for } i \textit{ is odd}. \end{cases}
\end{aligned}
$$

The diagram of this $\mathbb{Z}[\theta]G$-module is similar to the diagram in Proposition 71. Observe that $M'_{2n+1}/\mathfrak{p}M'_{2n+1} \cong M_{2n+1}$, where M_{2n+1} is defined in Section 2.2 and $\mathfrak{p} = (\theta - 1)$ is the unique prime ideal in $\mathbb{Z}[\theta]$ lying over (p). Since M'_{2n+1} is a free $\mathbb{Z}[\theta]$-module and $M'_{2n+1}/\mathfrak{p}M'_{2n+1}$ is $\mathbb{F}_pG$-indecomposable, M'_{2n+1} is an indecomposable $\mathbb{Z}[\theta]G$-module.

Via the inclusion $\iota : \mathbb{Z}G \to \mathbb{Z}[\theta]G$, we may regard M'_{2n+1} as a $\mathbb{Z}G$-module.

Proposition 72. *The $\mathbb{Z}G$-module M'_{2n+1} contains an indecomposable $\mathbb{Z}G$-submodule of $\mathbb{Z}$-rank greater than or equal to $2n+1$. In particular, there are infinitely many indecomposable $\mathbb{Z}G$-modules $\{M_i\}$ whose $\mathbb{Z}$-ranks are unbounded.*

PROOF. Suppose $M'_{2n+1} = N_1 \oplus \cdots \oplus N_r$ decomposes into indecomposable $\mathbb{Z}G$-modules. By Proposition 54 and Corollary 53, their completions $(N_i)_p$ are indecomposable $\mathbb{Z}_pG$-modules. Since $\mathfrak{p}(M'_{2n+1})_p$ is a $\mathbb{Z}_pG$-submodule, we have $M_{2n+1} = M'_{2n+1}/\mathfrak{p}M'_{2n+1} = \oplus(N_i)_p/\mathfrak{p}(M'_{2n+1})_p$. Since M_{2n+1} is $\mathbb{F}_pG$-indecomposable, after a suitable change of order of factors, we have $(N_1)_p/\mathfrak{p}(M'_{2n+1})_p = M_{2n+1}$ and $(N_i)_p/\mathfrak{p}(M'_{2n+1})_p = 0$ for all $i > 1$. Then the $\mathbb{Z}$-rank of N_1 is $\dim_{\mathbb{F}_p} N_1/pN_1 \geq \dim_{\mathbb{F}_p}(N_1)_p/\mathfrak{p}(M'_{2n+1})_p = 2n+1$. N_1 is a desired submodule.

Remark 73. By Proposition 54 and Corollary 53, the completions $\{(M_i)_p\}$ of indecomposable $\mathbb{Z}G$-modules in Proposition 72 are $\mathbb{Z}_pG$-indecomposable. We shall prove that M'_{2n+1} is not $\mathbb{Z}G$-indecomposable in general.

Here is another construction of infinitely many $\mathbb{Z}C_p \times C_p$-modules when $p = 3$. Similar to Proposition 72, we consider a $\mathbb{Z}[\theta]G$-module first.

Let θ be a primitive root of $X^3 - 1$, therefore $\theta^2 + \theta + 1 = 0$. Let $G = \langle a \rangle \times \langle b \rangle$, where orders of a and b are 3. Let N'_{2n+1} be a $\mathbb{Z}[\theta]G$-module, generated by x_i, for $i = 1, \cdots, n$. Define

$$(a - \theta^j)x_i = y_{i,j},\ (b - \theta^j)x_i = z_{i,j}.$$

The $\mathbb{Z}[\theta]$-module X (the free $\mathbb{Z}[\theta]$-module with basis $\{x_i\}$) is the first floor of N'_{2n+1}, and $Y + Z$ is the second floor. The third is not clear yet. (The different floors have no intersection.)

Replacing N'_{2n+1} by a quotient of N'_{2n+1} if necessary, we may require that N'_{2n+1} is annihilated by $(a^2 + a + 1)$ and $(b^2 + b + 1)$. Then $(a - \theta)^2 = a^2 - 2\theta a + \theta^2 = (a^2 + a + 1) + (-2\theta a - a - 1 + \theta^2) = (a^2 + a + 1) + [(-2\theta - 1)(a - \theta) - (\theta^2 + \theta + 1)]$. Therefore,

$$\begin{aligned}(a-\theta)y_{i,1} = (a-\theta)^2 x_i &= (a^2+a+1)x_i + (-2\theta-1)(a-\theta)x_i - (\theta^2+\theta+1)x_i \\ &= (-2\theta-1)y_{i,1} - (\theta^2+\theta+1)x_i = -(2\theta+1)y_{i,1}. \qquad (3.1)\end{aligned}$$

Thus, we must define $(a - \theta)y_{i,1}$ using (3.1). Using a similar way to calculate other terms, and then we should define $(a - \theta^2)y_{i,2} = (2\theta + 1)y_{i,2}$.

Since $(a - \theta^j)x_i = y_{i,j}$, we have $ax_i = y_{i,1} + \theta x_i = y_{i,2} + \theta^2 x_i$. Therefore, we get $y_{i,2} = y_{i,1} + (\theta - \theta^2)x_i$. Doing the same for $z_{i,2}$, we only consider the actions on $y_{i,1}$ and

$z_{i,1}$. If we identify $z_{i-1,1}$ and $y_{i,1}$, then we get the following relations:

$$(a-\theta)z_{i,1} = (a-\theta)y_{i+1,1} = -(2\theta+1)y_{i+1,1} = -(2\theta+1)z_{i,1}, \ for\ 1 \leq i < n,$$
$$(b-\theta)y_{i,1} = (b-\theta)z_{i-1,1} = -(2\theta+1)z_{i-1,1} = -(2\theta+1)y_{i,1}, \ for\ 1 < i,$$
$$(a-\theta)z_{n,1} = (a-\theta)(b-\theta)x_n = (b-\theta)(a-\theta)x_n = (b-\theta)y_{n,1} = -(2\theta+1)y_{n,1},$$
$$(b-\theta)y_{1,1} = (b-\theta)(a-\theta)x_1 = (a-\theta)(b-\theta)x_1 = (a-\theta)z_{1,1} = -(2\theta+1)z_{n,1}.$$

Since $\mathbb{Z}[\theta]/(1-\theta) = \mathbb{F}_3$, we have $2\theta+1=0$ in $\mathbb{F}_3$, and hence $N'_{2n+1}/(1-\theta)N'_{2n+1} = M_{2n+1}$. Thus, N'_{2n+1} is $\mathbb{Z}[\theta]G$-indecomposable. Via the inclusion $\iota : \mathbb{Z}G \to \mathbb{Z}[\theta]G$, again we regard N'_{2n+1} as a $\mathbb{Z}G$-module.

Proposition 74. *The $\mathbb{Z}G$-module N'_{2n+1} contains an indecomposable $\mathbb{Z}G$-module N with $\mathbb{Z}$-rank $\geq 2n+1$.*

Proof. The proof is similar to that of Proposition 72.

We now give an example that M'_{2n+1} is a decomposable $\mathbb{Z}G$-module. Take $n=2$ and $p=3$. The $\mathbb{Z}$-rank of M'_5 is $(2n+1)(p-1) = 10$. Let N_1 be the $\mathbb{Z}G$-submodule of M'_{2n+1} generated x_1 and x_2. Since M'_{2n+1} is annihilated by $(a-\theta)(a-\theta^2) = a^2+a+1$ and b^2+b+1, it is actually a $\mathbb{Z}[\theta][a,b]/(a^2+a+1, b^2+b+1)$-module. Also $\mathbb{Z}[a,b]/(a^2+a+1, b^2+b+1) = \mathbb{Z}\langle 1, (a-1), (b-1), (a-1)(b-1)\rangle$. Therefore, N_1 is generated by elements $x_1, x_2, (a-1)x_1, (b-1)x_1, (a-1)(b-1)x_1, (a-1)x_2, (b-1)x_2, (a-1)(b-1)x_2$

doi:10.6342/NTU201800167

over $\mathbb{Z}$. We compute all of them:

$$\begin{aligned}
(a-1)x_1 &= (a-\theta)x_1 + (\theta-1)x_1 = y_0 + (\theta-1)x_1,\\
(b-1)x_1 &= (b-\theta)x_1 + (\theta-1)x_1 = y_1 + (\theta-1)x_1,\\
(a-1)(b-1)x_1 &= (a-1)(y_1 + (\theta-1)x_1) = (a-1)y_1 + (\theta-1)(y_0 + (\theta-1)x_1)\\
&= (\theta-1)y_1 + (\theta-1)y_0 - 3\theta x_1,\\
(a-1)x_2 &= (a-\theta^2)x_2 + (\theta^2-1)x_2 = y_1 + (-\theta-2)x_2,\\
(b-1)x_2 &= (b-\theta^2)x_2 + (\theta^2-1)x_2 = y_2 + (-\theta-2)x_2,\\
(a-1)(b-1)x_2 &= (a-1)(y_2 + (-\theta-2)x_2) = (a-1)y_2 + (-\theta-2)(y_1 + (-\theta-2)x_2)\\
&= (-\theta-2)y_2 + (-\theta-2)y_1 + (3\theta+3)x_2.
\end{aligned}$$

Note that $(\theta-1)^2 = \theta^2 - 2\theta + 1 = -3\theta$ and $(\theta+2)^2 = \theta^2 + 4\theta + 4 = (3\theta+3)$. On the other hand, let N_2 be the $\mathbb{Z}G$-submodule generated by y_1. We have $a \cdot y_1 = \theta y_1$ and $b \cdot y_1 = \theta^2 y_1 = (-\theta-1)y_1$. Then $N_2 = \langle y_1, \theta y_1 \rangle_{\mathbb{Z}}$. Now it is easy to see that the 8 $\mathbb{Z}$-generators of N_1 and 2 $\mathbb{Z}$-generators of N_2 form a $\mathbb{Z}$-basis for M_5'. This shows that $M_5' = N_1 \oplus N_2$ decomposes into two indecomposable $\mathbb{Z}G$-modules.

doi:10.6342/NTU201800167

Chapter 4

Integral representations of specific finite groups

According to Theorem 69, given an arbitrary finite group G, we know precisely when $\mathbb{Z}G$ is of finite representation type with respect to $\mathbb{Z}G$-lattices. As a remainder, $\mathbb{Z}G$-modules in this chapter will be meant to be $\mathbb{Z}G$-lattices (cf. Definition 38 and Section 3.3). We describe integral representations of cyclic groups of order p and dihedral groups of order $2p$ with p a prime number. Our references are Reiner [33] and Lee [30]. At the end of this chapter, we use results of Lee [30] to discuss integral representations of $S_3 = D_3$ in more details.

4.1 Cyclic groups of prime order

This section states the main theorem of [33] without proof. We only consider integral representations. Let p be a prime number, $\mathfrak{o}$ the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\theta)$, where θ is a primitive p-th root of unity. Let $\Phi_p(X) = X^{p-1} + \cdots + 1$. Let G be a cyclic group generated by g of order p and $\mathbb{Z}G$ be its group ring. Let $s = \Phi_p(g) = 1 + g + \cdots + g^{p-1}$.

doi:10.6342/NTU201800167

Suppose M is an integral representation of $\mathbb{Z}G$. Consider a submodule M_0 of M,

$$M_0 = \{m \in M : sm = 0\},$$

and M_0 can be viewed as a $\mathbb{Z}G/(s) \cong \mathfrak{o}$-module. Suppose for some $m \neq 0 \in M_0$, and $f(g)m = 0$, for some $f(X) \in \mathbb{Z}[X]$. Since $sm = 0$, we may assume $\deg(f) \leq \deg(\Phi_p)$. Since $\Phi_p(X)$ is irreducible in $\mathbb{Z}[X]$, we have $f(X) = n$ or $n\Phi_p(X)$; otherwise, $f(X)g(X) + h(X)\Psi_p(X) = m$ for some integer m and $g(X),\ h(X) \in \mathbb{Z}[X]$. The former is impossible, since $m \neq 0$. Consequently, M_0 is $\mathfrak{o}$-torsion free. Therefore M_0 is $\mathfrak{o}$-isomorphic to

$$\mathfrak{o} \oplus \cdots \oplus \mathfrak{o} \oplus \mathfrak{a}, \tag{4.1}$$

with n direct summands, $\mathfrak{a}$ an element of ideal class of $\mathfrak{o}$. Observe that as $\mathfrak{o}$-modules, we have

$$M_0 \supset (g-1)M \supset (g-1)M_0 = (\theta - 1)M_0.$$

Since $M_0 \cong \mathfrak{o} \oplus \cdots \oplus \mathfrak{o} \oplus \mathfrak{a}$ and $(g-1)M$ is its submodule, $(g-1)M \cong \mathfrak{e}_1 \oplus \cdots \oplus \mathfrak{e}_n\mathfrak{a}$ for some integral $\mathfrak{o}$-ideals $\mathfrak{e}_1, \ldots, \mathfrak{e}_n$. Also since $(g-1)M \supset (\theta-1)M_0$, we have $\mathfrak{e}_i$ can only be $\mathfrak{o}$ or $(\theta - 1)$ for each i. Assume there are precisely r elements of $\{\mathfrak{e}_i\}$ such that $\mathfrak{e}_i = \mathfrak{o}$. After permutation of the order, we let B be

$$(g-1)M/(\theta-1)M_0 = \mathfrak{o}/(\theta-1) \oplus \cdots \oplus \mathfrak{o}/(\theta-1) \cong \mathbb{F}_p \oplus \cdots \oplus \mathbb{F}_p,$$

with r direct summands. The last isomorphism follows from that p is totally ramified in $\mathbb{Q}(\theta)$ and $p\mathfrak{o} = (1-\theta)^{p-1}$. Consider M/M_0, a $\mathbb{Z}$-free module. Hence we have $M = M_0 \oplus X$

as $\mathbb{Z}$-modules, for some $X \cong M/M_0$ as $\mathbb{Z}G$-modules. Then this gives us

$$(g-1)M = (g-1)M_0 + (g-1)X \tag{4.2}$$

$$= (\theta-1)M_0 + (g-1)X. \tag{4.3}$$

Note that this may not be a direct sum. By (4.3), we have a *surjective* $\mathbb{Z}$-linear map $\phi : X \to B$ defined by

$$\phi(x) = \overline{(g-1)x},\ x \in X.$$

Therefore given $x \in X$, we have

$$(g-1)x \equiv a_1\bar{\beta}_1 + \ldots + a_r\bar{\beta}_r \bmod (1-\theta)M_0,\ a_i \in \mathbb{F}_p.$$

Since M/M_0 is a free $\mathbb{Z}$-module, we may assume that it is of rank m with basis $\{x_i\}$. Moreover, since ϕ is surjective, we can choose $\{x_i\}$ such that $\{\phi(x_1),\ \cdots,\ \phi(x_r)\}$ is linearly independent, and we have $m \geq r$. By changing the basis, we may assume

$$\phi(x_i) = c_i\bar{\beta}_i,\ c_i \in \mathbb{F}_p,$$

$$c_i \neq 0 \text{ when } 1 \leq i \leq r, \text{ and } c_i = 0 \text{ when } r < i \leq m.$$

Therefore, we have $(g-1)x_i = c_i\beta_i + (g-1)u_i,\ u_i \in M_0$. Let $y_i = x_i - u_i$, then $(g-1)y_i = c_i\beta_i$. Since $M = M_0 \oplus X$ as $\mathbb{Z}$-modules, we have

$$M = M_0 \oplus Y = M_0 \oplus \mathbb{Z}y_1 \oplus \cdots \oplus \mathbb{Z}y_m,$$

and

$$gy_i = y_i + c_i\beta_i,\ gm = \theta m,\ m \in M_0.$$

Furthermore, we may assume (cf. [33], Lemma 4), $c_i = 1,$ for $1 \leq i \leq r$.

doi:10.6342/NTU201800167

Theorem 75. *Suppose M is an integral representation of $\mathbb{Z}G$. Let n be the $Z[\theta]$-rank of M_0, $\mathfrak{a}$ in (4.1) , r the dimension of $(g-1)M/(\theta-1)M_0$, and m the $\mathbb{Z}$-rank of M/M_0. Then m, n, r and $\mathfrak{a}$ (with restrictions $r \leq m,\ r \leq n$) are invariants of M and determine M uniquely. We may write $M = M_0 \oplus \mathbb{Z}y_1 \oplus \cdots \mathbb{Z}y_r \oplus \cdots \oplus \mathbb{Z}y_m$ as $\mathbb{Z}$-modules. The action of G on M is defined by*

$$gy_i = y_i + \beta_i, 1 \leq i \leq r,$$

$$gy_j = y_j, r+1 \leq j \leq m,$$

$$gm = \theta m,\ \ m \in M_0.$$

Proof. See [33], Theorem, p. 145.

Corollary 76. *The indecomposable $\mathbb{Z}G$-modules are described as in Theorem 75 with $(r,\ m,\ n) = (0,\ 1,\ 0)$ or $(0,\ 0,\ 1)$ or $(1,\ 1,\ 1)$. Hence the number of non-isomorphic indecomposable $\mathbb{Z}G$-modules is $2h+1$, where h is the class number of $\mathbb{Z}[\theta]$.*

Proof. See [33], Corollary, p. 145.

Example 77. Let $G = \langle g \rangle$ be a cyclic group of order 2. Using Theorem 75 and Corollary 76, we find out all $\mathbb{Z}G$-indecomposable modules. Our θ, the primitive 2-th root of unity, equals to -1.

(1) For $(r,\ m,\ n) = (0,\ 1,\ 0)$, we have $M_0 = 0$, $M = 0 \oplus \mathbb{Z}y = \mathbb{Z}y$, $B = (g-1)M/(\theta-1)M_0 = 0$. By Theorem 75, we have $g \cdot y = y$. This is the trivial representation of G, denoted by $\mathbb{Z}$.

(2) For $(r,\ m,\ n) = (0,\ 0,\ 1)$, we have $M_0 = \mathbb{Z}$, $(g-1)M = (\theta-1) = (2)$, $M = M_0 = \mathbb{Z}x$, and $(g+1) \cdot x = 0$. Therefore, we have $g \cdot x = -x$, and denote M by $\mathbb{Z}'$.

(3) For $(r,\ m,\ n) = (1,\ 1,\ 1)$, we have $M_0 = \mathbb{Z}$, $(g-1)M = \mathbb{Z} = M_0$, and $M = M_0 \oplus \mathbb{Z}y = \mathbb{Z}x \oplus Zy$. If we pick $\beta = x$, then $g \cdot x = -x, g \cdot y = y + x$. Letting $e_1 = y$ and $e_2 = x + y$, we have $g \cdot e_1 = e_2$ and $g \cdot e_2 = e_1$, and denote M by L.

doi:10.6342/NTU201800167

These 3 integral representations of $G = C_2$ will be used in Section 4.2.

4.2 Dihedral groups of order $2p$

Let $p \neq 2$ be a prime. In the following, we state some results of integral representations of dihedral groups of order $2p$. Our reference is Lee [30].

Let $S = \mathbb{Z}$ or $\mathbb{Z}_{(2p)} = \{\frac{n}{m} | n, m \in \mathbb{Z}$ for $k \nmid m, k = 2$ and $p\}$. Let θ be a primitive p-th roots of unity, K the field $\mathbb{Q}(\theta)$ and K_0 the field $\mathbb{Q}(\theta + \bar{\theta})$, where $\bar{\theta}$ is the conjugate of θ. Let R and R_0 be the integral closures of S in K and K_0. Let $G = \langle a, b \rangle$, where $a^2 = b^p = e$, and $ab = b^{p-1}a$.

Let $\mathrm{Aut}(K/K_0) = \langle \alpha \rangle \cong C_2$. Let $\Lambda = R \circ C_2$ be a twisted group ring (cf. Definition 35). Note that R_0 is fixed by α, and hence Λ is an R_0-algebra via $\phi : R_0 \to \Lambda$, where $1 \mapsto 1$. However, Λ is not an R-algebra. Let $\Lambda_{\mathbb{Q}} := \mathbb{Q} \otimes_{\mathbb{Z}} \Lambda$, and then $\Lambda_{\mathbb{Q}}$ is a K_0-algebra. Moreover, $\Lambda_{\mathbb{Q}}$ is isomorphic to $M_2(K_0)$ (cf. [10] Example 28.3).

The following is the motivation for studying projective Λ-modules of finite R-rank.

At first, SG is the twisted group ring $S[b] \circ C_2$, where $C_2 = \langle a \rangle$ and C_2 acts on $S[b]$ by $a(b) = aba^{-1} = b^{p-1}$ and $a(1) = 1$ (cf. Definition 35). Let $\Psi_p(X) = X^{p-1} + X^{p-2} + \ldots + 1$, the cyclotomic polynomial of degree $p - 1$. We have that

$$SG/\Psi_p(b)SG \cong \Lambda \text{ by } a \mapsto \alpha \text{ and } b \mapsto \theta.$$

Suppose M is a finitely generated S-free SG-module. Consider the submodule

$$M_0 = \{m \in M : \Psi_p(b)m = 0\},$$

and we can regard M_0 as an $SG/\Psi_p(b)SG \cong \Lambda$-module. This is a finitely generated, R-torsion free module, hence an R-projective module. By Proposition 78, M_0 is Λ-

doi:10.6342/NTU201800167

projective. Since M/M_0 is annihilated by $(b-1)$, M/M_0 is an $S[a]$-module. Hence M is an extension of M/M_0 by M_0.

In [30], it is proved that the number of isomorphism classes of indecomposable $\mathbb{Z}G$-modules is related to the class number of R_0. We describe this relation between an S-free SG-indecomposable module and an ideal of R_0 briefly.

Given an SG-module M, the module M is an extension of an $S[a]$-module M/M_0 by M_0, which is a Λ-module. Hence, we need to study Λ-modules M_0, $S[a]$-modules M/M_0 and extensions of M/M_0 by M_0.

Consider $\phi : R \to \Lambda, 1 \mapsto 1$, the natural map, and ϕ is a ring homomorphism. Hence a Λ-module can be regarded as an R-module.

Proposition 78. *Every R-projective Λ-module is Λ-projective.*

Proof. See [30] Proposition 1.1.

Definition 79. A ring R is said to be a *left hereditary* ring if every left ideal of R is a left projective R-module.

Proposition 80. *The ring Λ is a left hereditary ring.*

Proof. See [30] Proposition 1.2.

Proposition 81. *Suppose Γ is a left hereditary ring. Then any Γ-projective module is Γ-isomorphic to an external direct sum of left ideals of Γ.*

Proof. See [10] Proposition 4.3.

By Propositions 80, 81 we have that any Λ-projective module is Λ-isomorphic to an external direct sum of left ideals of Λ. Since Λ is an R-free module of rank 2, the submodules of Λ are of R-rank 1 or 2. Ideals of Λ which are of R-rank two are Λ-isomorphic to direct sums of two R-rank one ideals of Λ (see [30] Theorem 1.1). Hence any Λ-projective module is isomorphic to an external direct sum of left ideals of R-rank 1 of Λ.

doi:10.6342/NTU201800167

Definition 82. An R-ideal I in K is said to be *ambiguous* if $I = \bar{I}$.

Suppose I is an ambiguous ideal in K. If $x \in I$, we have $\bar{x} \in I$. Therefore, we may regard I as a Λ-module of R-rank 1 by defining $\alpha \cdot x = \bar{x}$ for $x \in I$.

Proposition 83. *Two ambiguous ideals I_1 and I_2 of K are Λ-isomorphic if and only if $I_1 = xI_2$ for some $x \in K_0^{\times}$.*

Proof. If I_1 is Λ-isomorphic to I_2, then it is R-isomorphic to I_2. We have $I_1 = xI_2$ for some $x \in K^{\times}$. Since I_1 and I_2 are Λ-isomorphic, we have $x(a \cdot y) = \alpha \cdot (xy)$, $\forall y \in I_2$. Therefore, we have $x\bar{y} = \overline{xy}$, so $x \in K_0^{\times}$. The converse is clear.

Proposition 84. *The set of isomorphism classes of left ideals of Λ of R-rank 1 is in bijection with that of $K_0^{\times}$-equivalence classes of fractional ambiguous ideals of K.*

Proof. Suppose I is an ambiguous ideal in K. We know that I can be viewed as a Λ-module of R-rank 1. Since I is R-torsion free, I is R-projective, therefore, Λ-projective. By Proposition 81, it is Λ-isomorphic to a left ideal of Λ.

Conversely, suppose L is a left ideal of Λ of R-rank one, and then $L_{\mathbb{Q}}$ is a left ideal of $\Lambda_{\mathbb{Q}}$ of K-rank one. Recall that we have an isomorphism $\Lambda_{\mathbb{Q}} \cong M_2(K_0)$. Hence $L_{\mathbb{Q}}$ is a simple $\Lambda_{\mathbb{Q}}$-module. We can embedd $K \hookrightarrow \Lambda_{\mathbb{Q}}$ as $\Lambda_{\mathbb{Q}}$-modules by sending r to $r \cdot (1 + \alpha)$. Since any two simple modules over $\Lambda_{\mathbb{Q}}$ are isomorphic, we have a $\Lambda_{\mathbb{Q}}$-isomorphism $L_{\mathbb{Q}} \simeq K$. Therefore, we have $L \hookrightarrow K$ as a Λ-embedding; hence L is Λ-isomorphic to an ambiguous ideal of K. By Proposition 83, two ambigiuous ideals of R are Λ-isomorphic if and only if they are $K_0^{\times}$-equivalent. The proof is complete.

Proposition 85. *An ideal I in R is ambiguous if and only if I can be written as the form $(1-\theta)^{\varepsilon}WR$, where W is an ideal of R_0 and $\varepsilon = 0$ or 1.*

Proof. Suppose I is an ambiguous ideal of R. We can decompose I into a product of prime ideals, say, $I = Q_1Q_2 \cdots Q_r$. Since $\bar{I} = I$, Q_i breaks into 2 cases. For some Q_i, there exists Q_j in the decomposition of I such that $Q_j = \overline{Q_i}$, and the other $Q_i = \overline{Q_i}$. We may write I as $(Q_1\bar{Q_1})\cdots(Q_m\bar{Q_m})(Q_{2m+1}\cdots Q_r)$, where the first $2m$ factors are of the first case and the remnants of the factors are of the second case. Note that since $\mathbb{Q}(\theta)$ is a field extension of K_0 of degree 2, given an ideal P of R_0, we have that

$$PR = \begin{cases} Q\bar{Q} & \text{, if P is split,} \\ Q^2 & \text{, if P is ramified,} \\ Q & \text{, if P is inert.} \end{cases}$$

Also since K is the p-th cyclotomic extension, we have that P is ramified only if P is the prime ideal lying over (p). The prime ideal lying over ramified P is $(1-\theta)$. For $2m+1 \leq i \leq r$, Q_i is either ramified or inert. So we have that

$$I = P_1 \cdots P_m P_{2m+1} \cdots P_n (1-\theta)^{r-n} R = (1-\theta)^{\varepsilon} W R,$$

where $\varepsilon = 1$ if $r-n$ is odd and $\varepsilon = 0$ if $r-n$ is even.

On the other hand, consider $(1-\theta^i)/(1-\theta^j)$ where $ij \neq 0 \pmod{p}$. Since p is a prime number, we have $mj + np = i$ for some m and $n \in \mathbb{Z}$. Therefore, we have

$$(1-\theta^i) = 1 - \theta^{mj}\theta^{np} = 1 - \theta^{mj} = (1-\theta^j)(1-(\theta^j)^2 + \cdots + (\theta^j)^{m-1}).$$

Consequently, $(1-\theta^i)/(1-\theta^j) \in R$. Similarly for its inverse, hence $(1-\theta^i)/(1-\theta^j)$ is a unit of R. Also since θ is a unit of R, the element $(\theta-\bar{\theta})/(1-\theta) = \theta(1-\theta^{p-2})/(1-\theta)$ is a unit of R. Hence $(1-\theta)^{\varepsilon}WR = (\theta-\bar{\theta})^{\varepsilon}WR$, and $(\theta-\bar{\theta})^{\varepsilon}WR$ is obvious an ambiguous ideal of R.

Proposition 86. *Two ambiguous ideals $(1-\theta)^{\varepsilon}WR$ and $(1-\theta)^{\varepsilon'}W'R$ are Λ-isomorphic if and only if $\varepsilon = \varepsilon'$ and W and W' are in the same ideal class of R_0.*

Proof. By Proposition 83, two ambiguous ideals $(1-\theta)^{\varepsilon}WR$ and $(1-\theta)^{\varepsilon'}W'R$ are Λ-isomorphic $\Leftrightarrow$ $(1-\theta)^{\varepsilon}WR = x(1-\theta)^{\varepsilon'}W'R$ for some $x \in K_0^{\times}$. Multiplying both sides by a non-zero element of R_0, we may assume $x \in R_0$. Also we have that $xR = (1-\theta)^m X$, where X is a coprime-to-$(1-\theta)$ ideal of R and m is even. Therefore, we have $\varepsilon = \varepsilon'$. Further, we have $WR = xW'R$. Since the homomorphism $\iota : I(R_0) \to I(R)$ is injective, where $I(R_0)$ is the ideal group of R_0 and $I(R)$ is the ideal group of R, we have $W = xW'$. Therefore, $(1-\theta)^{\varepsilon}WR = x(1-\theta)^{\varepsilon'}W'R \Leftrightarrow \varepsilon = \varepsilon'$ and W and W' are in the same ideal class of R_0.

Theorem 87. *Let h be the class number of R_0. There are $2h$ non-isomorphic, indecomposable, projective, Λ-modules of R-rank 1.*

Proof. Suppose M is a projective and indecomposable Λ-module of R-rank 1. Then M is isomorphic to a left ideal of Λ of R-rank 1 by Proposition 84. Then this follows from Propositions 83, 85 and 86.

We may choose a set of representatives $\{U_i\}$ for ideal classes of R_0, and express the ambiguous ideals of R by $(\theta-\bar{\theta})^{\varepsilon}U_iR$ up to Λ-isomorphism.

Proposition 88. *If M is a projective Λ-module, then M is isomorphic to a direct sum of U_iR and $(\bar{\theta}-\theta)U_iR$.*

Proof. This follows from Propositions 81 and 85.

Proposition 89. *Suppose M is a projective Λ-module of R-rank N, and*

$$M \cong \bigoplus_{i=1}^{n} U_{n_i}R \bigoplus_{i=1}^{N-n} (\bar{\theta}-\theta)U_{m_i}R.$$

The class of $(\prod U_{n_i})(\prod U_{m_i})$ in R_0 and n are invariants of M, and they determine M uniquely up to Λ-isomorphism.

doi:10.6342/NTU201800167

PROOF. See [30] Theorem 1.3.

Let X and Y be two SG-modules. Let $F \in \mathrm{Hom}_S(SG, \mathrm{Hom}_S(Y, X))$ be an element, then $F(a)$ and $F(b)$ are elements in $\mathrm{Hom}_S(Y, X)$. Write F_a and F_b for $F(a)$ and $F(b)$, respectively. We will use F to construct an SG-module M_F which is an extension of Y by X. Let $M_F = X \oplus Y$ as S-modules. We define the action of G on M_F as follows:

$$a \cdot (x, y) = (a \cdot x + F_a(y), a \cdot y),\ \ b \cdot (x, y) = (b \cdot x + F_b(y), b \cdot y).$$

We can find out what conditions of F should be satisfied to order to make M an SG-module. For example, since

$$\begin{aligned}(aa) \cdot (x, y) &= a \cdot (a(x, y)) = a(a \cdot x + F_a(y), a \cdot y) \\ &= ((aa) \cdot x + a \cdot F_a(y) + F_a(a \cdot y), (aa) \cdot y) = 1 \cdot (x, y) = (x, y),\end{aligned}$$

we have

$$a \cdot F_a(y) + F_a(a \cdot y) = 0. \tag{4.4}$$

Similarly, we have

$$\sum_{i=0}^{p-1} b^{p-1-i} F_b(b^i \cdot y) = 0 \tag{4.5}$$

and

$$aF_b(y) + F_a(b \cdot y) = b^{p-1} \cdot F_a(y) - b^{p-1} F_b(b^{p-1} a \cdot y). \tag{4.6}$$

These are all restrictions on F for making M an SG-module. We denote M_F by $(X, Y; F)$. Conversely, suppose we have an SG-module M and M is an extension of Y by X. Since

doi:10.6342/NTU201800167

Y is S-projective, we can choose a decomposition of S-modules $M = X \oplus Y$. This decomposition induces an element $F \in \mathrm{Hom}_S(SG, \mathrm{Hom}_S(Y, X))$ which satisfies above conditions.

Denote by S the trivial representation of G, and denote by $S' := S$ the SG-module with G-action given by $a \cdot s = -s$ and $b \cdot s = s$, for $s \in S$. Let L be a free S-module with basis $\{e_1, \ e_2\}$, together with G-action given by $a \cdot e_1 = e_2$ and $a \cdot e_2 = e_1$ and $b \cdot e_i = e_i$ for $i = 1$ or 2. Let $\{U_i\}$ be a representative system of the ideal class group of R_0. Let A_i denote the SG-module U_iR with G-action given by $a \cdot x = \bar{x}$ and $b \cdot x = \theta x$, for $x \in U_iR$. Let A_i' denote the SG-module with set elements in U_iR but with G-action given by $a \cdot x = -\bar{x}$ and $b \cdot x = \theta x$ for $x \in U_iR$. According to the discussion at the beginning of this section, together with Theorem 89 and Example 77, every SG-module M is an extension of

$$S^r \oplus S'^s \oplus L^t \quad \text{by} \quad A_{n_1} \oplus \cdots \oplus A_{n_\alpha} \oplus A'_{m_1} \oplus \cdots \oplus A'_{m_\beta}.$$

Since the functor Hom commutes with the functor *oplus*, we may consider only $F \in \mathrm{Hom}_S(SG, \mathrm{Hom}_S(Y, X))$ with $Y = S$, S' or L, and $X = A_i$ or A_i' first.

Proposition 90. *After fixing $(Y, \ X)$ such that $(Y, \ X) \neq (S, \ A_i)$ or (S', A_i'), there exists a unique indecomposable extension of Y by X up to SG-isomorphism. In other words, the extension of Y by X is either trivial (decomposable) or the unique indecomposable SG-module up to isomorphism.*

Proof. See [30] Proposition 2.2.

Proposition 91. *For $(Y, \ X) = (S, \ A_i)$ or (S', A_i'), there does not exist any indecomposable extension.*

Proof. See [30] Lemma 2.1.

doi:10.6342/NTU201800167

By Proposition 90, we may drop F from the notation $(X, Y; F)$ and denote the unique indecomposable extension by (X, Y). The following is a more explicit expression of these indecomposable extensions.

Let $F_a, F_b \in \mathrm{Hom}_S(S, A'_i)$, and define

$$F_b(s) = sn_0, \quad \text{and} \quad F_a(s) = \frac{-\bar{F_b}(1) + \bar{\theta} F_b(1)}{(\bar{\theta} - 1)} = s\frac{(-\bar{n}_0 + \bar{\theta} n_0)}{\bar{\theta} - 1} \tag{4.7}$$

for $n_0 \in A'_i$ and $n_0 \notin (\theta - 1)A'_i$. For $F_a, F_b \in \mathrm{Hom}_S(L, A_i)$, we define

$$F_a(e_1) = n_0 \text{ and } F_b(e_2) = n_0$$

where n_0 is an element in A'_i and $n_0 \notin (\theta - 1)A'_i$ and for any P , $P|2R$, $n_0 \notin P$.

Using the conditions (4.4) and (4.6), we have that

$$F_a(e_2) = \overline{F_a(e_1)} \text{ and } \bar{n}_0 + F_a(e_2) = \bar{\theta} n_0 - \bar{\theta} F_b(e_1). \tag{4.8}$$

By Proposition 46 and the fact that M_0 is $\mathbb{Z}$-free, we can reduce finding the indecomposable $\mathbb{Z}G$-modules to finding the indecomposable $\mathbb{Z}_{(2p)}G$-modules. Now we denote by R and R_0 the integral closures of $\mathbb{Z}_{(2p)}$ in K and K_0, respectively. Since $\mathbb{Z}_{(2p)}$ has only finitely many maximal ideals (in fact two), R and R_0 have only finitely many maximal ideals as well. Thus, R_0 and R are Dedekind domains having only finitely many maximal ideals, and hence they are PID. Lee proves that any indecomposable $\mathbb{Z}_{(2p)}G$-modules is one of the following 5 forms:

$$(A', \mathbb{Z}_{(2p)}),\ (A, \mathbb{Z}'_{(2p)}),\ (A, L),\ (A', L) \text{ and } (A' + A, L).$$

The former 4 types are proved by a matrix calculation, and the last one follows from a result of Swan [39]. Once all indecomposable $\mathbb{Z}_{(2p)}G$-modules are known, all indecomposable $\mathbb{Z}G$-modules are known.

For $S=\mathbb{Z}$ or $\mathbb{Z}_{(2p)}$, there are 5 types of indecomposable SG-extensions. Also there are A_i, A_i' and S, S', L as SG-modules. Eventually, all integral representations of G are of these $7h+3$ types, where h is the class number of the integral closure of S in K_0.

Theorem 92. *For $S=\mathbb{Z}$ or $\mathbb{Z}_{(2p)}$ and R_0 be the integral closure of S in K_0. Let h be the class number of R_0. These $7h+3$ isomorphism classes of indecomposable SG-modules are all isomorphism classes of indecomposable SG-modules.*

Proof. See [30] Theorem 2.1.

Since the Krull-Schmidt Theorem holds for $\mathbb{Z}_{(p)}G$- and $\mathbb{Z}_{(2)}G$-modules (see [30] Theorem 3.1.), we can consider the unique decompositions of $\mathbb{Z}_{(2p)}G$-modules into indecomposable $\mathbb{Z}_{(p)}G$- and $\mathbb{Z}_{(2)}G$-modules after scalar extensions. For two $\mathbb{Z}_{(2p)}G$-modules M and N, by Proposition 47 $M\cong N$ if and only if $M_{(p)}\cong N_{(p)}$ and $M_{(2)}\cong N_{(2)}$.

If a $\mathbb{Z}_{(2p)}G$-module M decomposes as

$$\begin{aligned}M\cong \mathbb{Z}_{(2p)}^{s_1}\oplus {\mathbb{Z}'_{(2p)}}^{s_2}\oplus L^l\oplus A^{r_1}\oplus A'^{r_2}\oplus (A,\mathbb{Z}'_{(2p)})^{u_1}\oplus (A',\mathbb{Z}_{(2p)})^{u_2}\\ \oplus (A,L)^{v_1}\oplus (A',L)^{v_2}\oplus (A+A',L)^t,\end{aligned}$$

then

$$s_1+u_2,\ s_2+u_1,\ r_1,\ r_2,\ u_1+v_1+t,\ u_2+v_2+t,\ s_1+l+v_1,\ s_2+l+v_2$$

are invariants of M and determine M up to $\mathbb{Z}_{(2p)}G$-isomorphic. This follows from Proposition 47. Below is the chart of decompositions of indecomposable $\mathbb{Z}_{(2p)}G$-modules.

doi:10.6342/NTU201800167

$\mathbb{Z}_{(2p)}G$-module	$\mathbb{Z}_{(2)}G$-module	$\mathbb{Z}_{(p)}G$-module
$\mathbb{Z}_{(2p)}$	$\mathbb{Z}_{(2)}$	$\mathbb{Z}_{(p)}$
$\mathbb{Z}'_{(2p)}$	$\mathbb{Z}'_{(2)}$	$\mathbb{Z}'_{(p)}$
L	$L_{(2)}$	$\mathbb{Z}_{(p)} \oplus \mathbb{Z}'_{(p)}$
$R_0R = R$	$R_{(2)}$	$R_{(p)}$
$R'_0R = R'$	$R'_{(2)}$	$R'_{(p)}$
$(R, \mathbb{Z}')$	$R_{(2)} \oplus \mathbb{Z}'_{(2)}$	$(R_{(p)}, \mathbb{Z}'_{(p)})$
$(R', \mathbb{Z})$	$R'_{(2)} \oplus \mathbb{Z}_{(2)}$	$(R'_{(p)}, \mathbb{Z}_{(p)})$
(R, L)	$R_{(2)} \oplus L_{(2)}$	$(R_{(p)}, \mathbb{Z}_{(p)} \oplus \mathbb{Z}'_{(p)}) = \mathbb{Z}_{(p)} \oplus (R_{(p)}, \mathbb{Z}'_{(p)})$
(R', L)	$R'_{(2)} \oplus L_{(2)}$	$(R'_{(p)}, \mathbb{Z}_{(p)} \oplus \mathbb{Z}'_{(p)}) = \mathbb{Z}'_{(p)} \oplus (R'_{(p)}, \mathbb{Z}_{(p)})$
$(R + R', L)$	$R_{(2)} \oplus R'_{(2)} \oplus L_{(2)}$	$(R_{(p)} + R'_{(p)}, \mathbb{Z}_{(p)} \oplus \mathbb{Z}'_{(p)}) =$ $\mathbb{Z}'_{(p)} \oplus (R'_{(p)}, \mathbb{Z}_{(p)}) \oplus \mathbb{Z}_{(p)} \oplus (R_{(p)}, \mathbb{Z}'_{(p)})$

Table 4.1: Decompositions of $\mathbb{Z}_{(2p)}D_p$ modules with coefficients $\mathbb{Z}_{(p)}$ and $\mathbb{Z}_{(2)}$

Theorem 93. *Let M be a $\mathbb{Z}G$-module, and write*

$$M \cong \mathbb{Z}^{s_1} \oplus \mathbb{Z}'^{s_2} \oplus L^l \oplus U_{i_\delta}R^{r_1} \oplus (\bar{\theta} - \theta)U_{i_\epsilon}R^{r_2} \oplus (U_{i_\zeta}R, \mathbb{Z}')^{u_1} \oplus (\bar{\theta} - \theta)U_{i_\eta}R, \mathbb{Z})^{u_2}$$

$$\oplus (U_{i_\lambda}R, L)^{v_1} \oplus ((\bar{\theta} - \theta)U_{i_\mu}R, L)^{v_2} \oplus (R + (\bar{\theta} - \theta)U_{i_\nu}R, L)^t,$$

then we have $s_1 + u_2,\ s_2 + u_1,\ r_1,\ r_2,\ u_1 + v_1 + t,\ u_2 + v_2 + t,\ s_1 + l + v_1,\ s_2 + l + v_2$ are invariants of M and they determine M up to $\mathbb{Z}_{(2p)}G$-isomorphism. The class of

$$(\prod U_{i_\delta})(\prod U_{i_\epsilon}(\prod U_{i_\zeta}(\prod U_{i_\eta})(\prod U_{i_\lambda})(\prod U_{i_\mu})(\prod U_{i_\eta})$$

in R_0 is also an invariant of M.

4.3 An example

We keep the notation in Section 4.2. Let $p = 3$, $G = S_3$, and R_0 be the integral closure of $S = \mathbb{Z}$ in $\mathbb{Q}(\theta + \bar{\theta})$, where $\theta = (1 + \imath\sqrt{3})/2$. Fortunately, $R_0 = \mathbb{Z}$ is PID. Hence, there are $7 + 3 = 10$ isomorphism classes of indecomposable $\mathbb{Z}S_3$-modules. We will write down these indecomposable $\mathbb{Z}S_3$-modules explicitly.

doi:10.6342/NTU201800167

Via $\rho : \mathbb{Z}G \to \mathbb{Z}C_2$, with $C_2 = \langle a \rangle$, $a \mapsto a$ and $b \mapsto 1$, we have 3 indecomposable $\mathbb{Z}G$-modules, $\mathbb{Z}, \mathbb{Z}'$ and L. Since the class number of R_0 is 1, $A = \mathbb{Z}R = R = \mathbb{Z}[\theta]$ with $a \cdot r = \bar{r}$ and $b \cdot r = \theta r$, and $A' = \mathbb{Z}R = R = \mathbb{Z}[\theta]$ with $a \cdot r = -\bar{r}$ and $b \cdot r = \theta r$.

For the other indecomposable $\mathbb{Z}G$-extensions, since we can pick $A = \mathbb{Z}R$, we can choose $n_0 = 1$, whch satisfies all conditions in (4.7) and (4.2).

For $(A, \mathbb{Z}'; F) = R \oplus \mathbb{Z}$, substituting n_0=1 in (4.7), we have $F_b(s) = s$, and $F_a(s) = s$.

For $(A, L; F) = R \oplus \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$, we have $F_a(e_1) = 1$, $F_a(e_2) = 1$, $F_b(e_2) = 1$ and $F_b(e_1) = -2\theta + 1$.

Recall the action of G on $(X, Y; F)$ is defined by

$$a \cdot (x, y) = (a \cdot x + F_a(y), a \cdot y) \text{ and } b \cdot (x, y) = (b \cdot x + F_b(y), b \cdot y).$$

Then we have the Table 4.2. Due to typesetting, we write the module $(A + A', L; F)$ separately.

For $(r, r', s_1e_1, s_2e_2) \in (A + A', L; F)$,

$$a \cdot (r, r', s_1e_1, s_2e_2) = (\bar{r} + s_1 + s_2, -\bar{r}' + s_1 + s_2, s_2e_1, s_1e_2),$$

$$b \cdot (r, r', s_1e_1, s_2e_2) = (\theta r + s_2 + (-2\theta + 1)s_1, \theta r' + s_2 + (-2\theta + 1)s_1,\ s_1e_1, s_2, e_2).$$

doi:10.6342/NTU201800167

SG-Module	F_a	a acts on it
$\mathbb{Z}$		$s \mapsto s$
$\mathbb{Z}'$		$s \mapsto -s$
L		$e_1 \mapsto e_2,\ e_2 \mapsto e_1$
A		$s \mapsto \bar{s}$
A'		$s \mapsto -\bar{s}$
$(A', \mathbb{Z}; F)$	$F_a(s) = s$	$(r,\ s) \mapsto (-\bar{r} + s,\ s)$
$(A, \mathbb{Z}'; F)$	$F_a(s) = s$	$(r,\ s) \mapsto (\bar{r} + s,\ -s)$
$(A, L; F)$	$F_a(e_1) = 1,$	$(r,\ s_1e_1,\ s_2e_2)$
	$F_a(e_2) = 1$	$\mapsto (\bar{r} + s_1 + s_2,\ s_2e_1, s_1e_2)$
$(A', L; F)$	$F_a(e_1) = 1,$	$(r,\ s_1e_1,\ s_2e_2)$
	$F_a(e_2) = 1$	$\mapsto (-\bar{r} + s_1 + s_2,\ s_2e_1, s_1e_2)$

SG-Module	F_b	b acts on it
$\mathbb{Z}$		$s \mapsto s$
$\mathbb{Z}'$		$s \mapsto s$
L		$e_1 \mapsto e_1,\ e_2 \mapsto e_2$
A		$s \mapsto \theta s$
A'		$s \mapsto \theta s$
$(A', \mathbb{Z}; F)$	$F_b(s) = s$	$(r,\ s) \mapsto (\theta r + s,\ s)$
$(A, \mathbb{Z}'; F)$	$F_b(s) = s$	$(r,\ s) \mapsto (\theta r + s,\ s)$
$(A, L; F)$	$F_b(e_2) = 1,$	$(r,\ s_1e_1, s_2e_2)$
	$F_b(e_1) = (-2\theta + 1)$	$\mapsto (\theta r + s_2 + (-2\theta + 1)s_1,\ s_1e_1, s_2, e_2)$
$(A', L; F)$	$F_b(e_2) = 1,$	$(r,\ s_1e_1, s_2e_2)$
	$F_b(e_1) = (-2\theta + 1)$	$\mapsto (\theta r + s_2 + (-2\theta + 1)s_1,\ s_1e_1, s_2, e_2)$

Table 4.2: Actions of S_3 on indecomposable $\mathbb{Z}S_3$-lattices and $\mathbb{Z}_{(6)}S_3$-lattices

Chapter 5

Chow's theorem for semi-abelian varieties and bounds for splitting fields for algebraic tori

5.1 Introduction

A connected algebraic group T over a field k is an algebraic torus if there is a $\bar{k}$-isomorphism $T \otimes \bar{k} \simeq (\mathbb{G}_{\mathrm{m}})^d \otimes_k \bar{k}$ of algebraic groups, where $d = \dim T$, $\bar{k}$ is an algebraic closure of k and k_s is the separable closure of k in $\bar{k}$. We say T splits over a field extension K of k if there is a K-isomorphism $T \otimes_k K \simeq (\mathbb{G}_{\mathrm{m}})^d \otimes_k K$. The main purpose of this paper is to extend methods for proving the following fundamental result.

Theorem 94. *Any algebraic torus T over a field k splits over k_s. In other words, T_s splits over a finite separable field extension of k.*

This theorem is well known and it is stated and proved in the literature several times. Surprisingly, different authors chose their favorite proofs which are all quite different. The first proof is given by Takashi Ono [32, Proposition 1.2.1]. Armand Borel gave another proof in his book *Linear Algebraic Groups*; see [2, Proposition 8.11]. In the second edition of his book *Linear Algebraic Groups*, T.A. Springer included a systematic treatment of the rationality problem of algebraic groups where he also gave another proof of Theorem 94; see [37, Proposition 13.1.1]. Another proof, due to John Tate, is given in Borel and Tits [3, Proposition 1.5]. Jacques Tits himself also provided one proof in his Yale University Lectures Notes; see [41, Theorem 1.4.1].

The proof given by Borel uses the property that the k_s-valued points of T are semisimple. Note that this property is also shared by diagonalizable groups. Thus, Borel's proof generalizes Theorem 94 to diagonalizable k-groups. Springer's proof has more flavor of differential geometry; one key ingredient of his proof uses derivations. One may view that Springer uses derivations and connections to treat purely inseparable descent. Note that the classical Galois descent deals with the descent of *separable* algebraic extensions. It is known that this method of using group theory fails for the descent of inseparable field extensions. However, the hidden information can be revealed using derivations and connections. Springer's proof of Theorem 94 is an interesting application of the inseparable descent. The proofs given by Tits and by Tate uses only the properties of characters. The ideas of their proofs are similar: Both uses the same argument that a suitable p-power of any character χ of T is defined over k_s. The only difference is that Tits works with the coordinate ring $\bar{k}[T]$ of T while Tate works with its function field $\bar{k}(T)$. That Tate proves the k_s-rationality of χ uses the language in Weil's foundation, while Tits' argument is more elementary.

Ono's proof relies on an analogue of Chow's theorem for tori (see [32, Lemma 1.2.1]) Chow's theorem states as follows. Let K/k be a primary field extension, that is, k is separably algebraically closed in K. If X and Y are two abelian varieties over k, then the monomorphism $\mathrm{Hom}_k(X, Y) \to \mathrm{Hom}_K(X_K, Y_K)$, where $X_K := X \otimes_k K$, is also surjective; see [8], also see [29, Chapter II, Theorem 5], [6, Lemma 1.2.1.2], [9, Theorem 3.19] and [45, Lemma 6.7]. Ono did not give a proof of the analogous result for tori. However, he

doi:10.6342/NTU201800167

pointed out (in the proof of [32, Lemma 1.2.1]) that the original proof of Chow for abelian varieties also works for tori . Thus, we revisit Chow's theorem, aiming at supplementing Ono's proof. The original proof given by Chow uses the language in Weil's foundation. A modern proof of Chow's theorem, due to Brian Conrad, is given in [9, Theorem 3.19]. The central idea is Grothendieck's faithfully flat descent.

Grothendieck's descent theory has been a very powerful tool of algebraic geometry. The standard reference is SGA 1 [16]. The reader can also find the exposition in some books or articles working with moduli spaces or étale cohomology, for example, Milne [31, Chapter 1, Section 2], Freitag and Kiehl [15, Appendix A], , Bosch, Lütkebohmert, and Raynaud [4, Chapter 6] and B. Conrad [9, Section 3]. The faithfully flat descent is a very clean formulation which reorganizes both the classical Galois descent and the purely inseparable descent through derivations over fields in one unified way (regardless the explicit structure of the flat base in question). More powerfully, this simple formulation works for arbitrary base schemes, so it is far beyond the combination of both separable and inseparable descent over fields.

The idea of Conrad's proof of Chow's theorem is pursued further in this article. We generalize Chow's theorem to semi-abelian varieties, which includes the case of tori. This completes Ono's proof of Theorem 94 by an alternative method. We refer to Section 5.5.2 for the definition of semi-abelian varieties.

Theorem 95. *Let X and Y be two semi-abelian varieties over a field k, and let K be a primary field extension of k. Then the monomorphism of $\mathbb{Z}$-modules*

$$\mathrm{Hom}_k(X,Y) \to \mathrm{Hom}_K(X_K, Y_K), \quad X_K := X \otimes_k K, \tag{5.1}$$

is bijective.

Besides proofs given by Borel, Springer, Tate, Ono, Tits, we also give a new proof of

doi:10.6342/NTU201800167

Theorem 94. Our proof is based on a second proof of Theorem 95, which does not rely on he faithfully flat descent.

It is obvious that Theorem 94 is merely one of many theorems appearing in the theory of algebraic groups. Why do we care only on this single result? Below are two reasons:

(a) There are already several different and interesting proofs given by experts from the viewpoints from algebraic geometry, number theory. differential geometry, group representation theory and arithmetic. Thus, reorganizing these proofs as well as the methods and ingredients behind should be useful and illuminating.

(b) Though tori are the simplest connected linear algebraic groups and have been studied for several decades, there are several problems that remain open and have been tried out in various cases up to now. Among them, we are interested in the classification of algebraic tori over an arbitrary field. Because a solution would rely on the development of integral representations of finite groups, solutions to the Inverse Galois problem and Noether's problem. These are very active ongoing research topics.

We illustrate the point (b) in more detail. Let $\Gamma_k := \mathrm{Gal}(k_s/k)$ be the absolute Galois group of k. Using Theorem 94, the functor

$$\text{a } k\text{-torus } T \ \mapsto X_*(T) := \mathrm{Hom}_{k_s}(\mathbb{G}_{\mathrm{m}k_s}, T_{k_s}) \tag{5.2}$$

gives rise to an equivalence between the category of algebraic tori over k and the category of finite free $\mathbb{Z}$-module together with a continuous action of Γ_k, or $\mathbb{Z}\Gamma_k$-lattices. If K/k is a finite Galois extension with Galois group $G := \mathrm{Gal}(K/k)$, then this functor induces a bijection

$$\left\{\begin{array}{l}\text{isomorphism classes}\\ \text{of } k\text{-tori splitting}\\ \text{over } K\end{array}\right\} \xrightarrow{\sim} \left\{\begin{array}{l}\text{isomorphism}\\ \text{classes of } \mathbb{Z}G\text{-}\\ \text{lattices}\end{array}\right\}. \tag{5.3}$$

Thus, classification of tori over k can be divided into two steps:

(1) Classify all finite groups G which are quotients of Γ_k (the IGP).

(2) Classify integral representations of G.

Noether's problem is the most prominent and famous problem in the IGP. We refer to [26] for a survey of Noether's problem and the references within for more details. For recent development of Noether's problem, we refer to works of M.-C. Kang [22, 24] and those of H. Kitayama and A. Yamasaki [28, 27, 44].

We conclude this paper with the best bound for the degrees of splitting fields of tori.

Proposition 96. *(Corollary 118) For any $d \geq 1$ and any number field k, there exists a d-dimensional T over k such that $[k_T : k] = \mathrm{Max}(d, \mathbb{Q})$, where k_T is the (minimal) splitting field of T and $\mathrm{Max}(d, \mathbb{Q})$ is the maximal order of finite subgroups of $\mathrm{GL}_d(\mathbb{Q})$.*

The paper is organized as follows. Section 2 consists of minimal preliminaries of diagonalizable groups and gives a proof of Theorem 94 due to Borel. Section 3 includes basic properties of derivations and connections as well as a formulation for purely inseparable descent. A proof due to Springer is also included. Section 4 includes the proofs of Tits and Tate. Theorem 95 is proved in Section 5; we also give a different proof of Theorem 95 and hence that of Theorem 94.

5.2 Characters and diagonalizable groups

In this section we shall present a proof of Theorem 94 due to Armand Borel. A basic result is that any set of characters is linearly independent in the following sense.

Lemma 97. *Let H be an abstract group, k any field, and let X be the set of all homomorphisms $H \to k^\times$. Then X is k-linearly independent as a subset in the k-vector space*

doi:10.6342/NTU201800167

$\mathcal{C}(H,k)$ of k-valued functions on H. That is, for any distinct characters $\chi_1,\dots,\chi_n$ and elements $a_1,\dots,a_n\in k$, then

$$a_1\chi_1+\cdots+a_n\chi_n=0 \text{ in } \mathcal{C}(H,k) \implies a_1=\cdots=a_n=0. \tag{5.4}$$

Proof. See [2, Lemma 8.1].

Let G be a linear algebraic group over a field k. Put $K:=\bar{k}$. Let $X(G):=\mathrm{Hom}_{\bar{k}\text{-gp}}(G,\mathbb{G}_{\mathrm{m}})$ denote the group of all characters, which is a finitely generated abelian group. The subgroup of k-rational characters is denoted by $X(G)_k$.

Definition 98. (1) We say that G is *diagonalizable* if the coordinate ring $K[G]$ is spanned by $X(G)$ over K.

(2) We say that a diagonalizable group G splits over k if the coordinate ring $k[G]$ is spanned by $X(G)_k$ over k.

By Lemma 97, the abelian group $X(G)$ is a linearly independent subset in $K[G]$. So if G is diagonalizable, then $K[G]$ is equal to the group algebra $K[X(G)]$ of the abelian group $X(G)$. Any group algebra $K[H]$ admits a natural structure of Hopf algebra with the co-multiplication $\Delta: K[H]\to K[H]\otimes_K K[H]$ defined by $\Delta(h)=h\otimes h$. Then $K[G]=K[X(G)]$ as Hopf algebras. Particularly, G is commutative.

It is clear from the definition that an algebraic torus is precisely a connected diagonalizable algebraic group. We recall basic properties of diagonalizable groups. Let $\mathbf{D}_n\subset \mathrm{GL}_n$, for $n\ge 1$, denote the diagonal split torus of dimension n.

Proposition 99. *Let G be a linear algebraic group over K. The following statements are equivalent:*

1. *G is diagonalizable.*

doi:10.6342/NTU201800167

2. *G is isomorphic to a subgroup of $\mathbf{D}_n$ for some $n \geq 1$.*

3. *For any rational representation $\pi : G \to \mathrm{GL}_n$, the subgroup $\pi(G)$ is conjugate to a subgroup of $\mathbf{D}_n$.*

4. *G contains a dense commutative subgroup consisting of semi-simple elements.*

Proof. See [2, Proposition 8.4].

Proposition 100. *Let G be a diagonalizable group over k. The following statements are equivalent:*

1. *G splits over k.*

2. *G is isomorphic to a k-subgroup of $\mathbf{D}_n$ for some $n \geq 1$.*

3. *For any rational representation $\pi : G \to \mathrm{GL}_n$ defined over k, the subgroup $\pi(G)$ is conjugate over k to a subgroup of $\mathbf{D}_n$.*

Proof. See [2, Proposition 8.4'].

Theorem 101. *Any diagonalizable k-group G splits over k_s.*

Proof. Choose a k-embedding $G \subset \mathrm{GL}_n$. By Proposition 99, $G(k_s)$ contains a dense commutative subgroup S consisting of semi-simple elements. As S is commutative and every element s in S is diagonalizable in $\mathrm{GL}_n(k_s)$, we can diagonalize simultaneously the matrices s for all $s \in S$. That is, there is an element $g \in \mathrm{GL}_n(k_s)$ such that $gSg^{-1} \subset \mathbf{D}_n(k_s)$. Since S is dense, the inner automorphism $\mathrm{Int}(g)$ sends G into a subgroup of $\mathbf{D_n}$. Therefore, G is k_s-isomorphic to a subgroup of $\mathbf{D_n}$, which splits over k by Proposition 100. This completes the proof of the theorem. ∎

Theorem 94 follows from Theorem 101, because any algebraic torus is a diagonalizable group. We remark that the property Proposition 99 (4) was also used by Rosenlicht who showed that any algebraic k-torus is unirational; see [35, Proposition 10].

doi:10.6342/NTU201800167

5.3 Derivations, connections and inseparable descent

In this section we present the second proof of Theorem 94 due to T.A. Springer. The proof is actually quite long as one needs to develop several setups. The key idea is to deduce purely inseparable descent through derivations and connections. This may be viewed as an extension of the Galois descent which handles only the case of separable extensions.

5.3.1 Derivations

Definition 102. Let R be a commutative ring and A a commutative R-algebra. Let M be an A-module. An R-derivation of A on M is an R-linear map $D : A \to M$ such that

$$D(ab) = aD(b) + bD(a), \quad \forall\, a, b \in A. \tag{5.5}$$

Let $\mathrm{Der}_R(A, M)$ denote the set of all R-derivations of A on M. It is equipped with a natural A-module structure by defining $(bD)(x) := bD(x)$ for $b \in A$ and $D \in \mathrm{Der}_R(A, M)$. Note that $D(r \cdot 1) = 0$ for any $r \in R$.

If $\phi : A \to B$ is an R-algebra homomorphism and N is a B-module, then one can regard N as an A-module. Thus, one obtains a map of A-modules

$$\phi_0 : \mathrm{Der}_R(B.N) \to \mathrm{Der}_R(A.N), \quad D \mapsto D \circ \phi. \tag{5.6}$$

The map ϕ_0 induces a short exact sequence of A-modules

$$0 \to \mathrm{Der}_A(B.N) \to \mathrm{Der}_R(B.N) \to \mathrm{Der}_R(A.N). \tag{5.7}$$

doi:10.6342/NTU201800167

5.3.2 Tangent spaces

We show how to use derivations to reformulate the tangent space of an algebraic variety at a point. Let $X \subset \mathbf{A}^n$ be a closed subvariety of the affine n-space over K, where K is an algebraically closed field, and let $x = (a_1, \dots, a_n) \in X$ be a K-point. We write the coordinate ring of X by $K[X] = K[T]/I$, where $T = (T_1, \dots, T_n)$ and $I = (f_1, \dots, f_s) \subset K[T]$ is the ideal of definition. Write the tangent space $T_x\mathbf{A}^n = K^n$ with the standard basis $\partial/\partial T_i$ for $i = 1, \dots, n$. Then the tangent space $T_xX \subset T_x\mathbf{A}^n$ consists of vectors $(v_1, \dots, v_n) \in K^n$ satisfying the linear equations

$$\sum_{i=1}^n v_i \frac{\partial f_j}{\partial T_i}(x) = 0, \quad j = 1, \dots, s. \tag{5.8}$$

Let $M_x \subset K[X]$ be the maximal ideal corresponding to x, and $K(x) := K[X]/M_x = K[T]/(T_1 - a_1, \dots, T_n - a_n)$ the residue field at x, viewed as a $K[X]$-module or a $K[T]$-module. We can identify the tangent space $T_x\mathbf{A}^n$ with $\mathrm{Der}_K(K[T], K(x))$ as

$$T_x\mathbf{A}^n \simeq \mathrm{Der}_K(K[T], K(x)), \quad v = (v_1, \dots, v_n) \mapsto D_v = \sum_{i=1}^n v_i D_i, \tag{5.9}$$

where D_i is the unique derivation such that $D_i(T_j) = \delta_{ij}$ for $j = 1, \dots, n$. One easily sees that the derivation $D_v : K[T] \to K(x)$ factors through $K[X] \to K(x)$ if and only v satisfies the condition (5.8). Thus, the identification (5.9) induces a natural isomorphism

$$T_xX \simeq \mathrm{Der}_K(K[X], K(x)). \tag{5.10}$$

Note that D_v is uniquely determined its restriction on M_x, because $K[X] = K \oplus M_x$. Thus, by (5.10), we obtain a natural isomorphism

$$T_xX \simeq \mathrm{Hom}_K(M_x/M_x^2, K(x)) = (M_x/M_x^2)^*. \tag{5.11}$$

doi:10.6342/NTU201800167

We call the $K(x)$-vector space M_x/M_x^2 the *cotangent space of X at x*. The isomorphisms (5.10) and (5.11) provide two alternative definitions for the tangent space T_xX of X at a point. These reformulations show that the tangent space T_xX is an intrinsic property, in the sense that does not depend on the choice of an embedding of X into the affine space $\mathbf{A}^n$. Furthermore, we can use these reformulations to define the tangent spaces of an arbitrary scheme.

Let $f : X \to Y$ be a morphism of algebraic varieties and let $x \in X$ be a point. Then the differentiation of f gives a K-linear map of vector spaces

$$(df)_x : T_xX \to T_yY, \quad y = f(x). \tag{5.12}$$

If $g : Y \to Z$ is another morphism of algebraic varieties and put $z = g(y)$. Then the differentiation of the composition $g \circ f$ has the property

$$(d\,g{\circ}f)_x = (dg)_y \circ (df)_x \quad \text{(the chain rule)}. \tag{5.13}$$

5.3.3 Kähler differentials

Definition 103. Let R and A be as in Definition 102. Let $I_{A/R}$ denote the kernel of the multiplication $m : A \otimes_R A \to A$. The *Kähler differential* $\Omega^1_{A/R}$ of A over R is defined by

$$\Omega^1_{A/R} := I_{A/R}/I^2_{A/R}. \tag{5.14}$$

This is an A-module by the isomorphism $A \otimes_R A/I_{A/R} \simeq A$.

It is easy to see that the ideal $I_{A/R}$ is generated by elements $a \otimes 1 - 1 \otimes a$ for all $a \in A$. For $a \in A$, write

$$da := [a \otimes 1 - 1 \otimes a], \quad a \in A \tag{5.15}$$

the class in $\Omega^1_{A/R}$. Then the map $d : A \to \Omega^1_{A/R}$ is an R-derivation of A on $\Omega^1_{A/R}$. If M is an A-module and $\varphi : \Omega^1_{A/R} \to M$ is a morphism A-module, then the composition

$$d \circ \varphi : A \to \Omega^1_{A/R} \to M \tag{5.16}$$

is an R-derivation of A on M. Conversely, any R-derivation $D \in \mathrm{Der}_R(A, M)$ arises in this way. That is, there is a unique A-homomorphism $\varphi_D : \Omega^1_{A/R} \to M$ such that $D = d \circ \varphi_D$. This gives a canonical isomorphism of A-modules

$$\mathrm{Hom}_A(\Omega^1_{A/R}, M) \xrightarrow{\sim} \mathrm{Der}_R(A, M) \tag{5.17}$$

which is functorial for all A-modules M.

Consider a covariant functor from the category (A-mod) of A-modules to (A-mod) defined by

$$\mathrm{Der}_R(A, \cdot) : A\text{-mod} \to A\text{-mod}, \quad M \mapsto \mathrm{Der}_R(A, M). \tag{5.18}$$

Then by (5.17) the Kähler differential $\Omega^1_{A/R}$ represents this functor, and d is the universal family.

The isomorphism (5.17) linearizes the R-derivations. Thus, the computation of R-derivations $\mathrm{Der}_R(A, M)$ is reduced to calculating $\Omega^1_{A/R}$, which can be done explicitly by linear relations as follows.

Suppose that A is essentially of finite type over R, say $A = R[x_1, \ldots, x_n]_S = (R[T]/I)_S$, where $T = (T_1, \ldots, T_n)$, $I = (f_1, \ldots, f_s)$ and S is a multiplicatively closed subset which does not contain zero divisors. Then

$$\Omega^1_{A/R} = A\langle\, dx_1, \ldots, dx_n \,\Big|\, \sum_{i=1}^{n} y_{ji} dx_i = 0,\ j = 1, \ldots, s \,\rangle, \tag{5.19}$$

where $y_{ji} := (\partial f_j / \partial T_i)(x_1, \ldots, x_n) \in A$.

Let $X = \operatorname{Spec} A \to \operatorname{Spec} K$ be an affine algebraic variety of dimension d. Then X is a non-singular algebraic variety if and only if the Kähler differential $\Omega^1_{A/K}$ is a locally free A-module of rank d. This follows from the Jacobian criterion for simple points and the computation of $\Omega^1_{A/K}$ (see (5.19)). More generally, if $f : X \to S$ is a morphism of locally Noetherian schemes locally of finite type, then $\Omega^1_{X/S}$ is a locally free $\mathcal{O}_X$-module of rank equal to the relative dimension $\dim(X/S)$ and f is flat if and only if f is smooth (see [31, I, Proposition 3.24] and see [31, I. Remark 3.22] for the definition of smooth morphisms).

Let $\phi : A \to B$ be an R-algebra homomorphism. Then there is a unique morphism $d\phi : \Omega^1_{A/R} \to \Omega^1_{B/R}$ of A-modules making the following diagram commutative

$$\begin{tikzcd}
A \arrow[r, "\phi"] \arrow[d, "d_A"] & B \arrow[d, "d_B"] \\
\Omega^1_{A/R} \arrow[r, "d\phi"] & \Omega^1_{B/R}.
\end{tikzcd} \tag{5.20}$$

Note that $d_B \circ \phi$ is an R-derivation of A on $\Omega^1_{B/R}$. So the commutative diagram (5.20) follows from the universal property of $(\Omega^1_{A/R}, d_A)$. One easily sees that $d\phi(da) = d\phi(a)$ for all $a \in A$. The map $d\phi$ induces an exact sequence of B-modules

$$B \otimes_A \Omega^1_{A/R} \xrightarrow{1_B \otimes d\phi} \Omega^1_{B/R} \longrightarrow \Omega^1_{B/A} \longrightarrow 0. \tag{5.21}$$

Let N be a B-module and $\varphi : \Omega^1_{B/R} \to N$ a B-linear homomorphism. The pull-back $(d\phi)^*(\varphi) = \varphi \circ d\phi : \Omega^1_{A/R} \to N$ is a morphism of A-modules. We then have the commutative diagram

$$\begin{tikzcd}
\operatorname{Hom}_B(\Omega^1_{B/R}, N) \arrow[r, "\sim"] \arrow[d, "(d\phi)^*"] & \operatorname{Der}_R(B, N) \arrow[d, "\phi^*"] \\
\operatorname{Hom}_A(\Omega^1_{A/R}, N) \arrow[r, "\sim"] & \operatorname{Der}_A(A, N),
\end{tikzcd} \tag{5.22}$$

where the horizontal ones are canonical isomorphisms.

5.3.4 Separable field extensions

Definition 104 (cf. [20, Chap. VI, Sect. 2], [37, Sect. 4.2, p. 63-64])**.** (1) A field extension E/k is said to be *separably generated* if there is a subset $\{t_\alpha\} \subset E$ such that

(i) the extension $k(\{t_\alpha\})/k$ is purely transcendental, and

(ii) the extension $E/k(\{t_\alpha\})$ is algebraic and separable.

The subset $\{t_\alpha\}$ is called a *separating transcendental base.*

(2) We call E/k a *separable* extension if either

- $\operatorname{char} k = 0$, or
- $\operatorname{char} k = p > 0$ and for any k-linearly independent elements $x_1, \dots, x_n$ in K, their pth powers $x_1^p, \dots, x_n^p$ are also k-linearly independent.

Proposition 105. (1) *If k is perfect, then any field extension K/k is separable.*

(2) *A field extension K/k of finite type is separably generated if and only if it is separable.*

Proof. (1) This follows easily from the definition. Indeed, suppose that $\{x_i^p\}$ is k-linearly dependent, say $\sum_i a_i x_i^p = 0$. Then one has $\sum_i b_i x_i = 0$ and hence $\{x_i\}$ is k-linearly dependence. (2) See [37, Proposition 4.2.10 and Exercise 4.2.15 (5)]). ∎

Note that Proposition 105 (2) fails if K/k is not of finite type. Indeed, let $k = \mathbb{F}_p$ and $K = \cup_{n\geq 1}\mathbb{F}_p(t^{1/p^n})$. Then K/k is not separably generated but K/k is separable.

Definition 106. Let X and Y be irreducible algebraic varieties over a field k, and $f : X \to Y$ a morphism of finite type.

(1) We say that f is *dominant* if the image $f(X)$ is Zariski dense. In this case, the function field $k(Y)$ can be viewed as a subfield of $k(X)$ through the pull-back of functions.

(2) We say that f is *separable* if f is dominant and the field extension $k(X)/k(Y)$ is separable.

Proposition 107. *Let $f : X \to Y$ be a separable morphism of irreducible normal algebraic varieties over k such that f is a homeomorphism. Then f is an isomorphism.*

Proof. The field extension $k(X)/k(Y)$ is separable of finite type. Since f is a homeomorphism, f is finite and $\dim X = \dim Y = \operatorname{trdeg}_k k(X) = \operatorname{trdeg}_k k(Y)$. It follows that $k(X) = k(Y)$ as $k(X)/k(Y)$ is both a separable and inseparable finite extension. Thus, f is a birational finite morphism of normal varieties and it is an isomorphism by the Zariski main theorem. ∎

We give an example that f is birational and homeomorphic but not isomorphism. Consider the normalization morphism $f : \widetilde{X} \to X$, where $X = \operatorname{Spec} \mathbb{Q}[x, y]/(y^2 - x^3)$. Then f satisfies these properties.

Proposition 108. *Let E/k be a field extension of finite type.*

(1) $\dim_E \Omega^1_{E/k} \geq \operatorname{trdeg}_k E$.

(2) *The equality in (1) if and only if E/k separably generated.*

Proof. See [37, Theorem 4.2.9].

Let E and E' be field extensions of k of finite type with $E' \subset E$. Applying the constructions (5.7) and (5.21), we get short exact sequences:

$$0 \longrightarrow \operatorname{Der}_{E'}(E, E) \longrightarrow \operatorname{Der}_k(E, E) \xrightarrow{\beta} \operatorname{Der}_k(E', E), \tag{5.23}$$

$$E \otimes_{E'} \Omega^1_{E'/k} \xrightarrow{\alpha} \Omega^1_{E/k} \longrightarrow \Omega^1_{E/E'} \longrightarrow 0. \tag{5.24}$$

Clearly, these two are dual with each other. Therefore, β is surjective and α is injective.

Corollary 109. *Assume that k is perfect. The following statements are equivalent:*

(a) E/E' is separately generated.

(b) α *is injective.*

(c) β *is surjective.*

Proof. As is already shown, statements (b) and (c) are equivalent. By (5.24), α is injective if and only if $\dim_{E'} \Omega^1_{E'/k} + \dim_E \Omega^1_{E/E'} = \dim_E \Omega^1_{E/k}$. Since k is perfect, by Prop. 105 and 108 $\dim_B \Omega^1_{B/k} = \operatorname{trdeg}_k B$ for $B = E$ or E'. On the other hand, we always have $\operatorname{trdeg}_k E = \operatorname{trdeg}_{E'} E + \operatorname{trdeg}_k E'$. It follows that α is injective if $\dim_E \Omega^1_{E/E'} = \operatorname{trdeg}_{E'} E$. The latter is equivalent to that E/E' is separably generated by Proposition 108. ∎

5.3.5 Connections

Let A be a commutative k-algebra, where k is any field. Let $\mathcal{D} = \mathcal{D}_A := \operatorname{Der}_k(A, A)$ denote the A-module of all k-derivations of A on itself. It admits a natural structure of Lie algebra over k. If $D_1, D_2 \in \mathcal{D}$, then the Lie bracket is defined by $[D_1, D_2] := D_1D_2 - D_2D_1$. The bracket is not A-bilinear. Let $\operatorname{hor}(A) := \{a \in A | D(a) = 0, \forall\, D \in \mathcal{D}\}$. Elements of $\operatorname{hor}(A)$ are called horizontal elements. It is easy to check that $\operatorname{hor}(A)$ is a k-subalgebra of A, and that the bracket is $\operatorname{hor}(A)$-bilinear.

If $\operatorname{char} k = p > 0$, then $D^p := D \circ D \circ \cdots \circ D$ (p times) is again a k-derivation of A. This gives a p-Lie (or restricted Lie) algebra structure on $\mathcal{D}$. More precisely, the operator $D \mapsto D^p$ satisfies the following three conditions (cf. [37, Sect. 4.4]:

(a) $(aD)^p = a^p D^p$ for $a \in k$ and $D \in \mathcal{D}$.

(b) $\operatorname{ad}(D^p) = (\operatorname{ad} D)^p$ for all $D \in \mathcal{D}$.

(c) We have (Jacobson's formula)

$$(D + D')^p = D^p + D'^p + \sum_{i=1}^{p-1} i^{-1} s_i(D, D'), \tag{5.25}$$

doi:10.6342/NTU201800167

where $s_i(D,D')$ is the coefficient of a^i in $\mathrm{ad}(aD+D')^{p-1}(D')$ for $1 \le i \le p-1$, i.e. $\sum_{i=1}^{p-1} s_i(D,D')a^i = \mathrm{ad}(aD+D')^{p-1}(D')$.

We now introduce connections. We consider a field extension E/k of finite type, and let $\mathcal{D} = \mathcal{D}_E := \mathrm{Der}_k(E,E)$. The subfield $\mathrm{hor}(E)$ of horizontal elements consists of all algebraic and separable elements of E over k. Recall that E/k is said to be primary if k is the algebraic separable closure of k in E. Then E/k is primary if and only if $k = \mathrm{hor}(E)$. We shall give two definitions of connections and then show that they represent the same notion through a natural transformation.

Definition 110. Let E/k and $\mathcal{D}_E$ be as above, and let A be an E-vector space.

(1) A *connection* on A for the extension E/k is a map

$$\nabla : A \to \Omega^1_{E/k} \otimes_E A \tag{5.26}$$

such that $\nabla(ax) = da \otimes x + a\nabla(x)$ for all $x \in A$ and $a \in E$.

(2) A *connection* of $\mathcal{D}_E$ on A is an E-linear map

$$c : \mathcal{D}_E \to \mathrm{End}_k(A) \tag{5.27}$$

such that $c(D)(ax) = D(a)x + a(c(D)(x))$ for all $D \in \mathcal{D}_E, a \in E$ and $x \in A$.

Suppose $\nabla : A \to \Omega^1_{E/k} \otimes_E A$ is a connection. For any $D \in \mathcal{D}_E$, let $\varphi_D : \Omega^1_{E/k} \to E$ the corresponding E-linear map so that $D = \varphi_D \cdot d$. The contraction ∇_D at D is defined to be the composition

$$\nabla_D : A \xrightarrow{\nabla} \Omega^1_{E/k} \otimes A \xrightarrow{\varphi_D \otimes 1} A. \tag{5.28}$$

Lemma 111.

(1) *One has* $\nabla_D(ax) = D(a)x + a\nabla_D(x)$ *and* $\nabla_{aD} = a\nabla_D$ *for all* $a \in E$ *and* $x \in A$.

doi:10.6342/NTU201800167

(2) *Conversely, let $c : \mathcal{D}_E \to \mathrm{End}_k(A)$ be a connection then there exists a unique ∇ such that $c(D) = \nabla_D$ for all $D \in \mathcal{D}_E$.*

PROOF. (1) By definition, $\nabla_D(ax) = \varphi_D(da \otimes x + a\nabla(x)) = D(a)x + a\nabla_D(x)$. The equality $\nabla_{aD} = a\nabla_D$ follows from $\varphi_{aD} = a\varphi_D$ and $\nabla_D = \varphi_D \cdot \nabla$.

(2) Choose an E-basis $\{df_i\}$ for $\Omega^1_{E/k}$. Let $\{\varphi_i\}$ be the dual basis for $\mathrm{Hom}_E(\Omega^1_{E/k}, E)$. Recall that $\Omega^1_{E/k}$ is an finite dimensional E-vector space. Put $D_i := \varphi_i \cdot d$. Then the map c is uniquely determined by $c(D_i) \in \mathrm{End}_k(A)$. Put $x_i := c(D_i)(x) \in A$. Define $\nabla(x) = \sum_i df_i \otimes x_i$. The condition of E/k being of fintie type is used here. It is easy to see $\nabla_{D_i}(x) = x_i = c(D_i)(x)$ for all i. Thus, $\nabla_D(x) = c(D)(x)$ for all $D \in \mathcal{D}_E$. ∎

Given a connection ∇, one extends morphisms

$$\nabla_i : \Omega^i_{E/k} \otimes A \to \Omega^{i+1}_{E/k} \otimes A, \quad \Omega^i_{E/k} := \wedge^i \Omega^1_{E/k}, \quad \nabla_0 = \nabla \quad (i \geq 1) \tag{5.29}$$

by

$$\nabla_i(\omega \otimes x) = d\omega \otimes x + (-1)^i \omega \wedge \nabla_{i-1}(x). \tag{5.30}$$

Definition 112.

(1) The *curvature* of ∇ is $K(\nabla) := \nabla_1 \cdot \nabla : A \to \Omega^2_{E/k} \otimes A$. $K(\nabla)$ is a 2-form with values in $\mathrm{End}_k(A)$.

(2) A connection ∇ is said to be *integrable* or *flat* if $K(\nabla) = 0$.

Lemma 113. *Let $c : \mathcal{D}_E \to \mathrm{End}_k(A)$ be the connection of $\mathcal{D}_E$ on A associated to a connection ∇ on A. Then ∇ is integrable if and only if c is a Lie algebra homomorphism.*

PROOF. This follows from a straightforward computation which we omit.

5.3.6 Inseparable descent

Suppose that $A = A_0 \otimes_k E$ is endowed with a k-structure defined by a k-subspace A_0. We define a flat connection c_A by $c_A(D)(\sum a_i \otimes x_i) = \sum D(a_i) \otimes x_i$ for $a_i \in E$ and $x_i \in A_0$.

c_A is the unique flat connection such that $c_A(D)(A_0) = 0$ for all $D \in \mathcal{D}_E$, and it is called the canonical flat connection on A (of course, with respect to the k-structure A_0). We now formulate inseparable descent in terms of connections. This is the key ingredient used in Springer's proof of Theorem 94

Proposition 114 (Inseparable descent)**.** *Let E/k be a field extension of finite type and $\mathcal{D}_E$ the k-derivations on E to itself. Assume that* $\operatorname{hor}(E) := \{a \in E | D(a) = 0, \forall\, D \in \mathcal{D}_E\} = k$.

(1) Let A_0 be a k-vector space and $A := A_0 \otimes_k E$. One has $\{x \in A | c_A(D)(x) = 0\ \forall\, D \in \mathcal{D}_E\} = A_0$.

(2) If $W \subset A$ be an E-subspace, then W is defined over k if and only if $c_A(D)(W) \subset W$ for all $D \in \mathcal{D}_E$.

(3) Let B_0 be another k-vector space and $B := B_0 \otimes_k E$. Let $f : A \to B$ be an E-linear map. Then f is defined over k if and only if the diagram

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "c_A(D)"'] & B \arrow[d, "c_B(D)"] \\ A \arrow[r, "f"] & B \end{tikzcd} \tag{5.31}$$

commutes for all $D \in \mathcal{D}_E$.

Proof. See [37, Proposition 11.1.4 and Corollary 11.1.5].

5.3.7 Proof of Theorem 94

We may assume that $\operatorname{char} k = p > 0$. It suffices to show that the map $\operatorname{Hom}_k(T, \mathbb{G}_{\mathrm{m}}) \to \operatorname{Hom}_E(T, \mathbb{G}_{\mathrm{m}})$ is surjective for any finite purely inseparable extension E/k. That is, any character χ defined over E is defined over k.

We may also assume that $E^p \subset k$. Indeed, suppose that $E^{p^n} \subset k$ for some n. Then we have a filtration $E_n = kE^{p^n} \subset kE^{p^{n-1}} \subset \cdots \subset E_1 = kE^p \subset E_0 = E$ and $E_i^p \subset E_{i+1}$.

doi:10.6342/NTU201800167

By induction, it suffices to show the case $E^p \subset k$.

Let $A_0 = k[T]$ and $A = A_0 \otimes_k E = E[T]$, and c_A the flat connection of $\mathcal{D}_E$ on A. Denote by $\Delta : A \to A \otimes_E A$ the co-multiplication; this is an E-algebra homomorphism. Since T is defined over k, one has $\Delta = \Delta_0 \otimes E$ with the co-multiplication $\Delta_0 : A_0 \to A_0 \otimes_k A_0$. Thus, by Proposition 114 one has a commutative diagram

$$\begin{tikzcd}
A \arrow[r, "\Delta"] \arrow[d, "c_A(D)"] & A \otimes_E A \arrow[d, "c_{A\otimes A}(D)"] \\
A \arrow[r, "\Delta"] & A \otimes_E A.
\end{tikzcd} \tag{5.32}$$

As $\chi \in X(T)$, one has $\Delta(\chi) = \chi \otimes \chi$. Put $f := \chi^{-1} \cdot c_A(D)(\chi)$. One computes

$$\begin{aligned}
\Delta(f) &= \Delta(\chi^{-1}) \cdot \Delta(c_A(D)(\chi)) \\
&= \chi^{-1} \otimes \chi^{-1} \cdot c_{A\otimes A}(D)(\chi \otimes \chi) \\
&= \chi^{-1} \otimes \chi^{-1} \cdot [1 \otimes \chi \cdot (c_A(D)(\chi) \otimes 1) + \chi \otimes 1 \cdot (1 \otimes c_A(D)(\chi))] \\
&= f \otimes 1 + 1 \otimes f.
\end{aligned} \tag{5.33}$$

Write $f = \sum_{\psi \in X(T)} c_\psi \psi$ with characters c_ψ in $\bar{k}[T]$. It follows from

$$\Delta(f) = f \otimes 1 + 1 \otimes f = \sum c_\psi(\psi \otimes 1 + 1 \otimes \psi) = \sum c_\psi(\psi \otimes \psi)$$

that $c_\psi = 0$ if $\psi \neq 1$. For $\psi = 1$, it follows from $c_1(1 \otimes 1 + 1 \otimes 1) = c_1(1 \otimes 1)$ that $c_1 = 0$. Thus $f = 0$ and $c_A(D)\chi = 0$ for all $D \in \mathcal{D}_E$. This proves that $\chi \in A_0$, by Proposition 114. ∎

5.4 Three more proofs of Theorem 94

5.4.1 Ono's proof

Let T be an algebraic tori over k. It suffices to show that any character $\chi \in X(T)_{\bar{k}} = \mathrm{Hom}_{\bar{k}}(T, \mathbb{G}_{\mathrm{m}})$ is defined over k_s.

Since $\bar{k}/k_s$ is primary, applying Theorem 95 to $A = T$ and $B = \mathbb{G}_{\mathrm{m}}$, we have an isomorphism

$$\mathrm{Hom}_{k_s}(T, \mathbb{G}_{\mathrm{m}}) \xrightarrow{\sim} \mathrm{Hom}_{\bar{k}}(T, \mathbb{G}_{\mathrm{m}}).$$

Thus, every character is defined over k_s. ∎

We remark that T. Ono did not provide a proof of Theorem 95 for tori. Instead he pointed out (see [32, Lemma 1.2.1]) that the proof of Chow's theorem [8] also works for tori. Note that Chow's proof was established upon Weil's foundation. Brian Conrad [9, Theorem 3.19] gave a modern proof of Chow's Theorem. We extend Conrad's idea and prove Theorem 95; see Section 5.5. The main ingredient is Grothendieck's faithfully flat descent.

5.4.2 Tits' proof

Let T be an algebraic tori over k and $k[T]$ the coordinate ring. Choose a k-basis $\{\varphi_i\}$ for $k[T]$. Let $\chi \in X(T)_{\bar{k}} \subset \bar{k}[T] = k[T] \otimes_k \bar{k}$ be a character over $\bar{k}$. We shall show that $\chi \in k_s[T]$.

Write $\chi = \sum_{i=1}^n a_i \varphi_i$, where $a_i \in \bar{k}$. If $\mathrm{char}\, k = 0$, there is nothing to prove. Thus, we assume $\mathrm{char}\, k = p > 0$. There exists a p-power $q = p^r$ such that $a_i^q \in k_s$ for all i. Then $\chi^q = \sum_i a_i^q \varphi_i^q$ lies in $k_s[T]$. For $t \in T$, we have $\chi^q(t) = \chi(t^q) = \sum_i a_i \varphi_i(t^q)$, because χ is a character. So,

$$\chi^q = \sum_i a_i \varphi_i', \quad \varphi_i'(t) := \varphi_i(t^q).$$

doi:10.6342/NTU201800167

Using the fact that the morphism $T \to T$, $t \mapsto t^q$, is defined over k and is surjective, one easily shows that $\{\varphi_i'\}$ is a k_s-linearly independent subset in $k[T]$. If V_0 is the k_s-subspace generated by φ_i', then $V_0 \otimes_{k_s} \bar{k}$ is a subspace of $\bar{k}[T]$ defined over k_s, and we have $\sum a_i \varphi_i' \in k_s[T] \cap V_0 \otimes_{k_s} \bar{k} = V_0$. This shows that $a_i \in k_s$ and $\chi \in k_s[T]$. ∎

5.4.3 Tate's proof

We include Tate's proof [3, Proposition 1.5] for the sake of completeness. In fact Tate's proof is close to Tit's but it uses the language in Weil's foundation. Again it suffices to show that if χ is a character defined over a finite inseparable extension of k, then it is defined over k. Again we can assume $\operatorname{char} k = p > 0$. Let q be a p-power so that $\chi \in k^{1/q}$. One has $\chi(t^q) = \chi^q(t) \in k(t)$, then $\chi(t^q) \in k(t) \cap k^{1/q}(t^q)$ $(t \in T)$. But if t is generic over k, the field $k(t)$ is linearly disjoint of $\bar{k}$, and then $k(t) \cap k^{1/q}(t) = k(t^q)$ and $\chi(t^q) \in k(t^q)$. The element t^q is also generic over k, because $x \mapsto x^q$ is a bijective morphism from T to itself; the inclusion $\chi(t^q) \in k(t^q)$ then shows that χ is defined over k. ∎

5.5 Chow's theorem for semi-abelian varieties

In this section we shall give a proof of Theorem 95. As mentioned in Section 5.1, the main ingredient is Grothendieck's faithfully flat descent.

5.5.1 Faithfully flat descent

We recall some basic terminology needed to describe the flat descent.

Definition 115.

(1) A ring homomorphism $A \to B$ of commutative rings is said to be *flat* if the functor $\otimes_A B : A\text{-mod} \to B\text{-mod}$ is exact, where A-mod denotes the category of A-modules.

(2) A morphism $f : X \to Y$ of schemes is said to be *flat* if for any point $x \in X$ with $y = f(x)$, the ring homomorphism $\mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$ of local rings is flat. We say f is *faithfully flat* if it is flat and surjective.

(3) We say f is *quasi-compact* if the pre-image $f^{-1}(U)$ of every open affine subscheme U of Y is quasi-compact, that is, it is a finite union of open affine subschemes.

(4) A scheme X is said to be *quasi-affine* if it is quasi-compact and it is contained in an affine scheme. A morphism f of schemes is said to be *quasi-affine* if it is quasi-compact and the pre-image $f^{-1}(U)$ of every open affine subscheme U of Y is quasi-affine.

(5) Let Y be a Noetherian scheme. A morphism $f : X \to Y$ of schemes of finite type is said to be *projective* (resp. quasi-projective) if X is isomorphic to a closed (resp. locally closed) subscheme of the projective scheme $\mathbf{P}^N_Y$ for some positive integer N.

We first describe the flat descent for morphisms. Let $p : S' \to S$ be a morphism of base schemes, and let $X \to S$ be a morphism of schemes. For any integer $n > 1$, write $S^{(n)} := S' \times_S \cdots \times_S S'$ (n times), and $X^{(n)} := X \times_S S^{(n)}$. Let $p_1, p_2 : S'' := S^{(2)} \to S'$ be two projection maps.

Proposition 116. *Let $p : S' \to S$ be a faithfully flat and quasi-compact morphism of base schemes. Let X and Y be two schemes over S and let $f' : X' \to Y'$ a morphism of schemes over S'. If $p_1^*(f') = p_2^*(f')$, then there is a unique morphism $f : X \to Y$ over S such that $f' = p^*(f)$.*

Proof. See [15, A.III.1 Lemma].

We now describe the flat descent for objects. For any two integers $1 \le i < j \le 3$, denote by $p_{ij} : S^{(3)} \to S^{(2)}$ the projection map at the i-th and j-th components. Let $p_i^n : S^{(n)} \to S'$ denote the i-th projection map. Clearly, one has $p_1 p_{ij} = p_i^3$ and $p_2 p_{ij} = p_j^3$ in $\mathrm{Hom}(S^{(3)}, S')$. If X'/S' is a scheme over S' and $\alpha : p_1^*(X') \to p_2^*(X')$ is a morphism over $S^{(2)}$, then the pull-back morphism $p_{ij}^*(\alpha)$ is a morphism

$$p_{ij}^*(\alpha) : (p_i^3)^*(X') \to (p_j^3)^*(X').$$

Definition 117.

(1) Let $p : S' \to S$ be a faithfully flat and quasi-compact morphism of schemes. A *descent datum* for p consists of a pair $(X'/S', \alpha)$, where X'/S' is a scheme over S' and $\alpha : p_1^*(X') \xrightarrow{\sim} p_2^*(X')$ is an isomorphism of schemes over S'' satisfying the condition

$$p_{23}^*(\alpha) \circ p_{12}^*(\alpha) = p_{13}^*(\alpha). \tag{5.34}$$

(2) A descent datum $(X'/S', \alpha)$ is said to be *effective* if there exits a scheme X/S over S and an isomorphism $p^*(X) \simeq X'$ over S'.

Theorem 118. *Let $(X'/S', \alpha)$ be a descent datum for a faithfully flat and quasi-compact morphism $p : S' \to S$ of base schemes. If X'/S' is quasi-affine, then $(X'/S', \alpha)$ is effective.*

Proof. See [15, A.III.6 Proposition].

Remark 119. A classical Weil descent states that if $p : S' \to S$ is $\operatorname{Spec} K \to \operatorname{Spec} k$ for an algebraic separable field extension K/k and X' is a quasi-projective algebraic variety over K, then any descent datum $(X'/K', \alpha)$ is effective. Comparing Weil's descent and Theorem 118, one may ask whether the assumption of X' in Grothendieck's flat descent can be weakened by assuming only that X' is quasi-projective. However, this is not the case. Indeed, there exists an étale covering $S' \to S$ of schemes and a descent datum $(X'/S', \alpha)$ relative to $S' \to S$ such that $X' \to S'$ is projective, but the descent datum is not effective in the category of schemes. See [38, Tag 08KF] for a counterexample.

doi:10.6342/NTU201800167

5.5.2 Proof of Theorem 95

Recall that a semi-abelian variety is a connected commutative smooth algebraic group G which is an extension of abelian variety by an algebraic torus, that is, the affine subgroup of G is an algebraic torus.

Recall the statement of Theorem 95 that X and Y are two semi-abelian varieties over a field k, and K/k is a primary field extension. We must show that any morphism $f : X_K \to Y_K$ over K is defined over k.

Let $p : S := \operatorname{Spec} K \to \operatorname{Spec} k$ and $p_1, p_2 : S'' := S \times_{Speck} S \to S$ be the projection maps. Put $K' := K \otimes_k K$. Since K/k is a primary extension, the scheme S'' is irreducible and hence connected. Now let $f \in \operatorname{Hom}_K(X_K, Y_K)$. By Proposition 116, it suffices to show that $p_1^*(f) = p_2^*(f)$.

Let $x = \Delta : \operatorname{Spec} K = S \to S'' = S \times_{\operatorname{Spec} k} S$ be the K-valued point of S'' defined by the diagonal morphism. As $p_i \circ \Delta = id$, one has $x^* p_1^*(f) = x^* p_2^*(f)$, i.e. the morphisms $p_1^*(f)$ and $p_2^*(f)$ agree on the fiber over the point x. Let ℓ be any prime different from $\operatorname{char} k$. The morphism $p_i^*(f) : X_{K'} \to Y_{K'}$ induces a morphism $X_{K'}[\ell^n] \to Y_{K'}[\ell^n]$, where $X_{K'}[\ell^n]$ denotes the ℓ^n-torsion finite subgroup scheme of $X_{K'}$. Since $X_{K'}[\ell^n]$ has order prime to $\operatorname{char} k$, it is a finite étale group scheme. Denote by $p_i^*(f)[\ell^n]$ the restriction of $p_i^*(f)$ to the finite group scheme $X_{K'}[\ell^n]$. As $p_1^*(f)_x = p_2^*(f)_x$, one has $p_1^*(f)[\ell^n]_x = p_2^*(f)[\ell^n]_x$. Since $X_{K'}[\ell^n]$ is finite étale over K' and S'' is connected, the rigidity of étale morphisms [31, I. Corollary 3.13, p. 26] shows that $p_1^*(f)[\ell^n] = p_2^*(f)[\ell^n]$. Now the collection $\{X_{K'}[\ell^n]\}_n$ forms a Zariski dense subset of $X_{K'}$, and it follows that $p_1^*(f) = p_2^*(f)$. This proves Theorem 95. ∎

5.5.3 A descent lemma

The purpose of this subsection is to prove another descent result. This yields a second and simpler proof of Theorem 95 and hence yields another proof of Theorem 94 using

doi:10.6342/NTU201800167

Ono's approach.

Lemma 120. *Let X and Y be k-schemes locally of finite type. Let $\{X_n\}_{n\geq 1}$ be a sequence of closed k-subschemes of X. Suppose that the scheme-theoretic closure of the image $\coprod X_n \to X$ is equal to X. Let K/k be a field extension, and $f : X \otimes_k K \to Y \otimes_k K$ a K-morphism. If the morphisms $f_n := f|_{X_n} : X_n \otimes K \to Y \otimes K$ are defined over k for all n, then f is defined over k.*

Proof. We first show that we can reduce the statement to the case where both X and Y are affine. Let U_i and V_i be affine coverings of X and Y, respectively, such that $f(U_i \otimes K) \subset V_i \otimes K$. Clearly, $\{X_n \cap U_i\}_{n\geq 1}$ is a sequence of closed subschemes of U_i satisfying the same condition of the lemma. If each morphism $f_i := f|_{U_i \otimes K}$ is defined over k, then we can glue f_i to be a map g which is defined over k and one has $g \otimes K = f$.

Write $X = \operatorname{Spec} A$ and $Y = \operatorname{Spec} B$. Let I_n be the ideal of A defining the closed subscheme X_n. The map f is given by a map also denoted by $f : B \otimes K \to A \otimes K$. The assumptions say that the induced map $f_n : B \otimes_k K \to (A/I_n) \otimes_k K$ is defined over k, that is, $f_n(B) \subset A/I_n$, and that the natural map $A \to \prod_n A/I_n$ is injective. Since the image $f(B)$ is contained in $A \otimes K$ and $\prod_n A/I_n$, it is contained in A. This proves the lemma. ∎

5.5.4 Second proof of Theorem 95

Let $f \in \operatorname{Hom}_K(X_K, Y_K)$. Let ℓ be a prime different from $\operatorname{char} k$. Since $X[\ell^n]$ and $Y[\ell^n]$ are finite étale group schemes, the functor $\mathcal{H}(S) := \operatorname{Hom}_S(X[\ell^n] \times S, Y[\ell^n] \times S)$ for any k-scheme S is representable by a finite $\mathbb{Z}/\ell^n$-module scheme over k. In particular, one has $\mathcal{H}(K) = \mathcal{H}(k)$ for any primary field extension K/k. Thus, the restriction of f to $X[\ell^n] \otimes_k K$ is defined over k for any n. Since the collection $\{X[\ell^n]\}_{n\geq 1}$ of finite étale group subschemes forms a Zariski dense subset of X and X is reduced, it follows from Lemma 120 that f is defined over k. ∎

5.6 Bounds for splitting fields of tori

5.6.1 Splitting fields

Let T be an algebraic torus over a field k of dimension d. The group of characters of T. denoted $X(T)$, is a finite free $\mathbb{Z}$-module of rank d equipped with a continuous action of the Galois group $\Gamma_k := \mathrm{Gal}(k_s/k)$. Thus, one has a group homomorphism

$$\rho_T : \Gamma_k \to \mathrm{Aut}(X(T)) \simeq \mathrm{GL}_d(\mathbb{Z}). \tag{5.35}$$

The spitting field of T by definition is the smallest field extension k_T of k such that T splits over k_T. Clearly, $\ker \rho_T = \mathrm{Gal}(\bar{k}/k_T) =: \Gamma_{k_T}$ and ρ_T induces a faithful representation of $\mathrm{Gal}(k_T/k)$ on $X(T)$. In particular, k_T is a finite Galois extension of k. For studying algebraic tori, it is useful to bound the degree of the splitting field of an algebraic torus.

For any positive integer $d \geq 1$, let $\mathrm{Max}(d, \mathbb{Q})$ denote the maximal order of finite subgroups in $\mathrm{GL}_d(\mathbb{Q})$. Clearly, one has $[k_T : k] \leq \mathrm{Max}(d, \mathbb{Q})$ for any d-dimensional algebraic torus T/k. The following lemma provides explicit bounds for $[k_T : k]$.

For any integer $N \geq 1$, let $T[N]$ denote the N-torsion finite group subscheme of T. When N is prime-to-$\mathrm{char}\, k$, let $k(T[N])$ be the field extension of k in k_s jointing all the coordinates of points in $T[N](k_s)$, and let

$$\rho_{T,N} : \Gamma_k \to \mathrm{Aut}(T[N]_{k_s}) \simeq \mathrm{GL}_d(\mathbb{Z}/N\mathbb{Z}). \tag{5.36}$$

Clearly, $k(T[N])$ is the Galois separable extension with $\Gamma_{k(T[N])} = \ker \rho_{T,N}$.

Lemma 121. *Let T be a d-dimensional algebraic torus over k.*

(1) *For any prime-to-*$\mathrm{char}\, k$ *positive integer N with $N \geq 3$, one has $k_T \subset k(T[N])$ and $[k_T : k] \mid \# \mathrm{GL}_d(\mathbb{Z}/N\mathbb{Z})$.*

(2) *If* $\mathrm{char}\, k \neq 2$, *then $[k_T : k] \mid 2\# \mathrm{GL}_d(\mathbb{F}_2)$.*

doi:10.6342/NTU201800167

Proof. This follows from the fact that the reduction map $\mathrm{GL}_d(\mathbb{Z}) \to \mathrm{GL}_d(\mathbb{Z}/N\mathbb{Z})$ induces an injective map on any finite subgroup G if $N \geq 3$ and a map with $\ker \cap G \subset \{\pm 1\}$ if $N = 2$. This fact follows immediately from a lemma of Serre. ∎

Definition 122. We say k is a *Hilbertian field* if it satisfies one of the following variants of the Hilbert irreducibility property:

(a) For any irreducible and separable polynomial $f(x,t) = a_d(t)x^d + \cdots + a_0(t) \in k(t)[x]$ over $k(t)$ of degree $n \geq 1$, where x and t are indeterminates, there exist infinitely many specializations $t = t_0 \in k$ such that $f(x, t_0)$ is an irreducible and separable polynomial over k of degree d.

(b) For any $n \geq 1$ and any finite separable extension $K_t/k(t_1, \ldots, t_n)$ of a rational function field $k(t_1, \ldots, t_n)$ of transcendental degree n, there exist infinitely many specializations $t \rightsquigarrow t_0 \in k$ such that K_{t_0} is a finite separable extension of k of same degree $[K_t : k(t_1, \ldots, t_n)]$.

It is well known that any global field is Hilbertian and if k is any field and K is a finite extension of the rational field $k(t)$ then K is Hilbertian (cf. [13, p. 155]).

We shall prove

Theorem 123. *For any $d \geq 1$ and any Hilbertian field k of characteristic zero, there exists a finite Galois extension K/k with group isomorphic to a finite subgroup $G \subset \mathrm{GL}_d(\mathbb{Q})$ of order $\mathrm{Max}(d, \mathbb{Q})$.*

As an immediate consequence of Theorem 123, we attain the best bound for $[k_T : k]$.

Corollary 124. *For any $d \geq 1$, there exists a d-dimensional algebraic torus T over k such that $[k_T : k] = \mathrm{Max}(d, \mathbb{Q})$.*

doi:10.6342/NTU201800167

5.6.2 Proof of Theorem 123

According to [14], the signed permutation group $\{\pm 1\}^d \rtimes S_d \subset \mathrm{GL}_d(\mathbb{Q})$ attains the maximal order of finite subgroups of $\mathrm{GL}_d(\mathbb{Q})$ except for $d \in \{2, 4, 6, 7, 8, 9, 10\}$. The exceptional cases are listed in Table 1 with maximal-order finite subgroups. Here $W(D)$ denotes the Weyl group of the root system with Dynkin diagram D.

d	Maximal-order subgroup G	$\mathrm{Max}(d, \mathbb{Q}) = \#G$
2	$W(G_2)$	12
4	$W(F_4)$	1152
6	$\langle W(E_6), -I\rangle$	103680
7	$W(E_7)$	2903040
8	$W(E_8)$	696729600
9	$W(E_8) \times W(A_1)$	1393459200
10	$W(E_8) \times W(G_2)$	8360755200
all other d	$W(B_d) = W(C_d) = \{\pm 1\}^d \rtimes S_d$	$2^d d!$

Table 5.1: Maximal-order finite subgroups of $\mathrm{GL}_d(\mathbb{Q})$

Theorem 123 follows from the following proposition.

Proposition 125. *Let G be the finite subgroup as in Table 1. For any Hilbertian field k of characteristic zero, there exists a finite Galois extension K/k with group G.*

Proof. Note that G is a finite reflection group W except $d = 6$. Regarding $\mathrm{GL}_n(\mathbb{Q}) = \mathrm{GL}(V)$ and putting $V_k = V \otimes_{\mathbb{Q}} k$, where $V = \mathbb{Q}^n$ and $V_k = k^n$, one has $\mathrm{GL}_n(k) = \mathrm{GL}(V_k)$. In this case, $W \subset \mathrm{GL}_n(V_k)$ is also a finite reflection group acting on V_k. By a theorem of Chevalley [7], the invariant subring $k[x_1, \ldots, x_d]^W$ is $k[I_1, \ldots, I_d]$ for d invariant homogeneous algebraically independent polynomials I_i over k. Therefore, the invariant subfield $k(x_1, \ldots, x_d)^G = k(I_1, \ldots, I_d)$ is a purely transcendental extension of k except $d = 6$.

For $d = 6$, the invariant subring $k[x_1, \ldots, x_6]^{W(E_6)}$ is generated by invariant homogeneous polynomials $I_2, I_5, I_6, I_8, I_9, I_{12}$ of degrees $2, 5, 6, 8, 9, 12$, respectively. The element

$-I \in G$ maps $I_j \mapsto (-)^j I_j$. Thus, $k[x_1, \dots, x_6]^G = k[I_2, I_6, I_8, I_{12}, I_5^2, I_5 I_9, I_9^2]$ and hence the fixed subfield $k(x_1, \dots, x_6)^G = k(I_2, I_6, I_8, I_{12}, I_5^2, I_5 I_9)$ is rational over k.

We have proved that $k(x_1, \dots, x_d)^G$ is rational over k for all d. By the Hilbert irreducibility property, there exists a finite Galois extension K of k with Galois group isomorphic to G. ■

Consider pairs (Γ, ρ) which consist of a finite group Γ together with a group monomorphism $\rho : \Gamma \to \mathrm{GL}_d(\mathbb{Z})$ for some positive integer d. Two such pairs $(\Gamma_i, \rho_i : \Gamma_i \to \mathrm{GL}_{d_i}(\mathbb{Z}))$ $(i = 1, 2)$ are said to be *equivalent* if $d_1 = d_2$ and there exist an automorphism $\alpha : \Gamma_1 \xrightarrow{\sim} \Gamma_2$ and an element $g \in \mathrm{GL}_{d_1}(\mathbb{Z})$ such that $g\rho_1(\gamma)g^{-1} = \rho_2(\alpha(\gamma))$ for all $\gamma \in \Gamma_1$. Similarly, we consider pairs $(\Gamma, \rho_{\mathbb{Q}} : \Gamma \hookrightarrow \mathrm{GL}_d(\mathbb{Q}))$ and define equivalence classes on all such pairs in the same way. Denote by $\mathcal{T}$ (resp. $\mathcal{T}_{\mathbb{Q}}$) the set of equivalence classes of pairs (Γ, ρ) (resp. $(\Gamma, \rho_{\mathbb{Q}})$) as above.

To any algebraic tori T over k we associate a triple $(k_T, \mathrm{Gal}(k_T/k), \rho_T)$, where k_T is the splitting field of T, $\mathrm{Gal}(k_T/k)$ is the Galois group of k_T/k, and $\rho_T : \mathrm{Gal}(k_T/k) \to \mathrm{GL}_d(\mathbb{Z})$ $(d = \dim T)$ is the faithful representation induced by (5.35). By (5.3), the triple $(k_T, \mathrm{Gal}(k_T/k), \rho_T)$ determines T up to isomorphism. The pair $(\mathrm{Gal}(k_T/k), \rho_T)$ is called the type of T, which is uniquely determined by T up to equivalence. Thus, the association $(\mathrm{Gal}(k_T/k), \rho_T)$ to T induces a map from the set of isomorphism classes of tori over k to $\mathcal{T}$. The pre-image of each type (Γ, ρ) consists of all finite Galois extensions k' of k in k_s such that $\mathrm{Gal}(k'/k) \simeq \Gamma$. Let $\rho_{T,\mathbb{Q}} : \mathrm{Gal}(k_T/k) \to \mathrm{GL}_d(\mathbb{Q})$ denote the representation induced by the inclusion $\mathrm{GL}_d(\mathbb{Z}) \subset \mathrm{GL}_d(\mathbb{Q})$. Then the association $(\mathrm{Gal}(k_T/k), \rho_{T,\mathbb{Q}})$ to T induces a map from the set of isogeny classes of tori over k to $\mathcal{T}_{\mathbb{Q}}$, and the pre-image of $(\Gamma, \rho_{\mathbb{Q}})$ is the same as that of (Γ, ρ).

For any positive integer d, denote by $\mathcal{T}_d \subset \mathcal{T}$ (resp. $\mathcal{T}_{d,\mathbb{Q}} \subset \mathcal{T}_{\mathbb{Q}}$) the subset consisting of all pairs (Γ, ρ) (resp. $(\Gamma, \rho_{\mathbb{Q}})$) of degree d. It is obvious that $\#\mathcal{T}_1 = 2$ and $\#\mathcal{T}_{1,\mathbb{Q}} = 2$. We know from [42] and [40] that $\#\mathcal{T}_2 = 17$ and $\#\mathcal{T}_3 = 74$. Finite subgroups of $\mathrm{GL}_d(\mathbb{Q})$

up to conjugate for $d \leq 4$ are classified in [5], and we have $\#\mathcal{T}_{3,\mathbb{Q}} = 32$ and $\#\mathcal{T}_{4,\mathbb{Q}} = 227$ (also see [25, pp. 54, 69]).

doi:10.6342/NTU201800167

Bibliography

[1] N. Berry, A. Dubickas, N. Elkies, B. Poonen and C. Smyth, The conjugate dimension of algebraic numbers. *Q. J. Math.* **55** (2004), no. 3, 237–252.

[2] A. Borel, *Linear algebraic groups.* Second edition. Graduate Texts in Mathematics, **126**. Springer-Verlag, New York, 1991.

[3] A. Borel and J. Tits, Groupes réductifs. *Inst. Hautes Études Sci. Publ. Math.* **27** (1965), 55–150.

[4] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models.* Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 21. Springer-Verlag, Berlin, 1990. x+325 pp.

[5] Harold Brown, Rolf Bulow, Joachim Neubuser, Hans Wondratschek and Hans Zassenhaus, *C*rystallographic groups of four-dimensional space. Wiley Monographs in Crystallography. Wiley-Interscience, New York-Chichester-Brisbane, 1978. xiv+443 pp.

[6] Ching-Li Chai, Brian Conrad and Frans Oort, *Complex multiplication and lifting problems.* Mathematical Surveys and Monographs **195**. AMS, 387 pp.

[7] Claude Chevalley, Invariants of finite groups generated by reflections. *Amer. J. Math.* **77** (1955), 778–782.

[8] Wei-Liang Chow, Abelian varieties over function fields. *Trans. Amer. Math. Sci.* **78**, (1955). 253–275.

doi:10.6342/NTU201800167

[9] B. Conrad, Chow's K/k-image and K/k-trace, and the Lang-Néron theorem. Enseign. Math. **52** (2006), 37–108.

[10] C. W. Curtis and I. Reiner, *Methods of representation theory. Vol. I. With applications to finite groups and orders.* Pure and Applied Mathematics. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1981, 819 pp.

[11] Dummit, D. S. Foote, R. M.,Abstract Algebra, 2004. Third edition. John Wiley & Sons, Inc., Hoboken, NJ, 2004. xii+932 pp.

[12] Shizuo Endo and Ming-Chang Kang, Function fields of algebraic tori revisited. *Asian J. Math.* **21** (2017), no. 2, 197–224.

[13] Michael D. Fried and Moshe Jarden, *Field arithmetic.* Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 11. Springer-Verlag, Berlin, 1986, 458 pp.

[14] Walter Feit, Orders of finite linear groups. *Proceedings of the First Jamaican Conference on Group Theory and its Applications (Kingston, 1996)*, 9–11, Univ. West Indies, Kingston.

[15] E. Freitag and R. Kiehl, *Etale cohomology and the Weil conjecture. Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*, **13.** Springer-Verlag, Berlin, 1988. xviii+317 pp.

[16] A. Grothendieck, Revêtements étales et groupe fondamental (SGA 1), Lecture Notes in Math., vol. 224, Springer-Verlag, Springer-Verlag, 1971

[17] A. Heller and I. Reiner, Representations of cyclic groups in rings of integers, I, *Ann. of Math. (2)* **76** 1962 73—92.

[18] A. Heller and I. Reiner, Representations of cyclic groups in rings of integers, II, *Ann. of Math. (2)* **77** 1963 318—328.

[19] A. Heller, On group representations over a valuation ring, *Proc. Nat. Acad. Sci. U.S.A.* **47** 1961 1194—1197.

[20] Thomas W. Hungerford, *Algebra.* Graduate Texts in Mathematics, 73. Springer-Verlag, New York-Berlin, 1980. 502 pp.

[21] A. Jones, Groups with a finite number of indecomposable integral representations, *Michigan Math. J.* **10** 1963 257—261.

[22] Ming-Chang Kang, Noether's problem for metacyclic p-groups. *Adv. Math.* **203** (2006), no. 2, 554–567.

[23] Ming-Chang Kang, Retract rationality and Noether's problem. *Int. Math. Res. Not.*IMRN 2009, no. 15, 2760–2788.

[24] Ming-Chang Kang, Noether's problem for p-groups with a cyclic subgroup of index p^2. *Adv. Math.* **226** (2011), no. 1, 218–234.

[25] Ming-Chang Kang and Jian Zhou, The rationality problem for finite subgroups of $GL_4(\mathbb{Q})$. *J. Algebra* **368** (2012), 53–69.

[26] I. Kersten, Noether's problem and normalization. *Jahresber. Deutsch. Math.-Verein.* **100** (1998), no. 1, 3–22.

[27] Hidetaka Kitayama, Noether's problem for four and five dimensional linear actions. *J. Algebra* **324** (2010), no. 4, 591–597.

[28] Hidetaka Kitayama and Aiichi Yamasaki, The rationality problem for four-dimensional linear actions. *J. Math. Kyoto Univ.* **49** (2009), no. 2, 359–380.

[29] S. Lang, *Abelian Varieties.* Interscience, New York, 1959.

[30] Myrna Pike Lee, Integral representations of the dihedral groups of order 2p, *Trans. Amer. Math. Soc.* **110** 1964 213—231.

doi:10.6342/NTU201800167

[31] J. S. Milne, *Etale cohomology. Princeton Mathematical Series*, **33.** Princeton University Press, 1980. xiii+323 pp.

[32] T. Ono, Arithmetic of algebraic tori. *Ann. Math.* **74** (1961), 101–139.

[33] Irving Reiner, Integral representations of cyclic groups of prime order, *Proc. Amer. Math. Soc.* **8** (1957), 142—146.

[34] Irving Reiner, Failure of the Krull-Schmidt theorem for integral representations, *Michigan Math. J.* **9** 1962 225—231.

[35] M. Rosenlicht, Some rationality questions on algebraic groups. *Ann. Mat. Pura Appl.* (4) **43** (1957), 25–50.

[36] Jean-Pierre Serre, Linear representations of finite groups. Translated from the second French edition by Leonard L. Scott. Graduate Texts in Mathematics, Vol. **42**. Springer-Verlag, New York-Heidelberg, 1977. x+170 pp. ISBN: 0-387-90190-6

[37] T.A. Springer, *Linear algebraic groups.* Second edition. Progress in Mathematics, **9**. Birkhauser Boston, 1998. xiv+334 pp.

[38] The Stack Project Authors, Stacks Project, http://stacks.math.columbia.edu, (2017).

[39] R. Swan, Stacks Project,Induced representations and projective modules, *Annals of Mathematics Second Series, Vol.***71, No. 3** *(May, 1960), pp. 552-578*

[40] Kenichi Tahara, On the finite subgroups of $\mathrm{GL}(3,\mathbb{Z})$*. Nagoya Math. J.* **41** *(1971) 169–209.*

[41] J. Tits, Lectures on Algebraic Groups. Department of Mathematics, Yale University, 1970.

doi:10.6342/NTU201800167

[42] *V. E. Voskresenski, On two-dimensional algebraic tori. Izv. Akad. Nauk SSSR Ser. Mat. 29 1965 239—244.*

[43] *P. Webb, A course on finite group representation theory, 2016. http://www-users.math.umn.edu/ webb/RepBook/RepBookLatex.pdf*

[44] *Aiichi Yamasaki, Some cases of four dimensional linear Noether's problem. J. Math. Soc. Japan* **62** *(2010), no. 4, 1273–1288.*

[45] *C.-F. Yu, On the existence of maximal orders. Int. J. Number Theory* **7** *(2011), no. 8, 2091–2114.*

doi:10.6342/NTU201800167