

Part III (1996-7) Topics in representation theory

This will be a 24 lecture course on representations of finite groups, split roughly into three parts: 1. Finite dimensional algebras; 2. Integral representations; 3. Some applications to presentation theory.

The first part will cover basic material that everyone must know about group algebras of finite groups. The middle section will be an introduction to several important topics in integral representation theory, culminating in Swan's theorems on the structure of projective modules over integral group rings of finite groups. In the final part of the course results and methods from both of the earlier parts will be used to discuss some striking results in the more specialised area of relation modules of finite groups.

Prerequisites. The Part IB/IIA course 'Rings and Modules' and the Part IIB course 'Groups and Representation Theory'. In the second part of the course I shall assume some knowledge on tensor products and localisation from the Part III course 'Commutative Algebra'.

Books. **J.L. Alperin.** *Local representation theory. Cambridge studies in advanced mathematics 11* (Cambridge University Press, paperback edition 1993) is perhaps the best for the first part of the course. There are many other books that would do, for example, **I.N. Herstein** *Noncommutative rings* (Wiley, 1968) Alperin's book goes on to discuss some of the main theorems of Brauer, which are of the utmost importance if you want to understand finite groups; Herstein's goes on to give an introduction to some other topics in ring theory including simple algebras and the Brauer group. Two much more extensive and difficult books are **I. Reiner** *Maximal orders* (Academic Press, 1975) and **C.W. Curtis and I. Reiner** *Methods of Representation Theory Vol. I* (Wiley-Interscience, 1981). Everything that I shall do in the second and third parts of the course can be found in **K.W. Gruenberg** *Relation modules of finite groups. Regional conference series in mathematics, No. 25* (American Mathematical Society, 1976).

Outline schedule.

1. **Finite-dimensional algebras.** Simple modules, the radical, semi-simple modules, Wedderburn's theorems, rings with radical, indecomposable modules, Krull-Schmidt theorem.
2. **Integral representations.** Integral group rings, localisation techniques, projective modules, ZG -lattices, isomorphisms and local isomorphisms, genus, Bass's cancellation theorem; Swan's theorems on the structure of projective ZG -modules; corollaries on ZG -lattices and semi-local group rings.
3. **Some applications to presentation theory.** Presentations, relation modules, decompositions of relation modules into a projective part and a core; uniqueness of cores up to local isomorphism; the relation sequence, Schanuel's lemma; comparison of relation modules; local isomorphisms of minimal relations modules; presentation rank $pr(G)$ of a group G ; conditions for $pr(G)$ to be greater than n ; groups of arbitrarily high presentation rank; $pr(G)$ for soluble groups.

Depending on the time available I may be able to discuss (possibly without serious proof): Roiter's replacement theorem and its use to show relation cores form a genus; the formula for $pr(G)$ as the difference between the number of generators required for G and the number required for its augmentation ideal.

Topics In Representation Theory.

1.

I. Artinian Rings.

Let R be any ring. All rings will have a 1 ; these will be preserved under homomorphisms. Let $X \leq^+ R$. Write $X \triangleleft_r R$ to mean X is a right ideal of R , $X \triangleleft_l R$ for X a left ideal, and $X \triangleleft R$ to mean $X \triangleleft_r R$ and $X \triangleleft_l R$.

Define $X \triangleleft_r R$ to mean $rx \in X$ for $x \in X$ and $r \in R$, and $X \triangleleft_l R$ to mean $rx \in X$ for $x \in X$, $r \in R$.

If $Y \leq^+ R$, write XY for the additive subgroup generated by all xy , with $x \in X$, $y \in Y$: $XY = \{x_1y_1 + \dots + x_ny_n : n \geq 1, x_i \in X, y_i \in Y\}$.

R is Artinian \Leftrightarrow whenever $X_1 \geq X_2 \geq \dots \geq X_n \geq \dots$ are right ideals (or has "Min-r") then $\exists N$ such that $X_N = X_{N+1} = X_{N+2} = \dots$

Order the ideals by reverse inclusion: $X \triangleleft Y \Leftrightarrow Y \leq X$. By Zorn's Lemma, R is Artinian \Leftrightarrow in every non-empty set of right ideals there is a minimal one w.r.t. \leq .

(i.e., $\neq \emptyset$. $\exists X \in \mathcal{X}$ such that $Y \leq X$ and $Y \in \mathcal{X} \Rightarrow Y = X$).

Plan: Define $J(R) = J$, the Jacobson radical. Show that J is a nilpotent ideal containing every nilpotent ideal. R is semi-simple $\Leftrightarrow J=0$. R/J will be semi-simple.

Wedderburn I says that if R is Artinian semi-simple then R is uniquely a direct sum of simple Artinian rings.

Wedderburn II says that a simple Artinian ring is uniquely a matrix ring over a division ring.

Let M be an additive group. Say that M is a right R -module iff \exists a map $M \times R \rightarrow M$; $(\mu, r) \mapsto \mu r$, such that (i) $(\mu_1 + \mu_2)r = \mu_1r + \mu_2r$

$$(ii) \mu(r_1 + r_2) = \mu r_1 + \mu r_2$$

$$(iii) (\mu r_1)r_2 = \mu(r_1r_2)$$

$$(iv) \mu \cdot 1 = \mu.$$

Let $r^+ : \mu \mapsto \mu r$ for $\mu \in M$. (i) says $r^+ \in \text{End}_{\mathbb{Z}}(M)$. (iv) says that $1^+ = 1$. We have $t : R \rightarrow \text{End}_{\mathbb{Z}}(M)$ given by $r \mapsto r^+$. (ii) says that $(r_1 + r_2)^+ = r_1^+ + r_2^+$. (iii) says that $r_1^+ r_2^+ = (r_1 r_2)^+$. So t is a ring homomorphism.

Conversely, if we are given a homomorphism $t : R \rightarrow \text{End}_{\mathbb{Z}}(M)$ we can define μr to be μr^+ , and then (i)-(iv) all hold.

If $N \leq^+ M$ then N is a submodule $\Leftrightarrow \forall r \in N \quad \forall v \in N, rv \in R$.

If $X \leq^+ R$, write $NX = \{v_i x_1 + \dots + v_n x_n : v_i \in N, x_i \in X\}$. Then, N is a submodule $\Leftrightarrow NR \leq N \Leftrightarrow NR = N$.

Define M/N by $(N+u)r = N+ur$. M/N is the quotient module.

If M, N are right R -modules and $\theta: M \rightarrow N$ is a homomorphism of additive groups, then θ is an R -module homomorphism if $(ur)\theta = (u\theta)r \quad \forall u \in M, r \in R$. For example, $q: M \rightarrow M/N$ is the quotient homomorphism.

Isomorphism Theorem: If $\theta: M \rightarrow N$ is a homomorphism then $\ker \theta$ is a submodule and we have $M \xrightarrow{\theta} N$, where $\bar{\theta}$ is induced by θ and is injective. $(M/\ker \theta \cong M\theta)$.

Say that M is simple or irreducible \Leftrightarrow there are precisely two submodules: $0, M$. The submodules of M/N correspond 1-1 with the submodules of M which contain N , via $N \leq U \leq M \Leftrightarrow U/N$.

M/N is simple $\Leftrightarrow N \leq U \leq M$ implies $U=N$ or $U=M$, i.e., iff N is a maximal submodule of M . Write $N < \circ M$.

(1.1): Suppose M is finitely generated and non-zero. Then M has simple homomorphic images.

Proof: Suppose $M = u_1 R + \dots + u_d R$ with d minimal. Let $U=0$ if $d=1$, and $U=u_1 R + \dots + u_{d-1} R$ if $d>1$. Let \mathcal{F} be the set of all submodules that contain U but do not contain u_d . Partially order \mathcal{F} by inclusion, $N_1 \leq N_2$. Zorn's Lemma implies that \mathcal{F} has a maximal element N , say. So $N < \circ M$, and if $N < V < M$, then $u_d \in V$, so $V=M$, i.e., $N < \circ M$.

In $R=1.R$, submodules are right ideals. (1.1) says there are always maximal right ideals, $X \trianglelefteq R$, and R/X will be simple.

(1.2): If M is a simple R -module then $M \cong R/X$, some $X \trianglelefteq R$.

Proof: Let $m \in M$. Then $mR = \{mr : r \in R\}$. Consider $\theta: r \mapsto mr$. This is a homomorphism from R onto mR . Write $\mu^\circ = \{r : mr=0\}$ for the annihilator of m , the kernel of θ . We have $R/\mu^\circ \cong mR$. If M is simple and $0 \neq m$, then $mR = M$, and so $\mu^\circ \trianglelefteq R$.

Write $M^\circ = \text{annihilator of } M = \{r : Mr=0\} = \{r : mr=0 \quad \forall m \in M\}$.

(1.3) (i) $M^\circ = \bigcap_{m \in M} \mu^\circ_m$.

(ii) $M^\circ \triangleleft R$.

(iii) $M \cong M^\circ \Rightarrow M^\circ = M^\circ$.

Proof: (i) $M(rM^\circ) = (Mr)M^\circ \subseteq M \cdot M^\circ = 0$, so $M(rM^\circ) \subseteq M^\circ$.

(ii) Suppose $\theta: M \rightarrow M_1$ is a homomorphism. Then $(M\theta)M^\circ = (MM^\circ)\theta = 0\theta = 0$.

So, $M^\circ \subseteq (M\theta)^\circ$. Apply this to an isomorphism $\theta: M \rightarrow M_1$, get $M^\circ \subseteq M_1^\circ$, via θ' , get $M_1^\circ \subseteq M^\circ$.

Define $J = J(R)$, the Jacobson radical of R , to be $\bigcap_{\substack{M \text{-simple} \\ R\text{-module}}} M^\circ$

$$(1.4): J = \bigcap_{X \trianglelefteq R} X$$

Proof: Let $N = \bigcap_{X \trianglelefteq R} X$. If M is simple and $0 \neq M \in N$ then $\mu R = M$ and so $\mu^\circ \trianglelefteq R$, as in (1.2). $\mu^\circ \subseteq M^\circ$, so $N \subseteq M^\circ$, so $N \subseteq J$. Also, if $X \trianglelefteq R$, then R/X will be simple. So $(R/X)J = 0$, ie $RJ \leq X$, ie $J \leq X$. (This last bit: Suppose $N \leq M$. $M/N = \{N + \mu: \mu \in M\}$. $(N + \mu)r = N + \mu r = 0$ (in M/N) $\Leftrightarrow \mu r \in N$. So $(M/N)^\circ = \{\tau: M\tau \subseteq N\}$.)

Let $X \trianglelefteq R$. Then X is nilpotent $\Leftrightarrow X^n = 0$ for some $n \in \mathbb{N}$.

(1.5): (i) $J(R)$ contains every nilpotent ideal.

(ii) If R is Artinian then J is nilpotent.

Proof: (i) Let M be an R -module, let $X \trianglelefteq R$, then MX is a submodule. If M is simple, either $MX = 0$ or else $MX = M$, and so $M = MX = MX^2 = MX^3 = \dots$, which is impossible if X is nilpotent.

(ii) $J \supseteq J^2 \supseteq J^3 \supseteq \dots$. This must stop at, say, $K = J^n = J^{n+1} = J^{n+2} = \dots = J^{2n} = \dots$, so $K = K^2$. Suppose, if possible, that $K > 0$. Let $V = \sum X$, where $X \trianglelefteq R$, $X \subseteq K$, $XK = 0$. Obviously, $VK = 0$. Suppose $V < K$. Consider the right ideals of R contained in K and strictly containing V . (K is one of these). Let $V < W \leq K$ be a minimal element of this set. Clearly, $V \trianglelefteq W$, and so W/V is simple. Hence $(W/V)J = 0$, so $WJ \leq V$, so $WJK \leq VK = 0$. So $WK^2 = 0$, so $WK = 0$. $\Rightarrow W < V$ **.

Define R to be semi-simple if $J(R) = 0$.

We shall show that finitely generated modules over semi-simple Artinian rings are completely reducible.

(1.6): Let M be an f.g. module for an Artinian ring, R . Then M is Artinian [ie, M has the minimum condition on submodules, ie $M \in \text{min-}R$].

Proof: Let $M = \mu_1 R + \dots + \mu_d R$. If $d=1$, then $M \cong R/\mu$ is a homomorphic image of R , and the result is clear. If $d > 1$, let $U = \mu_1 R + \dots + \mu_{d-1} R$. By induction, U has min- R . Also, M/U is cyclic (on $\mu_d R$) and so has min- R . Suppose $V_1 \geq V_2 \geq V_3 \geq \dots$ be submodules of M . Then, $(U+V_1)/U \geq (U+V_2)/U \geq \dots$ must stop. And, $U \cap V_1 \geq U \cap V_2 \geq \dots$ must stop. So $\exists n$ with $U+V_n = U+V_{n+1} = U+V_{n+2} = \dots$ and $U \cap V_n = U \cap V_{n+1} = U \cap V_{n+2} = \dots$ $\Rightarrow V_n = (U \cap V_n) + V_{n+1}$ (Dedekind), $\Rightarrow V_n = U \cap V_{n+1} + V_{n+1} = V_{n+1}$.

(1.7): Let R be a ring and M a module with min- R . Let \mathcal{X} be a system of maximal submodules of M such that $\bigcap_{X \in \mathcal{X}} X = 0$. Let $0 \triangleleft U$ be a submodule. Then $M = U \oplus X_1 \oplus \dots \oplus X_n$ for suitable X_i in \mathcal{X} . Every simple image of M is isomorphic to M/X , some X in \mathcal{X} .

Proof: Let $T\mathcal{J}$ be the collection of all $X, n \dots nX_n = W$ with $X_i \in \mathcal{K}$ and $M = U + W$. Since $0 < U$ and $\bigcap_{X \in \mathcal{K}} X = 0$, there exists X in \mathcal{K} with $U \not\subseteq X$. Then $X < X+U = M$ and $X \in T\mathcal{J}$. Hence $T\mathcal{J} \neq \emptyset$, and so $T\mathcal{J}$ has a minimal member, W , say. We need $U \cap W = \emptyset$. Suppose not; as above, $\exists Y \in \mathcal{K}$ with $U \cap W + Y = M$, so $W = U \cap W + Y \cap W$, so $U + Y \cap W = W + U = M$. So $Y \cap W \in T\mathcal{J}$. Since W is minimal, and we get $Y \cap W = W$, ie $W \leq Y$, whence $Y = M - *$. Hence $U \cap W = 0$ and $M = U \oplus W$.

For the last sentence... if $0 \in \mathcal{K}$ then $M \cong M/0$ and we are done.

If $0 \notin \mathcal{K}$, suppose $Y < M$ (so that M/Y is the typical simple image.) Take W of the form $X, n \dots nX_n$ such that $M = Y \oplus W$. Take V of the same form, with $M = W \oplus V$. So $M/Y \cong W \cong M/V$. The only way this can be so is for $V = X \in \mathcal{K}$.

Think of $M = R$ and \mathcal{K} = system of all maximal right ideals. Hypothesis of (1.7) if R is Artinian and semi-simple. If X_1, \dots, X_n are in \mathcal{K} and $X, n \dots nX_n = 0$, then (1.7) will give every simple R -module isomorphic with one of R/X_i , $1 \leq i \leq n$. Of all the $X, n \dots nX_n$ with $X_i \in \mathcal{K}$, let W be a minimal one. If $0 < W$, then W cannot be in all X in \mathcal{K} . So $W \notin X \in \mathcal{K}$, some X , and so $W \cap X < W$, $* - so $W = 0$.$

(1.7') - Variation 1: Let R be a ring and M a module. Let \mathcal{K} be a system of minimal submodules of M such that $\sum_{X \in \mathcal{K}} X = M$. Let $0 < U$ be a submodule. If M/U has Max-R, then $M = U \oplus X_1 \oplus \dots \oplus X_n$ for suitable X_i in \mathcal{K} . Every simple submodule of M is isomorphic to X , some X in \mathcal{K} .

Proof: Exercise - 'dualise' the proof above.

Say M is faithful $\Leftrightarrow M^\circ = 0$. $\Leftrightarrow 0$ is the only ring element that acts like zero. Recall $t: R \rightarrow \text{End}_R(M)$, $r \mapsto r^+$, $\mu \mapsto \mu r$. t is a homomorphism with kernel M° . $R/M^\circ \hookrightarrow \text{End}_R(M)$.

(1.8): Let R be semi-simple Artinian. Then the following three statements are equivalent:

- (i) R is simple (ie, $0, R$ are the only ideals)
- (ii) R has a faithful simple module.
- (iii) R has a unique simple module.

Proof: (i) \Rightarrow (iii): Let M be a simple module. Then $0 \leq M^\circ \leq R$. Since R is simple, $M^\circ = 0$.

(iii) \Rightarrow (ii): Let M be a faithful simple R -module. So, $M^\circ = \bigcap_{\mu \in M} \mu^\circ = 0$, and all these μ° are maximal right ideals. By (1.7), any simple image of R is $\cong R/\mu^\circ$, by taking $\mathcal{K} = \{\mu^\circ : 0 \neq \mu \in M\}$ and $R \cong M$, and $R/\mu^\circ \cong M$.

(iii) \Rightarrow (i): Let M be the (unique) simple R -module. We need R simple. Let X be a maximal ideal of R (ie, R/X is a simple ring). We need $X = 0$.

Recall that any R/X -module is an R -module, annihilated by X .

~~R/X module, have $R \xrightarrow{\cong} R/X \rightarrow \text{End}_R(M)$. Let M_1 be any simple~~

~~R/X module, viewed as an R -module. Then $M_1^\circ = X$. Since M is unique, $J(R) = M^\circ = 0$. Hence $X = 0$ and R is simple.~~

(1.9): Let R be semisimple Artinian. Let M_1, M_2 be simple R -modules. If $M_1^\circ = M_2^\circ$ then $M_1 \cong M_2$.

Proof: M_1, M_2 are modules for R/M_1° , a semisimple ring with faithful simple module. By (1.8), (ii) \Rightarrow (iii), $M_1 \cong M_2$.

(1.10): R semisimple Artinian. If $0 < M$ is a f.g. R -module then M is a direct sum of simple modules.

Proof: By (1.6), M has min- R . Suppose (1.10) is false. Choose M_0 a f.g. submodule minimal wrt not being a direct sum of simple modules. Then M_0 is not simple. Let $U \subset M_0$. We have $M_0 = U + \mu R$ with $\mu \notin U$. Let $X = \{r \in R : \mu r \in U\}$, be the annihilator of $U + \mu R$ in R . By comment after (1.7), $R = X \oplus Y$, some $Y \triangleleft R$. Then $\mu R = \mu X + \mu Y$. So $M_0 = U + \mu Y = U \oplus \mu Y$. Hence, (ii) $\mu Y \cong M_0/U$ is simple, (iii) $U \cong M_0/\mu Y$ is f.g.

Wedderburn I: If R is semisimple Artinian then $R \cong R_1 \oplus \dots \oplus R_n$ where the R_i are simple Artinian, with uniqueness.

Proof: Let n be the number of simple modules, and let M_1, M_2, \dots, M_n be a list of them. Define $R_i = R/M_i^\circ$. Then R_i is Artinian semisimple with a faithful simple module M_i . So R_i is simple by (1.8). Consider $\theta: R \rightarrow R_1 \oplus \dots \oplus R_n$ via $\theta: r \mapsto (M_1^\circ + r, \dots, M_n^\circ + r)$. Now $\ker \theta = M_1^\circ \cap \dots \cap M_n^\circ = J(R) = 0$. To see θ is surjective, note M_i° are all different. We have $R = M_i^\circ + M_j^\circ$ if $j > 1$. Then $R = (M_1^\circ + M_2^\circ) \dots (M_1^\circ + M_n^\circ)$. Hence $R = M_1^\circ + M_2^\circ M_3^\circ \dots M_n^\circ = M_1^\circ + M_2^\circ \dots n M_n^\circ$. Let r run through this intersection. This shows that R_i is in the image of θ .

[Note: With this notation, $R = M_1^\circ \oplus (M_2^\circ \dots n M_n^\circ)$ and so if $N_j = \bigcap_{i \neq j} M_i^\circ$, $R = M_1^\circ \oplus N_j$, and it follows that $R = N_1 \oplus \dots \oplus N_j$.]

Conversely, suppose $R = R_1 \oplus \dots \oplus R_n$, where R_i are simple Artinian. Let M_i be the unique simple R_i -module viewed as an R -module. So $M_i^\circ = \{(\xi_1, \dots, \xi_{i-1}, 0, \xi_{i+1}, \dots, \xi_n) : \xi_j \in R_j\}$ and $R_i \cong R/M_i^\circ$. But $J(R) = 0$ because $M_1^\circ \cap \dots \cap M_n^\circ = 0$. Hence any simple R -module is of the form R/μ° , some μ in some M_i .

Wedderburn II: If R is simple Artinian then $R \cong \Delta_n$, the $n \times n$ matrix ring over a division ring Δ , with uniqueness. (If R is a ring, write R_n for the $n \times n$ matrix ring).

For R_n , write e_{ij} for the matrix with a 1 in the (i,j) th place, and 0 elsewhere.

Embed R into R_n via $r \mapsto r \cdot 1$. $R_n = \bigoplus_{i,j} e_{ij} R = \bigoplus_{i,j} R e_{ij}$.

Exercise: Prove $R = \text{set of matrices commuting with each } e_{ij}$.

$\Delta_n = \bigoplus_{i,j} e_{ij} \Delta$, a vector space of dimension n^2 over Δ . There aren't any chains of subspaces with more than $n^2 + 1$ members.

Let M_n be an R_n -module. Then $M = M1 = M(e_{11} + \dots + e_{nn}) = Me_{11} + \dots + Me_{nn}$. Let $U = Me_{11}$. Prove $Me_{11} = Ue_{11}$. Then $M = Ue_{11} + Ue_{12} + \dots + Ue_{nn}$. Consider $Me_{11} \cap (Me_{12} + \dots + Me_{nn})$. This

is annihilated by $e_{11} + \dots + e_{nn}$ and so by 1, so $Ue_1 + \dots + Ue_n$ is direct.

Write U^n for the direct sum of n copies of the R -module U . This can be thought of as $\mathcal{M}_n(U)$, the row vectors (u_1, \dots, u_n) with R_n acting in the usual way, $u \mapsto ua$.

(1.11): $M \rightarrow M_{\mathcal{M}_n} = U$ and $\mathcal{M}_n(U) \hookrightarrow U$ are inverse. It preserves \leq . Moreover, $(\mathcal{M}_n(U))^{\circ} = (U^{\circ})_n$. R has a faithful module U iff R_n has a faithful simple module $\mathcal{M}_n(U)$.

Δ a division ring. If $0 \neq \mu \in \Delta$, then $\mu\Delta = \Delta$ and so Δ is a faithful simple module for itself. Δ_n has $\mathcal{M}_n(\Delta)$ as its simple faithful module.

R a field, $V = k^n$. Choice of basis for V gives an isomorphism between $\text{Hom}_R(k^n, k^n)$ (the linear maps $V \rightarrow V$) and k^n .

Let R be any ring. Define R^{opp} , the opposite ring, to be R as additive group, but with multiplication \circ defined by $rsv = sr$.

Let M, N be R -modules. Then $\text{Hom}_R(M, N) =$ additive group of all R -module homomorphisms from M to N .

(1.12) (i) $\text{Hom}_R(R, R) \cong R^{\text{opp}}$.

(ii) $(R_n)^{\text{opp}} \cong (R^{\text{opp}})_n$.

(iii) (Schur's Lemma): If M is a simple R -module then $\text{Hom}_R(M, M)$ is a division ring.

(iv) $\text{Hom}_R(M^n, M^n) \cong (\text{Hom}_R(M, M))_n$.

Proof: (i) Let $\theta \in \text{Hom}_R(R, R)$. Then $r\theta = (1r)\theta = (1\theta)r$. θ multiplies on the left by 1θ .

Let $\lambda \in R$ and write $m_\lambda: r \mapsto \lambda r$ ($r \in R$). $m_\lambda \in \text{Hom}_R(R, R)$. It is obvious that $\theta \mapsto 1\theta$ and $m_\lambda \leftrightarrow \lambda$ are inverse maps, and additive. But $m_\lambda m_{\lambda'} = m_{\lambda' \lambda}$.

Hence these maps are anti-isomorphisms under multiplication.

(ii) Consider $a \mapsto a^T$, the transpose of a , from $(R_n)^{\text{opp}}$ to $(R^{\text{opp}})_n$. We need

$(a+b)^T = a^T \cdot b^T$ in $(R^{\text{opp}})_n$. Now $(a \cdot b)^T = (ba)^T$, and this has (i,j) th element $(ba)_{ji} = \sum_k b_{jk} a_{ki} = \sum_k a_{ki} \circ b_{jk} = \sum_k (a^T)_{ik} (b^T)_{kj} = (a^T \cdot b^T)_{ij}$.

(iii) Suppose $0 \neq \theta: M \rightarrow M$ be a module form. Then $M\theta$ is a non-zero submodule of M , so $M = M\theta$. Also, $M > \ker \theta$, and this is a submodule, so $\ker \theta = 0$.

(iv) Let $\theta \in \text{LHS}$. Let $(0, \dots, 0, \overset{(k\text{th})}{\mu}, 0, \dots, 0)\theta = (\mu\theta_{11}, \dots, \mu\theta_{nn})$. Then map θ to $(\theta_{ij}) \in (\text{Hom}_R(M, M))_n$. Let $\alpha_i: M \rightarrow M^n$ be the injection to the i th component. Let $\beta_j: M^n \rightarrow M$ be the projection to the j th component. So $\theta_{ij} = \alpha_i \circ \theta \circ \beta_j$. And since $\text{id} = \sum_k \alpha_k \circ \beta_k$, $(\theta \circ \Phi)_{ij} = \alpha_i \circ \theta \circ \beta_j = \sum_k \alpha_i \circ \theta \circ \beta_k = \sum_k \alpha_i \circ \Phi \circ \beta_k = \Phi_{ij}$.

Let $X \triangleleft R$, and $M = R/X$. Let $\theta \in \text{Hom}_R(M, M)$. $(X+r)\theta = ((X+1)r)\theta = (X+1)\theta r = X+\theta r$, where $X+\theta r = (X+1)\theta$. When $r \in X$ we must have $\theta r \in X$. Define $n(X)$, the normaliser of X , to consist of these t 's, ie, t such that $tX \subseteq X$. Clearly $X \subseteq n(X)$ and $X \triangleleft n(X)$. Conversely, if $t \in n(X)$, then $m_t: X+r \mapsto X+tr$ lies in $\text{Hom}_R(M, M)$. But $t \mapsto m_t$ is not 1-1, as its kernel is X .

(1.13) (i) If $X \trianglelefteq_r R$ then $\text{Hom}_R(R/X, R/X) \cong (\mathbb{M}^{(X)}/X)^{\text{opp}}$

(ii) (Schur): If $X \trianglelefteq_r R$ then $\mathbb{M}^{(X)}/X$ is a division ring.

Wedderburn II: Suppose R is a simple Artinian ring. Then R is (uniquely) Δ_n , for a division ring Δ .

Proof: Let M the unique simple module. Then R (as an R -module) $\cong M^n$, some n .

Then $R \cong (\text{Hom}_R(R, R))^{\text{opp}}$. Now, $\text{Hom}_R(M^n, M^n) \cong (\text{Hom}_R(M, M))_n = \Delta_n$, where $\Delta = \text{Hom}_R(M, M)$. Hence $R \cong (\Delta_n)^{\text{opp}} \cong (\Delta^{\text{opp}})_n$.

Uniqueness: Suppose $R = E_m$, E is a division ring. E has a unique simple module, namely E , so $\mathcal{N}_m(E)$ is the unique simple R -module. Let X be all the matrices which have zeroes in the top row. ($X = \mu^0$, where $\mu = (1, 0, \dots, 0) \in \mathcal{N}_m(E)$). $\mathcal{N}_m(E) = R/X = M$. $\text{Hom}_R(M, M) \cong (\mathbb{M}^{(X)}/X)^{\text{opp}}$.

Let $\lambda \in R$. Then $\lambda \in \mathbb{M}^{(X)} \Leftrightarrow \lambda e_{ij}$ for $i > 1$ has zero top row, i.e.,
 $(\text{top row of } \lambda) e_{ij} = 0$ ($i > 1$). I.e., λ must be of the shape $\begin{pmatrix} * & 0 & \dots & 0 \\ 0 & * & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$
Hence $\mathbb{M}^{(X)}/X \cong E$. Hence result.

Example: Let G be a finite group, and $R = \mathbb{C}G$. This is semi-simple and finite dimensional over \mathbb{C} . $\text{Hom}_R(M, M)$ for simple M is a division ring, finite dimensional over \mathbb{C} , and \mathbb{C} is the only one of these.

Hence Wedderburn gives $R = \bigoplus_{i=1}^n \mathbb{C}f_i$. Look at dimensions: LHS = $|G|$, RHS = $\sum_{i=1}^n f_i^2$. $\mathbb{C}f_i$ has $\mathcal{N}_{f_i}(\mathbb{C}) = M_i$, occurring f_i times, once per row.
Hence $\mathbb{C}G = \bigoplus_{i=1}^n M_i$.

1.2. Rings with Radical

R a ring. $X \trianglelefteq R$, X nilpotent. We suppose we know about $\bar{R} = R/X$. We need to 'lift' idempotents.

Take $e \in R$. e is idempotent if $e^2 = e$. Eg: $0, 1$, and in Δ_n , the e_{ii} are idempotents.

Can write as $e(1-e) = 0$ and $(1-e)e = 0$. But $1 = e + (1-e)$, so $R = eR \oplus (1-e)R$.

Suppose $R = X \oplus Y$, X, Y both right ideals. So $1 = \xi \oplus \eta$, so $\xi = \xi^2 \oplus \eta\xi$, and so $\xi^2 = \xi$ and $\eta\xi = 0$.

Let P be an R -module. Then P is projective $\Leftrightarrow \exists$ R -module Q with $P \oplus Q$ a free module R^n . We'll have a lot to do with these for $R = \mathbb{Z}G$, G finite.

If e and f are idempotents, then they are orthogonal, $e \perp f$, if $ef = fe = 0$.

If $1 = e_1 + \dots + e_n$, with e_i idempotents and $e_i e_j = 0$ if $i \neq j$, then we have an orthogonal decomposition of 1 . If R is semi-simple, $R = \bigoplus (\Delta_i)_{n_i}$, and we get an orthogonal decomposition of 1 .

If e is an idempotent in R/X and $\varepsilon \in R$, then e lifts to ε if $X + \varepsilon = e$.

(2.1): Let X be a nilpotent ideal of a ring R . Let e be an idempotent of $\bar{R} = R/X$, say $e = X + E$. Then \exists an idempotent α in $e\bar{R}e$, with $X + \alpha = e$. Suppose e_1, e_2 are idempotents in R ; with \bar{e}_1, \bar{e}_2 their images in \bar{R} . Then $e_1 R \cong e_2 R \Leftrightarrow \bar{e}_1 \bar{R} \cong \bar{e}_2 \bar{R}$.

Proof: By induction on n where $X^{2^n} = 0$. If $n=0$ then $X=0$ and we have nothing to do. Induction step depends on knowing that $(3X^2 - 2X^3)^2 - (3X^2 - 2X^3)$ has $X^2(X-1)^2$ as a factor. Suppose $X_n = X^{2^n}$ and we have an idempotent $X_n + E_n$ in R/X_n , and that $X_0 + E = X_0 + E_n$. Define $E_{n+1} = 3E_n^2 - 2E_n^3$. Is $X_{n+1} + E_{n+1}$ idempotent? Ie, does $E_{n+1}^2 - E_{n+1} \in X_{n+1}$? It has a factor $(E_n(E_n-1))^2$, is in X_{n+1} as $E_n(E_n-1)$ is in X_n .

Now, $X_n + E_{n+1} = X_n + E_n$, so we are done.

Last bit: Exercise.

(\Leftarrow): Argument applies more generally to lifting isomorphisms of projectives.

Have: $\begin{array}{ccc} e_1 R & & e_2 R \\ \downarrow \text{nat.} & & \downarrow \text{nat.} \\ \bar{e}_1 \bar{R} & \xrightarrow{f} & \bar{e}_2 \bar{R} \end{array}$ Suppose f is a module isomorphism as shown. Have $e_1 R + (1-e_1)R = R = 1.R$. Map $R \rightarrow \bar{e}_1 \bar{R}$ via $e_1 R \oplus (1-e_1)R \xrightarrow{\text{nat}} \bar{R}$.

Call it θ . Choose an element a in $e_2 R$ such that $a \cdot \text{nat} = \bar{a} = \bar{f}a$.

Define $\varphi: R \rightarrow e_2 R$ by $\varphi(1) = a$. Define $\alpha: e_1 R \rightarrow e_2 R$ to be the restriction of φ to $e_1 R$. Let $g: \bar{e}_2 \bar{R} \rightarrow \bar{e}_1 \bar{R}$ be f^{-1} , and repeat above to get β as shown.

So we get: $\begin{array}{ccc} e_1 R & \xrightarrow{\varphi} & e_2 R \\ \text{nat} \downarrow & \xrightarrow{\alpha} & \downarrow \text{nat.} \\ \bar{e}_1 \bar{R} & \xrightarrow{g} & \bar{e}_2 \bar{R} \end{array}$

Put $\gamma = \alpha\beta - 1: e_1 R \rightarrow e_1 R$. Thus $\bar{\gamma}: \bar{e}_1 \bar{R} \rightarrow \bar{e}_1 \bar{R}$ equals $fg - 1$, ie 0.

$e_1 R \gamma \leq e_1 X$. $(e_1 R) \gamma^2 = e_1 X \gamma = e_1 \gamma X \leq e_1 X^2$. So $(e_1 R) \gamma^n \leq e_1 X^n$ and this is eventually zero. So $\alpha\beta = 1 + \gamma$ and $\gamma^n = 0$, s.t. γ has inverse $1 - \gamma + \gamma^2 - \gamma^3 + \gamma^4 - \dots + (-1)^{n-1} \gamma^{n-1}$. Similarly, $\beta\alpha$ is invertible. So α, β are both isomorphisms.

(2.2): Let X be a nilpotent ideal of a ring R . Let e_1, \dots, e_n be in R and suppose $\bar{e}_1, \dots, \bar{e}_n$ are mutually orthogonal idempotents in $\bar{R} = R/X$. Then there exist mutually orthogonal idempotents e_1, \dots, e_n in R such that $\bar{e}_i = \bar{e}_i$, $1 \leq i \leq n$.

Proof: (2.1) is the case $n=1$. Suppose $n>1$ and suppose e_1, \dots, e_{n-1} are already found.

Method is to adjust e_n so that it becomes orthogonal to e_1, \dots, e_{n-1} .

Then use (2.1) to get $e_n = e_n^2$ with $\bar{e}_n = \bar{e}_n$ in $e_n R e_n$, and this will do it.

Define $e = e_1 + \dots + e_{n-1}$. Then $e^2 = e$, $e_i e = e e_i = e_i$. Write $R = eR \oplus (1-e)R$ and $e_n = \alpha \oplus \beta$. We show $\alpha \in X$, ie $\bar{\alpha} = 0$.

Now, $e e_n = e \alpha$ and $\bar{e} \bar{e}_n = 0$, so $e \alpha \in X$. But $\alpha = e \alpha$ so $\alpha \in X$. Replace e_n by $e_n - \alpha$. So we may assume $e_n \in (1-e)R$. Then $e_i e_n \in (e_i - e_i e)R = 0$.

Now replace e_n by $e_n - e_n e$ (Note $\bar{e}_n \bar{e} = 0$). So $e_n e_i - e_n e e_i = 0$, so this works.

Let e be an idempotent in R . Say that e is primitive if $e = e_1 + e_2$ with e_1, e_2 idempotent and orthogonal can hold only if $e_1 = e$ or $e_2 = e$.

Say M is indecomposable $\Leftrightarrow M = M_1 \oplus M_2$ can only hold if $M_1 = M$ or $M_2 = M$.

So e is primitive $\Leftrightarrow eR$ is indecomposable as a module.

(2.3): X , a nilpotent ideal of R , e an idempotent of R . Then e is primitive iff \bar{e} is primitive.

Proof: Suppose $e = e_1 + e_2$ with $e_1^2 = e_1$, $e_2^2 = e_2$, $e_1 e_2 = e_2 e_1 = 0$. Then $\bar{e} = \bar{e}_1 + \bar{e}_2$. If \bar{e} is primitive then one of the summands is zero. If $\bar{e}_1 = 0$ then $e_1 \in X$, so $e_1 \in X^n$ for all n , so $e_1 = 0$.

Conversely, suppose e is primitive. Suppose \bar{e} is not primitive. So $\bar{e} = \bar{e}_1 + \bar{e}_2$, \bar{e}_1, \bar{e}_2 orthogonal idempotents. Lift these by (2.2) to orthogonal idempotents e_1 and e_2 . Let $f = e_1 + e_2$. Then f is idempotent. Moreover, $\bar{e}\bar{R} = \bar{f}\bar{R}$.

By (2.1), last sentence, we get $eR \cong fR$. Since fR is decomposable, so is eR , i.e., e is not primitive. \blacksquare

(2.4): Hypothesis as before. Suppose $1 = e_1 + \dots + e_n$ is an orthogonal decomposition into idempotents. Then $\bar{1} = \bar{e}_1 + \dots + \bar{e}_n$ is as well. The $e_i R$ are indecomposable iff the $\bar{e}_i \bar{R}$ are indecomposable.

Example: Let R be Artinian, $X = J(R)$, $\bar{R} = R/X$. The Wedderburn Theorems say that $\bar{R} = \bar{R}_1 \oplus \dots \oplus \bar{R}_m$, with \bar{R}_i simple rings, and $\bar{R}_i = (\bar{\Delta}_i)_{\bar{n}_i}$ with $\bar{\Delta}_i$ a division ring. In $\bar{\Delta}_n$, we have $\bar{1} = \bar{e}_{11} + \dots + \bar{e}_{nn}$, and $\bar{\Delta}_n = \bar{e}_{11} \bar{\Delta}_n + \dots + \bar{e}_{nn} \bar{\Delta}_n$. Each \bar{e}_{ii} is idempotent, orthogonal to the others, and $\bar{e}_{ii} \bar{\Delta}_n = \bar{\Delta}_n / (\bar{\Delta}_n)$, simple modules.

R is Local $\Leftrightarrow R/J$ is a division ring.

(2.5): (i) R is local $\Leftrightarrow R - J = U(R)$, the unit group of R .

(ii) If R is local then $0, 1$ are the only idempotents.

(iii) If R is Artinian and $0, 1$ are the only idempotents, then R is local.

Proof: (i) \Rightarrow Let $x \in R - J$. Suppose $xR < R$. Then $\exists X$ with $xR \leq X \triangleleft R$.

But then $J \leq X$ and $\frac{J+xR}{J} \subset R/J$ # to $J+x$ being a unit in R/J .

Hence $xR = R$ so $\exists y$ with $xy = 1$. By same token, $\exists z$ with $yz = 1$.

So y is right and left invertible, so $x = z$, as required.

(ii) Let $e = e^2 \in R$. Then $1 = e + (1-e)$, so either e or $1-e$ fails to be in J , say e . So e^{-1} exists. But $e(1-e) = 0$, and so $e = 1$.

(iii) Exercise. (We know what Artinian rings look like).

(2.6): Let M be an R -module. Consider $E = \text{End}_R(M)$. Then

(i) If E is local then M is indecomposable.

(ii) If M is indecomposable, then $0, 1$ are the only idempotents in E .

Proof: (i) Suppose $M = M_1 \oplus M_2$. Let $\pi: M \rightarrow M_1$ be projection, so $\pi\pi = \pi^2$ in E .

E local $\Rightarrow \pi\pi = 0, 1$, hence $M_1 = 0$ or M .

(ii) If $\pi\pi = \pi^2 \in E$, then $M = M\pi \oplus M(1-\pi)$.

(2.7): Krull-Schmidt Theorem: Let R be a central subfield of a ring R and suppose $\dim_R R$ is finite. Let M be a finitely-generated R -module. Then M can be written in an essentially unique way as a direct sum of indecomposable modules.

Proof: It is obvious that M has such a decomposition. Suppose $M = M_1 \oplus \dots \oplus M_r = N_1 \oplus \dots \oplus N_s$ with all M_i, N_j indecomposable.

Let $\mu_i: M \rightarrow M_i$, $\nu_j: N \rightarrow N_j$ be the projections. Then $\mu_i = \sum_{j=1}^s \nu_j \mu_{ij}$.

Restrict this to M_i : $\text{id}_{M_i} = \sum_j (\nu_j \mu_{ij})|_{M_i}$ in $\text{End}_R(M_i)$, a local ring.

Now, id_{M_i} is not in the radical, so some summand is not in the radical, say $(\nu_j \mu_{ij})|_{M_i}$. We show $M_i \cong N_j$.

Let $\Phi = (\nu_j \mu_{ij})|_{M_i}$. So we have: $\begin{array}{ccc} M_i & \xrightarrow{\Phi} & M_i \\ \downarrow \nu_j \mu_{ij} & \nearrow \mu_{ij} & \\ N_j & & N_j \end{array}$, with Φ an isomorphism

Let $\alpha = \mu_{ij}|_{N_j}$, $\beta = \Phi^{-1} \circ \nu_j|_{M_i}: M_i \rightarrow N_j$. Then, $\beta \alpha = \text{id}_{M_i}$.

$N_j = M_i \beta \oplus \ker \alpha$ (exercise). Since N_j is indecomposable, $\ker \alpha = 0$, so α is injective. And α is surjective since $\beta \alpha = \text{id}_{M_i}$. Hence $N_j \cong M_i$.

Now, α injective means $N_j \cap (M_2 \oplus \dots \oplus M_r) = 0$. Moreover, M_i and N_j have the same dimension over R . Hence $N_j \oplus M_2 \oplus \dots \oplus M_r = M$, but also $N_j \oplus \dots \oplus N_s = M$. So $M_2 \oplus \dots \oplus M_r \cong M/N_j \cong N_2 \oplus \dots \oplus N_s$.

Let γ be an isomorphism from $N_2 \oplus \dots \oplus N_s$ onto $M_2 \oplus \dots \oplus M_r$. Then $N_2 \gamma \oplus \dots \oplus N_s \gamma = M_2 \oplus \dots \oplus M_r$ and we are done by induction.

2. $\mathbb{Z}G$ -modules for finite G .

Definition: Group rings: Take G a group, S a ring. Define SG , the group ring of G over S . Its elements are the sums $\sum_{x \in G} \sigma_x x$, where all but finitely many of the coefficients σ_x are 0.

Define addition: $\sum \sigma_x x + \sum \tau_x x = \sum (\sigma_x + \tau_x) x$

multiplication: $(\sum \sigma_x x)(\sum \tau_y y) = \sum \gamma_z z$, where $\gamma_z = \sum_{ab=z} \sigma_a \tau_b$.

The map $s \mapsto s1_G$ is a ring isomorphism from S to SG , and $x \mapsto 1_S \cdot x$ is a group isomorphism from G to SG . Identify s with $s1_G$, x with $1_S \cdot x$.

Once this is done, SG is generated by S and by G . Moreover, $sx = xs$ for s in S , x in G .

Note that if T is a ring with subring S , commuting elementwise with subgroup G , and $\varphi: S \rightarrow S$, $\theta: G \rightarrow G$, then \exists unique homomorphism $\kappa: SG \rightarrow T$, with $\kappa_s = \varphi$, $\kappa_g = \theta$.

If M is an SG -module then we have a homomorphism $\alpha: SG \rightarrow \text{End}_{\mathbb{Z}}(M)$.

$\alpha_s: S \rightarrow \text{End}_{\mathbb{Z}}(M)$ shows that M is an S -module, $\alpha_G: G \rightarrow \text{Aut}_S(M)$.

Conversely, if M is an S -module and $\theta: G \rightarrow \text{Aut}_S(M)$ is a homomorphism, then M becomes an SG -module, via $\mu(\sum \sigma_x x) = \sum (\mu(\sigma_x))(x\theta)$.

G a group. Let A be an abelian normal subgroup. $g^*: a \mapsto g^{-1}ag = a^{g_1, g_2}$ ($a \in A$) is an automorphism. $(g_1, g_2)^{-1} a g_1 g_2 = g_2^{-1} (g_1^{-1} a g_1) g_2$, ie $a^{g_1, g_2} = (a^{g_1})^{g_2}$, or $(g_1, g_2)^* = g_1^* g_2^*$. So $*$ is a homomorphism of G into $\text{Aut } A$.

Write A additively - A becomes a $\mathbb{Z}G$ -module.

If $b \in A$, then $b^{-1}ab = a$, ie $A^* = 1$. So $A \leq \ker *$, and $*: G/A \rightarrow \text{Aut}_{\mathbb{Z}} A$. So A becomes a $\mathbb{Z}(G/A)$ -module.

G a group. A presentation of G is a short exact sequence of groups:
 $1 \rightarrow R \rightarrow F \xrightarrow{\pi} G \rightarrow 1$, where F is free. (Label this sequence (i)).

A group F is free on $x = \{x_\lambda : \lambda \in \Lambda\}$ if F is generated by the x_λ such that whenever $\psi: X \rightarrow$ any group, then ψ extends uniquely to a homomorphism $F \rightarrow$ same group.

In (i), suppose $F = F_r\{x_\lambda : \lambda \in \Lambda\}$. Then $g_\lambda = x_\lambda \pi$, and $G = \langle g_\lambda : \lambda \in \Lambda \rangle$.

If $f(\underline{x}) = x_{\lambda_1}^{m_1} \cdots x_{\lambda_t}^{m_t}$ is a word in F , then $f(\underline{x})\pi = f(g)$.

Think of R as a normal subgroup of F , $R = \ker \pi$. If $f(\underline{x}) \in R$, then $f(g) = 1$, a relation between the generators g_λ , $\lambda \in \Lambda$, of G . R is called the relation subgroup.

If $R = \langle F_1(x)^F, \dots, F_n(x)^F \rangle$ and $\Lambda = \{1, \dots, n\}$, then we write:

$G = \langle g_1, \dots, g_n \mid f_1(x) = \dots = f_n(x) = 1 \rangle$, or $G = \langle g_1, \dots, g_n \mid f_1(x), \dots, f_n(x) \rangle$.

Examples: (i) $\langle x_1 | x_1^7 \rangle = F/R$, where $F = \langle x_1 \rangle$ = free, rank 1, ie cyclic.
 $R = \langle x_1^7 \rangle$ = cyclic of order 7.

(ii) $\langle a, b \mid a^2 = b^3 = (ab)^3 = 1 \rangle$ is S_3 . (Say $a = (12)$, $b = (123)$).

$F = F_r\{x, y\}$. $F \xrightarrow{\pi} S_3 \rightarrow 1$ with $x \mapsto (12)$, $y \mapsto (123)$.

This has kernel $\langle x^{2^F}, y^{3^F}, (xy)^{3^F} \rangle$.

(iii) $\langle a, b \mid a^2 = b^3 = (ab)^5 = 1 \rangle$ is A_5 .

(iv) $\langle x, y, z \mid y^x = z^2, z^y = x^2, x^z = y^2, xyz = 1 \rangle$ is C_7 .

(v) $\langle x, y, z \mid x^{-1}yz = y^2, y^{-1}zy = z^2, z^{-1}xz = x^2 \rangle$ has only one element.

(vi) $\langle x, y, z, t \mid x^{-1}yz = y^2, y^{-1}zy = z^2, z^{-1}tz = t^2, t^{-1}xt = x^2 \rangle$ is a 'famous' infinite simple group.

(vii) $\langle a, b \mid a^2 = b^4 = ba^{-1}ba = 1 \rangle$ is the quaternion group, of order 8.

Define $d(G) =$ minimum number of generators needed to generate G .

$d(G) = 1 \iff G$ is cyclic.

$d(G) = 2$ if G is a non-abelian simple group.

If $K \trianglelefteq G$, write $d_G(K)$ for the minimum number of G -conjugacy classes needed to generate K .

If $1 \rightarrow R \rightarrow F \xrightarrow{\pi} G \rightarrow 1$, then $d_F(R) =$ minimum number of relations needed amongst the g_λ to determine G .

In the above examples: (i) $d(F) = 1$, $d_F(R) = 1$. (ii) $d(F) = 2$, $d_F(R) = 3$. (iii) $d(F) = 2$, $d_F(R) = 3$.

(iv) $d(F) = 3$, $d_F(R) = 3$. (v) $d(F) = 3$, $d_F(R) = 3$. (vi) $d(F) = 4$, $d_F(R) = 4$. (vii) $d(F) = 2$, $d_F(R) = 2$.

Theorem: Suppose G is a finitely generated abelian group, and sequence

(i) is a finite presentation (ie, $d(F), d_F(R)$ finite) then

$d_F(R) - d(F) = \frac{1}{2}d(d-1) - p$, where $d = d(G)$ and p is the torsion free rank of G .

Proof: Hard exercise.

Let $F = \langle x_1, \dots, x_n \rangle$ be free of rank n . If $F \xrightarrow{\pi} G$ is abelian then $x_i \pi x_j \pi = x_j \pi x_i \pi$. F' , the derived group, equals $\langle [x_i, x_j]^F \mid 1 \leq i < j \leq n \rangle$, and $d_F(F') = \frac{1}{2}n(n-1)$

If G is a finitely generated abelian group given as F/R with F a free abelian with rank s , then one could change basis so that F is free abelian on a_1, \dots, a_s , and R is given by $a_1^{d_1}, \dots, a_t^{d_t}, d_1 | d_2 | \dots | d_t$, $t \leq s$.

Take R' , the derived group of R . $R \trianglelefteq F \Rightarrow R' \trianglelefteq F$. Get: $1 \rightarrow R/R' \rightarrow F/R' \xrightarrow{\pi} G \rightarrow 1$.

$R/R' = \bar{R}$ is the relation module. \bar{R} is an abelian normal subgroup of $\bar{F} = F/R'$.

\bar{R} is a module for \bar{F}/\bar{R} , ie G . To be precise, this action is for g in G , $g^*: R'F \mapsto R'F^x$ where $x \in F$ and $x\pi = g$.

If $\mathfrak{F} = \sum_{i=1}^r n_i g_i \in \mathbb{Z}G$, then $\mathfrak{F}^*: R'F \rightarrow R' \prod_{i=1}^r (F^{n_i})^{x_i}$ where $x_i \pi = g_i$, each i .

Suppose $d_F(R)$ is finite, then $R = \langle f_1^F, \dots, f_r^F \rangle$. Then $\bar{R} = \langle \bar{f}_1^{\bar{F}}, \dots, \bar{f}_r^{\bar{F}} \rangle$. now $\bar{F}_1 \mathbb{Z}G + \dots + \bar{F}_r \mathbb{Z}G$, a finitely-generated $\mathbb{Z}G$ -module.

If G is finite, S any ring, and M a finitely generated SG -module, then $M = \mu_1 SG + \dots + \mu_r SG = \sum_{x \in G} \mu_i x S$, a finitely generated S -module.

Nielsen-Schreier Theorems: (i) subgroups of free groups are free.

(ii) if G and $d(F)$ are both finite, then so is $d(R)$, and $|G| = \frac{d(R)-1}{d(F)-1}$.

The point about (ii) is that for us, \bar{R} will be a finitely generated free \mathbb{Z} -module.

Definition: A $\mathbb{Z}G$ -lattice is a $\mathbb{Z}G$ -module which is free of finite rank as a \mathbb{Z} -module.

Our relation modules are $\mathbb{Z}G$ -lattices. Swan's theorems are about these.

Suppose $\mathbb{Q} \subseteq K$ is a number field. Let I be the ring of integers.

Dedekind: I , as a \mathbb{Z} -module, is free of finite rank.

$G = \text{Gal}(K/\mathbb{Q})$ acts on I , so I is a $\mathbb{Z}G$ -lattice.

Let $U = U(I)$ be the units of K . Dirichlet: U is finitely generated.

Let U_0 be the units of finite order. Then U/U_0 is free abelian of finite rank. This is also a $\mathbb{Z}G$ -lattice.

2.2 Algebraic Preliminaries.

S a commutative ring, Noetherian. G : a finite group.

$\text{Mod-}S =$ finitely generated S -modules. $\text{Mod-}SG$ similarly.

Λ a multiplicatively closed subset of S .

$P \triangleleft_p S$, $\Lambda = S \setminus P$. Must know about $S_P = \Lambda^{-1}S$.

If $M \in \text{Mod-}S$, you should know $\Lambda^1 M \in \text{Mod-}\Lambda^1 S$, $\Lambda^1 M = M \otimes_S \Lambda^{-1} S$. Its elements are $M/\lambda \equiv \mu \otimes 1/\lambda$, $\mu \in M$, $\lambda \in \Lambda$. If $\Lambda = S \setminus P$, write $\Lambda^1 M = M_P$.

(3.2): (i) S_P is local, $\text{Jac}(S_P) = P_P$. $S_P/P_P \cong \text{ff}(S/P)$.

(ii) The primes of S_P are in 1-1 correspondence with those of S below P .

(iii) If $P < Q < S$ are primes, then $(S_Q)_{P_Q} \cong S_P$.

where S is a domain.

(3.3): Let M be in $\text{Mod-}S$. Then

(i) $M_P = 0 \Leftrightarrow M^0 \not\subset P$.

(ii) $M = 0 \Leftrightarrow M_P = 0 \vee P \triangleleft S$.

(iii) If $M \xrightarrow{F} N$ in $\text{Mod-}S$, then F is surjective (injective) $\Leftrightarrow f_P$ is surjective (injective).

Return to G . Consider the M in $\text{Mod-}SG \subseteq \text{Mod-}S$. $\Lambda^1 M$ becomes a $\Lambda^1 SG$ -module, by $(\mu/\lambda)g = \mu g/\lambda$.

(3.4): Let $h: \Lambda^1 M \rightarrow \Lambda^1 N$ be a $\Lambda^1 SG$ -module homomorphism. Then \exists an SG -homomorphism $f: M \rightarrow N$ and $\lambda \in \Lambda$ such that $h = \Lambda^1 f/\lambda$.

Re.(3.1): Suppose $S \xrightarrow{\theta} S_1$ and $G \xrightarrow{\varphi} G_1$ are homomorphisms. Then we get $SG \rightarrow S_1 G_1$ via $\sum \sigma_x x \mapsto \sum (\sigma_x)^{\theta} x^{\varphi}$.

Particular (and important) case is when $G_1 = 1$ and when $\theta = \text{id}_S$.

Get $\varepsilon: SG \rightarrow S$ with $\sum \sigma_x x \mapsto \sum \sigma_x$, the coefficient sum. ε is the augmentation, and its kernel is the augmentation ideal.

If $S = \mathbb{Z}$, write this as σ_g . If it's S , use σ_g when S is important.

So, if $A, B, C, \dots, F, G, H, \dots, R, \dots, W, \dots, Z$ are groups, then use:

$\sigma_a, \sigma_b, \sigma_c, \dots, \sigma_f, \sigma_g, \sigma_h, \dots, \sigma_r, \dots, \sigma_w, \dots, \sigma_z$.

We get:

(3.1): σ_g is a free S -module on the $x-1$ ($1+x \in G$)

Proof: The $x-1$ are in σ_g . Moreover, $\sum \sigma_x x = \sum \sigma_x x - \sum \sigma_x$, if $\sum \sigma_x \in \sigma_g$, $= \sum_{x \neq 1} \sigma_x (x-1)$.

This expression is unique, so we're done.

(3.41) : M, N SG-modules and $\Lambda^i M \xrightarrow{h} \Lambda^i N$ an Λ^i SG-homomorphism. Then \exists
 $f: M \rightarrow N$ an SG-map and $\lambda \in \Lambda$ with $h = \Lambda^i f / \lambda$.

Proof: $\Lambda^i \text{Hom}_{\text{SG}}(M, N)$ is a $\Lambda^i S$ -module. Get $w: \Lambda^i \text{Hom}_{\text{SG}}(M, N) \rightarrow \text{Hom}_{\text{SG}}(\Lambda^i M, \Lambda^i N)$
 $f \otimes \lambda \mapsto \Lambda^i f / \lambda$.

(3.42) : As in (i), but with w an isomorphism.

Proof: (i) $M = SG$, (ii) $M = (SG)^n$, (iii) M general. - 3 cases.

R. M, N R-modules. $\text{Hom}_R(M, N)$ is an additive group, an R-module if R is commutative. $\text{Hom}_R(R, N) \cong N$

$$0 \longmapsto 1_0$$

$$(n^*: r \mapsto nr) \longleftrightarrow n.$$

Let $s \in R$. $(ns)^*: r \mapsto nsr$. $n^*: r \mapsto nrs$. These are module maps over any central subring S of R.

(i) $M = SG$. $\Lambda^i \text{Hom}_{\text{SG}}(SG, N) \rightarrow \Lambda^i N \rightarrow \text{Hom}_{\Lambda^i SG}(\Lambda^i SG, \Lambda^i N)$.
 $f/\lambda \longmapsto (\Lambda^i f)/\lambda$
 $n/\lambda \mapsto (n/\lambda)^*: p \mapsto n/\lambda \cdot p$. $\Lambda^i f/\lambda \cdot p = p \cdot f/\lambda$.

The composite of these two is w.

(ii) $M = (SG)^n$. $M\mathbb{P} = \Lambda^i \text{Hom}_{\text{SG}}(M, N)$, $M\mathbb{Q} = \text{Hom}_{\Lambda^i SG}(\Lambda^i M, \Lambda^i N)$. Λ^i is exact,
 Hom preserves direct sums, so: $(M_1 \oplus M_2)\mathbb{P} \cong M_1\mathbb{P} \oplus M_2\mathbb{P}$.
 $(M_1 \oplus M_2)\mathbb{Q} \cong M_1\mathbb{Q} \oplus M_2\mathbb{Q}$.

So (ii) is true, via (i).

(iii) M general. Suppose $d(M) = n$, $M = \mu_1 SG + \dots + \mu_n SG$. Then map $(SG)^n$ onto M,
by $(r_1, \dots, r_n) \mapsto \mu_1 r_1 + \dots + \mu_n r_n$. Let M' be the kernel. This is fg over S.

We have $0 \rightarrow M' \rightarrow (SG)^n \rightarrow M \rightarrow 0$.

We get: $0 \rightarrow M\mathbb{P} \rightarrow (SG)^n \mathbb{P} \rightarrow M'\mathbb{P}$
 $\downarrow w_1 \quad \downarrow w_2 \quad \downarrow w_3$
 $0 \rightarrow M\mathbb{Q} \rightarrow (SG)^n \mathbb{Q} \rightarrow M'\mathbb{Q}$

(ii) says that w_2 is an isomorphism, so w_1 is injective.

This is true for every fg M. Hence w_3 is injective.

(3.43) : Suppose we have exact sequences of S-modules as shown, all commuting.

$$0 \rightarrow A \xrightarrow{i} B \xrightarrow{j} C$$

$\downarrow \alpha \quad \downarrow \beta \quad \downarrow \gamma$ If the vertical arrows are injective

$0 \rightarrow A' \xrightarrow{i'} B' \xrightarrow{j'} C'$ and β is surjective then α is surjective.

Proof: Exercise. This finishes (3.42)(iii).

(3.44) : (i) Suppose V is a finitely generated Λ^i SG-module. Then $V = \Lambda^i M$ for some fg SG-module M.

(ii) If V is torsion-free over S then M can be chosen torsion-free.

Proof: (i) $0 \rightarrow M_0 \rightarrow M \xrightarrow{\theta} \Lambda^i M$ is exact, $M_0 = \ker \theta = \Lambda$ -torsion submodule. $\{u: u\lambda = 0, \text{some } \lambda \in \Lambda\}$.

Then $0 \rightarrow M_0 \rightarrow M \rightarrow M/M_0 \rightarrow 0$ gives: $0 \rightarrow \bigoplus_{\lambda \in \Lambda} M_0 \rightarrow \Lambda^i M \rightarrow \Lambda^i (M/M_0) \rightarrow 0$.
 $\therefore \Lambda^i M \cong \Lambda^i (M/M_0)$.

(ii) Represent V as a homomorphic image of a free module:
 $(\Lambda^i SG)^n \rightarrow V \rightarrow 0$. (as V is fg)

The kernel V_0 is f.g. over $\Lambda^1 SG$. Represent V_0 as a homomorphic image of $(SG)^m$. We get $(\Lambda^1 SG)^m \xrightarrow{h} (\Lambda^1 SG)^n \rightarrow V \rightarrow 0$, exact.

From (3.4(i)), $h = \Lambda^1 f / \lambda$ where $f: (SG)^m \rightarrow (SG)^n$. Define M to be $\text{coker}(f)$.
 $\therefore (SG)^m \xrightarrow{f} (SG)^n \xrightarrow{\text{nat.}} M \rightarrow 0$.

Hence $(\Lambda^1 SG)^m \xrightarrow{\lambda h} (\Lambda^1 SG)^n \rightarrow \Lambda^1 M \rightarrow 0$.

Since λ is invertible, $\text{coker } h = V$ is the same as $\text{coker } \lambda h = \Lambda^1 M$.

What we need to know about projectives.

Let R be a ring and P an R -module. Then, say P is projective if whenever

$$\begin{array}{ccc} & P & \\ \downarrow \varphi & \downarrow \Phi & \\ M & \xrightarrow{\theta} M' & \rightarrow 0, \text{ exact} \end{array} \quad - \text{then a } \Psi \text{ exists to make the triangle commute.}$$

Examples: (i) Suppose $P = R^n$ and suppose we have Φ as above. Let $P = e_i R \oplus \dots \oplus e_n R$.

Define Ψ by $(e_i \cdot \Psi) \theta = e_i \Phi$ (permissible, since θ an epimorphism), and

extend: $(e_i v_i + \dots + e_n v_n) \Psi = (e_i \Psi) v_i + \dots + (e_n \Psi) v_n$, by linearity.

Free modules are projectives.

(3.5) (i) P and Q are projectives $\Leftrightarrow P \oplus Q$ is projective.

(ii) P is projective $\Leftrightarrow \exists Q$ with $P \oplus Q$ free.

(iii) Free modules are projective.

(iv) P is projective \Leftrightarrow whenever we have $M \xrightarrow{f} P \rightarrow 0$ exact, then f is split. (i.e., $\exists g: P \rightarrow M$ with $gf = \text{id}_P$)

Exercise: $M = Pg \oplus \ker f$ follows from $gf = \text{id}_P$.

Proof: (i) (\Rightarrow) We have: $\begin{array}{ccc} & P \oplus Q & \\ \downarrow \beta & \downarrow \alpha & \\ M & \xrightarrow{f} M' & \rightarrow 0 \end{array}$ $\begin{array}{l} \alpha_P \text{ lifts to, say, } \beta \\ \alpha_Q \text{ lifts to, say, } \gamma \end{array} \} \text{ so } \alpha \text{ lifts to } \beta + \gamma$.

(\Leftarrow) $\begin{array}{ccc} & P \oplus Q & \\ \downarrow \beta & \downarrow \alpha & \\ M & \xrightarrow{f} M' & \rightarrow 0 \end{array}$ β_P is a lifting of α .

(iii) (\Leftarrow) Done by (iii) and (ii)

(\Rightarrow) Choose a free module F and $F \xrightarrow{f} P \rightarrow 0$, so $F = Ph \oplus \ker f$.

If $d(P) = d$ then F can be chosen with d generators.

(iv) See example above.

(v) (\Rightarrow) $M \xrightarrow{f} P \rightarrow 0$ splits the sequence.

(\Leftarrow) Use for a free module F to get F a direct summand as in (iv).

Examples: (i) Projective \mathbb{Z} -modules are free

(ii) If R is a field and $|X(k)| \leq |G|$, then every module is projective (Maschke)

(iii) If $|X(k)| \geq |G|$, then the trivial module k is not projective. Consider $RG \xrightarrow{\epsilon} k \rightarrow 0$.

If k is projective, then $kG \cong k \oplus g_i$. Let $u = \sum x_i g_i$ be in k .

Then $uy = u$ for all $y \in G$. So $\sum \lambda_x xy = \sum \lambda_x x$, so $\lambda_x = \lambda_{xy} \forall y \in G$,
 $= \lambda$, say. Then $u = \lambda (\sum_{x \in G} x) \xrightarrow{E} \lambda |G| = 0$. i.e $u \in J(G)$, so $u = 0$.

(3.6): 0 and 1 are the only idempotents in $\mathbb{Z}G$. (or: $\mathbb{Z}G$ has no cyclic projectives).

Proof: Let $e \in \mathbb{Z}G$ with $e^2 = e$. Suppose $e = \sum_{x \in G} \lambda_x x$. Consider $\bar{e}: r \mapsto er$.

We know $\mathbb{Z}G = e\mathbb{Z}G + (1-e)\mathbb{Z}G$. Relative to a suitably chosen basis,
 e has matrix $\begin{pmatrix} s & 0 \\ 0 & 0 \end{pmatrix}$.

Now, $(\sum \lambda_x x)y = \sum \lambda_x xy$. Use the natural basis G of $\mathbb{Z}G$, and the (yy) th
spot of the matrix of \bar{e} is λ_1 . So trace \bar{e} is $\lambda_1 |G|$ and this must equal s .
Hence $s=0$ or $|G|=1$, i.e $e=0$ or 1 .

(3.7): P a projective SG -module, and for any $P \trianglelefteq S$. Then

(i) P/P_P is projective as an $S/\mathbb{Z}G$ -module.

(ii) P_P is a projective $S_P G$ -module.

Proof: (i) Have $F = P \oplus Q$, F free. So $F_P = P_P \oplus Q_P$. So $F/F_P \cong P/P_P \oplus Q/Q_P$.

Say $F = R^n$. Then $F/F_P = (R/P)^n$.

(iii) Similarly, but get $(R_P)^n = F_P \cong P_P \oplus Q_P$.

Remarks: Recall Artinian $\Rightarrow \text{Jac}$ is nilpotent.

$(\mathbb{Z}/p\mathbb{Z})G$ is Artinian if p is prime.

$\text{Jac}(\mathbb{Z}(p)) = (p)$. $\text{Jac}(\mathbb{Z}_{(p)}G)$ contains (p) . Let M be a simple
 $\mathbb{Z}_{(p)}G$ -module. Then M is fg over $\mathbb{Z}_{(p)}$ and has a maximal
 $\mathbb{Z}_{(p)}$ -submodule, say U . So $(M/U)(p) = 0$. $M_p = M(p) \subset M$. M_p is a
 $\mathbb{Z}_{(p)}G$ -submodule, so is zero.

Definition: Let $M \xrightarrow{f} N \in \text{Mod-}SG$ be an epimorphism. Then f is essential if
whenever $L \xrightarrow{g} M \xrightarrow{f} N$ with gf an epimorphism, then g is an epimorphism.
Alternatively, if $U \subset M$ then $Uf \subset N$.

(3.8.1) (Nakayama's Lemma): Let $x \in R$, $x \in \text{Jac}(R)$. Let M be an fg R -module.
The natural map $M \rightarrow M/Mx$ is essential.

Proof: Let $U \subset M$. Then $\exists V$ with $U \subset V \subset M$. Then $(M/V)x = 0$, so $U + Mx \leq V \subset M$.
So $\frac{U+Mx}{Mx} \leq \frac{V}{Mx} < \frac{M}{Mx}$.

(3.8.2): Suppose P, Q are projective SG -modules. Let $X \trianglelefteq SG$, $X \subseteq \text{Jac}(R)$.

Then $P \cong Q \Leftrightarrow P_{PX} \cong Q_{QX}$

Proof: $P \xrightarrow{\theta, \cong} Q$, so $P_X \xrightarrow{\cong} Q_X$, which induces $P_{PX} \xrightarrow{\cong} Q_{QX}$. Does (\Rightarrow)?

(\Leftarrow). $P \xrightarrow{\text{nat}} P_{PX}$, f exists, as P is projective.

$\begin{array}{ccc} P & \xrightarrow{\text{nat}} & P_{PX} \\ \downarrow f_{\text{nat}} & & \downarrow g \\ Q & \xrightarrow{\text{nat}} & Q_{QX} \end{array}$ By (3.8.1), f_{nat} is an epimorphism $\Rightarrow f$ is an epimorphism.

Since Q is projective, f is a split epimorphism, so $\exists h: Q \rightarrow P$ with
 $hf = \text{id}_Q$. $h \cdot \text{nat}, g$ is an epimorphism, g is an isomorphism, so $h \cdot \text{nat}$ is an epimorphism.
But nat is essential, so h is an epimorphism, so $\ker f = 0$. So f is an isomorphism.

(3.9): If R is local, then every projective is free.

Proof: Let $J = \text{Jac}(R)$. Suppose $P \oplus Q = R^n$. Then $\frac{P}{PJ} \oplus \frac{Q}{QJ} \cong (R/J)^n = \Delta^n$, with $\Delta = R/J$ a division ring. By linear algebra, $\frac{P}{PJ} \cong \Delta^n = \frac{R^n}{R^n J}$. By (3.8.2) we get $P \cong R^n$.

(3.10): $M, N \in \text{Mod-SG}$, and $M \xrightarrow{f} N$. Then f is a split epimorphism $\Leftrightarrow \text{Hom}_{\text{SG}}(M, N) \xrightarrow{\bar{f}} \text{Hom}_{\text{SG}}(N, N)$ is an epimorphism.

Proof: f is a split epimorphism $\Leftrightarrow g: N \rightarrow M$ with $gf = 1_N$. Clearly, if \bar{f} is an epimorphism, this holds. Conversely, if $gf = 1_N$, then any θ in $\text{Hom}(N, N)$ is of the form $(\theta g)f$ is $\theta g \circ f$.

(3.11.1): $M \xrightarrow{f} N$ in Mod-SG . Then f is a split epimorphism $\Leftrightarrow \forall P \triangleleft S$, $M_P \xrightarrow{f_P} N_P$ is a split epimorphism.

Proof: f a split epimorphism $\Leftrightarrow \text{Hom}_{\text{SG}}(M, N) \xrightarrow{\bar{f}} \text{Hom}_{\text{SG}}(N, N)$ is epimorphism.
 $\text{(by 3.3(iii))} \Leftrightarrow (\text{Hom}_{\text{SG}}(M, N))_P \xrightarrow{\bar{f}_P} (\text{Hom}_{\text{SG}}(N, N))_P$ is epimorphism $\forall P \triangleleft S$
 $\text{(by 3.4.2)} \Leftrightarrow \text{Hom}_{S_{\text{SG}}}(M_P, N_P) \xrightarrow{\bar{f}_P} \text{Hom}_{S_{\text{SG}}}(N_P, N_P)$ is epimorphism $\forall P \triangleleft S$
 $\text{(by 3.10)} \Leftrightarrow M_P \xrightarrow{f_P} N_P$ is a split epimorphism

(3.11.2) - Corollary: Let $P \in \text{Mod-SG}$. Then P is projective $\Leftrightarrow \forall P \triangleleft S$, P_P is a projective $S_P G$ -module.

Proof: LHS \Leftrightarrow all epimorphisms $M \xrightarrow{f} P \rightarrow 0$ split
 $(\text{LHS})_P \Leftrightarrow (\dots \dashv \dashv \dashv \dashv \dashv \dashv \dashv)_P$.

(3.12): Let P be an SG-lattice. If $|G| \in U(S)$ then P is projective.

P is an SG-lattice $\Leftrightarrow P \in \text{Mod-SG}$ is projective as an S -module.

Proof: (Essentially Maschke's Theorem): Let $M \xrightarrow{f} P \rightarrow 0$ be an epimorphism of SG-modules. Since P is S -projective, this splits, so $\exists \varphi \in \text{Hom}_S(P, M)$ with $\varphi f = 1_P$. Let $\theta \in \text{Hom}_S(P, M)$; define θ^g by $\theta^g = (g^{-1})_P \theta g_M$ ($g \in G$). θ is an SG-homomorphism $\Leftrightarrow \theta^g = \theta \ \forall g$, ie $\text{Hom}_{\text{SG}}(P, M)$ is the fixed points under this G -action.

Define $\Psi: P \rightarrow M$ by $\Psi = \frac{1}{|G|} \sum_{g \in G} \varphi^g$. This is obviously fixed by G , and it is in $\text{Hom}_{\text{SG}}(P, M)$.

$\Psi f = \frac{1}{|G|} \sum \varphi^g f = \frac{1}{|G|} \sum (\varphi f)^g$, because g is an SG-map, $= 1_P$.

(3.13.1): P an SG-lattice. Then P is projective $\Leftrightarrow P_P$ is projective $\wedge P \triangleleft S$ such that $|G| \in P$.

P_1, \dots, P_r primes of S . Then $S_{\{P_1, \dots, P_r\}} = \Lambda^1 S$, where $\Lambda = S \setminus (P_1, \dots, P_r)$. Let $\pi = \{P_1, \dots, P_r\}$. Write $S_{\{P_1, \dots, P_r\}}$ as S_{π} . This is a semi-local ring, with maximal ideals $\Lambda^1 P_1, \dots, \Lambda^1 P_r$, ie $P_{1\pi}, \dots, P_{r\pi}$.

Recall: $S_{\pi, P_i\pi} \cong S_{P_i}$.

(3.13.2): Let P be an $S\mathbb{G}$ -lattice. Then P_{π} (an $S_{\pi}\mathbb{G}$ -lattice) is projective as an $S_{\pi}\mathbb{G}$ -module $\Leftrightarrow P_{\pi}$ is $S_{\pi}\mathbb{G}$ -projective $\forall \pi \in \Pi$ [3.11.2] for S_{π} replacing S

(3.13.3): Let P be a $\mathbb{Z}\mathbb{G}$ -lattice, and π the set of primes dividing $|\mathbb{G}|$. Then P is projective $\Leftrightarrow P_{\pi}$ is $\mathbb{Z}_{\pi}\mathbb{G}$ -projective.

Define $\mathbb{Z}_{(G)} = \mathbb{Z}_{\pi}$ for this π , and similarly for any M in $\mathbb{Z}\mathbb{G}$.

(3.13.4): A $\mathbb{Z}\mathbb{G}$ -lattice P is projective $\Leftrightarrow P_{(G)}$ is projective.

(3.14): (Rim's Lemma): Let $X \triangleleft \mathbb{Z}\mathbb{G}$. Suppose $0 \neq m \in \mathbb{Z} \cap X$. If $(m, |\mathbb{G}|) = 1$, then X is projective.

Proof: $0 \rightarrow X \rightarrow \mathbb{Z}\mathbb{G} \rightarrow \mathbb{Z}\mathbb{G}/X \rightarrow 0$ is exact. So $0 \rightarrow X_{(G)} \rightarrow \mathbb{Z}_{(G)} \rightarrow (\mathbb{Z}\mathbb{G}/X)_{(G)} \rightarrow 0$ over $\mathbb{Z}_{(G)}\mathbb{G}$.

So $X_{(G)} \cong \mathbb{Z}_{(G)}$, so $X_{(G)}$ is free, rank 1, so X is projective by (3.13.4).

Example: Let P be a big prime. Then $\mathbb{Z}C_p$ has projective non-free ideals.

Let \mathfrak{S} be $e^{\frac{2\pi i}{p}}$ and $R = \mathbb{Z}[\mathfrak{S}]$ the integers of $\mathbb{Q}(\mathfrak{S})$.

If $p > 23$, the class number > 1 , which means R has a projective ideal which is not principal. Easy to arrange such an ideal A with $m \in A$, $p \nmid m$.

Let $\langle x \rangle$ have order p and let $T = \mathbb{Z}\langle x \rangle$. Then map T onto R via $\sum n_i x^i \mapsto \sum n_i \mathfrak{S}^i$. This has kernel BT with $B = 1 + x + \dots + x^{p-1}$.

Let X be the inverse image of A . $X \triangleleft T$, $m \in X$, so Rim's lemma says that X is projective. But X is not principal.

If X is free then $X \cong (\mathbb{Z}\langle x \rangle)^m$, $m > 1$, but $X \otimes_{\mathbb{Z}} \mathbb{Q} \cong (\mathbb{Q}\langle x \rangle)^m$.

But as T/X is killed by m , so LHS = $\mathbb{Q}\langle x \rangle - \#$ as $m > 1$ and commutative rings have fixed rank.

(4.1): P_1, \dots, P_r distinct maximal ideals of S and M an S -module. Suppose $m_1, \dots, m_r \in M$. Then $\exists \mu \in M$ with $\mu \equiv m_i \pmod{MP_i}$ for each i .

(Chinese Remainder Theorem).

Proof: $P_i + P_j = S$ if $i \neq j$. We get $P_i + \bigcap_{j \neq i} P_j = S$, so $x_i + \beta_i = 1$, with $x_i \in P_i$, $\beta_i \in \bigcap_{j \neq i} P_j$. So $\text{Mod } MP_i$, $\mu := \sum m_j \beta_j \equiv m_i \beta_i \equiv m_i(x_i + \beta_i) = m_i$.

(4.2): Suppose M and N are $S\mathbb{G}$ -lattices. Suppose P_1, \dots, P_r distinct maximal ideals of S . Suppose also that $M_{P_i} \cong N_{P_i}$ for each i . Then \exists exact sequence $0 \rightarrow M \rightarrow N \rightarrow X \rightarrow 0$ with $X_{P_i} = 0$ each i . (Here, S is a domain)

In particular, if P_1, \dots, P_r exhaust the maximal ideals of S , then $M \cong N$.

Proof: We find $M \xrightarrow{f} N$ so that f_{P_i} is an isomorphism for each i .

Then $0 \rightarrow U = \ker f \rightarrow M \xrightarrow{f} N \rightarrow X = \text{coker } f \rightarrow 0$.

Localising: $0 \rightarrow M_{P_i} \xrightarrow{f_{P_i}} N_{P_i} \rightarrow 0$.

But M is projective for S and so torsion-free, so $U_{\mathfrak{P}_i} = 0$ gives $U = 0$.
 So, apply (4.1) to $\text{Hom}_{S\text{-}\mathcal{C}}(M, N)$. Suppose $M_{\mathfrak{P}_i} \xrightarrow{g_i \cong} N_{\mathfrak{P}_i}$ are isomorphisms.
 By (3.8.2), $\exists M \xrightarrow{f_i} N$ and $\lambda_i \in P_i$ with $g_i \lambda_i = f_{i, \mathfrak{P}_i}$. Clearly f_{i, \mathfrak{P}_i} are
 isomorphisms. By (4.1), $\exists f \in \text{Hom}_{S\text{-}\mathcal{C}}(M, N) =: H$, such that $f \equiv f_i \pmod{H_{\mathfrak{P}_i}}$ each i .
 Hence f and f_i induce the same $M/M_{\mathfrak{P}_i} \rightarrow N/N_{\mathfrak{P}_i}$ map.
 But $M/M_{\mathfrak{P}_i} \cong M_{\mathfrak{P}_i}/M_{\mathfrak{P}_i} \mathfrak{P}_{i, \mathfrak{P}_i} =: \hat{M}_i$
 So $f_{\mathfrak{P}_i}$ and f_{i, \mathfrak{P}_i} induce the same map $\hat{M}_i \rightarrow \hat{N}_i$.
 In particular, $f_{\mathfrak{P}_i}$ induces an isomorphism $\hat{M}_i \cong \hat{N}_i$.
 Since $\mathfrak{P}_{i, \mathfrak{P}_i} \subseteq \text{Jac}(S_{\mathfrak{P}_i} G)$, we get $f_{\mathfrak{P}_i}$ is an isomorphism from $M_{\mathfrak{P}_i}$ to $N_{\mathfrak{P}_i}$.

(4.3): Let π be a finite set of rational primes. Suppose M, N are $\mathbb{Z}G$ -lattices.
 Then M_π and N_π are isomorphic $\mathbb{Z}G$ -lattices iff $M_{(p)} \cong N_{(p)}$ $\forall p \in \pi$.
 In particular $M_{(\pi)} \cong N_{(\pi)}$ if $M_{(p)} \cong N_{(p)}$ for all $p \in \pi$.

(4.4) (Maranda's Theorem): Let p be prime and $|G| = p^k m$ and $p \nmid m$. Let M, N be $\mathbb{Z}_p G$ -lattices. Then $M \cong N$ iff $M/M_{p^{k+1}} \cong N/N_{p^{k+1}}$.

Proof:

φ	\downarrow	M	Since M is $\mathbb{Z}_{(p)}$ -projective \exists a $\mathbb{Z}_{(p)}$ -module homomorphism
	\downarrow nat.		φ as shown.
	\downarrow	$M/M_{p^{k+1}}$	Since m is a unit in $\mathbb{Z}_{(p)}$, can write $\psi: M \rightarrow N$ for
	$\downarrow \alpha$		$\psi = \frac{1}{m} \sum_{x \in G} \varphi^x$. (Clear this is a $\mathbb{Z}_{(p)} G$ -map.)
N	$\xrightarrow{\text{nat}}$	$N/N_{p^{k+1}} \rightarrow 0$	Let $\theta = \text{nat} \alpha: M \rightarrow N/N_{p^{k+1}}$.

Consider $\psi \text{nat}: M \rightarrow N/N_{p^{k+1}}$. $\psi \text{nat} = \frac{1}{m} \sum_{x \in G} (\varphi \text{nat})^x = \frac{1}{m} \sum_x \theta^x = \frac{1}{m} |G| \theta = p^k \theta$.
 So ψnat maps M epimorphically onto $N_{p^k}/N_{p^{k+1}}$.
 But $N_{p^k} \rightarrow N_{p^k}/N_{p^{k+1}}$ is an essential epimorphism. Hence ψ maps onto N_{p^k} .
 $M \rightarrow M/M_p$
 $\psi \downarrow \quad \downarrow \bar{\psi}$ As before, enough to show $\bar{\psi}$ is an isomorphism.
 $N_{p^k} \rightarrow N_{p^k}/N_{p^{k+1}}$

Suppose $\bar{\mu} = M_p + \mu$ is in the kernel of $\bar{\psi}$. Then $\mu \psi \in N_{p^{k+1}}$, ie $\mu \psi \text{nat} = 0$,
 ie $\mu p^k \theta = 0$. So $\mu p^k \in \ker \theta = M_{p^{k+1}}$, say $\mu p^k = \mu_1 p^{k+1}$. But M is a torsion-free
 $\mathbb{Z}_{(p)}$ -module, so $\mu = \mu_1 p$, ie $\bar{\mu} = 0$. Hence $\bar{\psi}$ is an isomorphism and we're done.

(4.5) (Bass's Cancellation Theorem): Let π be a finite set of primes. Let L, M, N be $\mathbb{Z}_\pi G$ -lattices. If $L \oplus M \cong L \oplus N$ then $M \cong N$.

Proof: We know $M \cong N \iff M_{(p)} \cong N_{(p)}$ all $p \in \pi$. If $p \notin \pi$ then $L_{(p)} \oplus M_{(p)} \cong L_{(p)} \oplus N_{(p)}$,
 so assume $\pi = \{p\}$. If $|G| = p^k m$ with $p \nmid m$, then Maranda's Theorem says
 that all we need is $M/M_{p^{k+1}} \cong N/N_{p^{k+1}}$. But $L/L_{p^{k+1}} \oplus M/M_{p^{k+1}} \cong L/L_{p^{k+1}} \oplus N/N_{p^{k+1}}$,
 so we're reduced to $\mathbb{Z}/p^{k+1} \mathbb{Z} G$ -modules.

We have the Krull-Schmidt Theorem for finite rings. Let w_1, \dots, w_m, \dots be the indecomposable modules. Any $\mathbb{F}_q R$ -module A can be written uniquely as
 $w_1^{\alpha_1} \oplus w_2^{\alpha_2} \oplus \dots$ ($\alpha_i \geq 0, \alpha_i \in \mathbb{Z}$). Say $A \sim \underline{\alpha}$. If $B \sim \underline{\beta}$ then $A \oplus B \cong w_1^{\alpha_1 + \beta_1} \oplus w_2^{\alpha_2 + \beta_2} \oplus \dots$
 If $A \oplus B \cong A \oplus C$, then $\alpha_i + \beta_i = \alpha_i + \gamma_i$ and $\beta_i = \gamma_i$. Hence $B \cong C$.

Definition: M, N $\mathbb{Z}G$ -lattices. Say M and N are in the same genus $\Leftrightarrow M_{(G)} \cong N_{(G)}$.

Swan's Theorems will show that M, N are in the same genus $\Leftrightarrow M_{(p)} \cong N_{(p)}$, all p . Write $M \vee N$.

Corollary to Bass: Let L, M, N be $\mathbb{Z}G$ -lattices. Then if $L \otimes M \vee L \otimes N$, we have $M \vee N$.

Swan's Theorems.

Swan 1: $M \in \mathbb{Z}G\text{-proj.} \Rightarrow M \cong (\mathbb{Z}G)^t \oplus I$, with $I \triangleleft \mathbb{Z}G$ with $I \vee \mathbb{Z}G$, and I can be chosen so that $(\mathbb{Z}G/I)_\pi = 0$ at any finite set of primes.

Note: Let U be a f.g. \mathbb{Z} -module with $U_\pi = 0$. Then $Um = 0$ for some $m \in \mathbb{Z}$ coprime to π . Eg, $U_{(G)} = 0 \Leftrightarrow Um = 0$, some $m \nmid |G|$

Swan 2: If $M \in \mathbb{Z}G\text{-proj.}$, then $M_{(G)} \cong (\mathbb{Z}_{(G)}/G)^{t+1}$, ie $M \vee (\mathbb{Z}G)^{t+1}$

Corollary of S2: If $M \in \mathbb{Z}_{(G)}^G\text{-proj.}$, then M is free.

Proof of Corollary: (3.4.4) says that $M \cong V_{(G)}$ with V a $\mathbb{Z}G$ -lattice.

(3.14.4) says V is projective $\Leftrightarrow V_{(G)}$ is projective.

Swan 2 tells us $V_{(G)}$ is free, ie M is free.

Swan 3: If $M \in \mathbb{Z}G\text{-proj.}$, then $M\mathbb{Q} \cong (\mathbb{Q}G)^{t+1}$ is free. [$M\mathbb{Q} := M \otimes_{\mathbb{Z}} \mathbb{Q}$].

Swan 4: Let P be a prime. If M, N are $\mathbb{Z}_{(P)}/G$ -projective, then $M \cong N \Leftrightarrow M\mathbb{Q} \cong N\mathbb{Q}$.

Corollary of S4: $M \vee N \Leftrightarrow M_{(p)} \cong N_{(p)}$. ($M, N \in \mathbb{Z}G\text{-proj.}$)

Proof of Corollary: Suppose $M \vee N$, ie $M_{(G)} \cong N_{(G)}$, and $M_{(G)}\mathbb{Q} \cong N_{(G)}\mathbb{Q}$, ie $M\mathbb{Q} \cong N\mathbb{Q}$. But $M_{(p)}\mathbb{Q} \cong M\mathbb{Q}$, so we can apply Swan 4 to $M_{(p)}$ and $N_{(p)}$.

Plan: Will show: S3 + S4 \Rightarrow S2, S3 + S4 \Rightarrow S1 (via S2), S3, S4.

Proof of Swan 2: Suppose $M \in \mathbb{Z}G\text{-proj.}$ Swan 3 tells us that $M\mathbb{Q} \cong (\mathbb{Q}G)^m$.

Then $M_{(p)}\mathbb{Q} \cong (\mathbb{Z}_{(p)}/G \otimes \mathbb{Q})^m$, ie $M_{(p)}\mathbb{Q} \cong (\mathbb{Z}_{(p)}/G)^m \otimes \mathbb{Q}$.

Then Swan 4 applied to $M_{(p)}$ and $(\mathbb{Z}_{(p)}/G)^m$ gives Swan 2.

Proof of Swan 1:

(S.1): Suppose $M \in \mathbb{Z}G\text{-proj.}$ and $M \vee (\mathbb{Z}G)^t$, $t \geq 1$. Then $M = (\mathbb{Z}G)^{t-1} \oplus I$, $I \triangleleft \mathbb{Z}G$, $I \vee \mathbb{Z}G$.

Assume (5.1). From Corollary S4, since $I \vee \mathbb{Z}G$ we know $I_{(p)} \cong \mathbb{Z}_{(p)}G$ for all primes p , and so $I_\pi \cong \mathbb{Z}_\pi G$ for all finite sets π of primes.

Then (4.2) applies to give: $\exists 0 \rightarrow I \rightarrow \mathbb{Z}G \rightarrow X \rightarrow 0$, and $X_\pi = 0$.

Case t=1: exactly the same. $M \vee \mathbb{Z}G$, therefore $0 \rightarrow M \rightarrow \mathbb{Z}G \rightarrow X \rightarrow 0$, $X_\pi = 0$, any finite set of primes.

Proof of (5.1): By induction on t . Suppose $t > 1$. $M \vee (\mathbb{Z}G)^t$. By (4.2), we have $0 \rightarrow M \rightarrow (\mathbb{Z}G)^t \rightarrow X \rightarrow 0$, with $X_{(G)} = 0$. Let α be the projection of $(\mathbb{Z}G)^t$ onto the last summand.

$$\begin{array}{ccccccc} 0 & \rightarrow & M & \rightarrow & (\mathbb{Z}G)^t & \rightarrow & X \rightarrow 0 \\ & & \downarrow \alpha_M & & \downarrow \alpha & & \downarrow \beta \\ 0 & \rightarrow & I & \rightarrow & \mathbb{Z}G & \rightarrow & Y \rightarrow 0 \end{array}$$

β is an epimorphism, so $Y_{(G)} = 0$.
Thus $I_{(G)} \cong \mathbb{Z}_{(G)}G$.

(3.14.4) \Rightarrow I is projective.

Hence α_M is split and $M \cong I \oplus N$. Then $(\mathbb{Z}G)^t \vee \mathbb{Z}G \oplus N$. By Bass again we get $N \vee (\mathbb{Z}G)^{t-1}$ and, of course, $N \in \mathbb{Z}G$ -proj. By induction, $N \cong (\mathbb{Z}G)^{t-2} \oplus J$, with $J \vee \mathbb{Z}G$ and $J \trianglelefteq \mathbb{Z}G$. So $M \cong (\mathbb{Z}G)^{t-2} \oplus I \oplus J$. We want $I \oplus J \cong \mathbb{Z}G \oplus L$, with $L \trianglelefteq \mathbb{Z}G$.

$\exists 0 \rightarrow I \xrightarrow{\varphi} \mathbb{Z}G \rightarrow V \rightarrow 0$ and $V_{(G)} = 0$, by (4.2), i.e. $V_m = 0$, $(m, |G|) = 1$.

Corollary S4 said $J \vee \mathbb{Z}G \Rightarrow J_{(p)} \cong (\mathbb{Z}G)_{(p)}$, all p .

$\exists 0 \rightarrow J \xrightarrow{\psi} \mathbb{Z}G \rightarrow W \rightarrow 0$ with $(W^o, m) = 1$, by (4.2).

We now consider:

$$0 \rightarrow L \xrightarrow{\text{ker } (\varphi, \psi)} I \oplus J \xrightarrow{\varphi, \psi} \mathbb{Z}G \xrightarrow{\text{coker } (\varphi, \psi)} U \rightarrow 0.$$

Now $V^o + W^o \subseteq U^o$. But this means $U = 0$, by the choice of W^o , as they are coprime ideals. So we have: $0 \rightarrow L \rightarrow I \oplus J \rightarrow \mathbb{Z}G \rightarrow 0$. And as $\mathbb{Z}G$ is free, $I \oplus J \cong \mathbb{Z}G \oplus L$, as required.

Consider Swan 3: $M \in \text{proj } \mathbb{Z}G \Rightarrow M \otimes_{\mathbb{Z}} \mathbb{Q} = M\mathbb{Q}$ is a free module.

- (a) Discussion of a freeness criterion for kG -modules, k of characteristic zero.
- (b) Application of (a).

(a) M, V finitely generated kG -modules. $M^* = \text{Hom}_k(M, k)$.

(5.2.1): $M^* \otimes_k V \cong \text{Hom}_k(M, V)$.

Proof: $LHS \rightarrow RHS: g \otimes v \mapsto (u \mapsto (gu)v) \in RHS$. Let e_1, \dots, e_n be a basis of M , f_1, \dots, f_m a basis for V . Then if e_1, \dots, e_n is the dual basis of M^* , then $M^* \otimes_k V$ has basis $e_i \otimes f_j \mapsto \begin{cases} e_i \mapsto f_j & , \text{ has matrix } e_{ij} \\ e_k \mapsto 0 \text{ if } k \neq j & \text{the } \{e_{ij}\} \text{ are a basis.} \end{cases}$. This is an isomorphism, as

If $\Phi \in \text{Hom}_k(M, V)$, $g \in G$, then $\Phi^g = g^{-1} \Phi g$. $M \xrightarrow{g^{-1}} M \xrightarrow{\Phi} V \xrightarrow{g} V$. Then $\text{Hom}_k(M, V)$ is a kG -module. In particular, when $V = k$, the trivial module, then M^* is a kG -module via $\Phi^g = g^{-1} \Phi$.

If A, B are kG -modules, then $A \otimes_k B$ is a kG -module with action $(a \otimes b)g = ag \otimes bg$.

$$(5.2.2): M^* \otimes_{\mathbb{K}} V \xrightarrow{\cong} \text{Hom}_{\mathbb{K}G}(M, V)$$

$$(5.2.3): (M^* \otimes_{\mathbb{K}} V)^G \xrightarrow{\cong} \text{Hom}_{\mathbb{K}G}(M, V). \quad [M^G = \{\mu \in M : \mu g = \mu \ \forall g \in G\}]$$

V a $\mathbb{K}G$ -module, character χ . $\chi(g) = \text{trace } g_v$. $\chi(1) = d(V)$. $V \cong W \Leftrightarrow \chi_v = \chi_w$. Suppose $V = \mathbb{K}G$. If $g \in G$ then $rg \neq v$ unless $g = 1$. Then $\chi_v(1) = |G|$ and $\chi_v(x) = 0$ for all other x . So if $V = (\mathbb{K}G)^r$ then $\chi_v(1) = r|G|$, and $\chi_v(x) = 0$, all other x .

$$(5.3.1): V \text{ is free} \Leftrightarrow |G| \mid \chi_v(1) \text{ and } \chi_v(x) = 0, \text{ all other } x.$$

Proof: Suppose $\chi_v(1) = |G|r$. We need $V \cong (\mathbb{K}G)^r$ - follows as they have the same character.

$$(5.3.2): V \text{ is free} \Leftrightarrow \chi_v(x) = 0 \text{ for all non-trivial } x.$$

(V is free $\Leftrightarrow V$ is free for every $\mathbb{K}\langle x \rangle$, $1 \neq x \in G$).

Proof: If $M = \mathbb{K}G$, then $M^G = \mathbb{K} \sum_{g \in G} g$. If we have r copies of $\mathbb{K}G$, i.e. $V = (\mathbb{K}G)^r$, then $r = \dim V^G$.

Let $r = \dim(V^G)$. We need $V \cong (\mathbb{K}G)^r$. These two modules have characters vanishing at non-unit elements. We need $\dim(V) = r|G| = |G| \cdot \dim(V^G)$.

Consider $V^{|G|}$ and $(\mathbb{K}G)^{d(V)}$. These have same dimension and so they have the same character. So $V^{|G|} \cong (\mathbb{K}G)^{d(V)}$. Hence $(V^G)^{|G|} \cong \mathbb{K}^{d(V)}$.

$$\text{So } |G|d(V^G) = d(V).$$

Note: $V = \bigoplus_{M \in \mathcal{R}} M^{S_M}$, $S_i \geq 0$ M irreducible modules.

$$\mathbb{K}G = \bigoplus_{M \in \mathcal{R}} M^{r_M}. \quad V \text{ is free} \Leftrightarrow \exists r \text{ with } S_M = r r_M \text{ and } S_1 = r \cdot 1.$$

$$\Rightarrow V = (\mathbb{K}G)^r. \quad \text{The } r \text{ which has to come up in } S_1, \text{ and } S_1 = \dim V^G.$$

$$(5.4): T \in \mathbb{K}G\text{-mod} \text{ and } V \text{ a free } \mathbb{K}G\text{-module, then } T \otimes_{\mathbb{K}} V \text{ is free, } \cong V^{d(T)}, \text{ and hence } |G| \cdot d(T \otimes V)^G = d(T)d(V). \quad -(1)$$

$$(5.5) \text{ If } V \in \mathbb{K}G\text{-mod} \text{ then } V \text{ is free if (1) holds for all } T.$$

Proof of (5.4): Character of $T \otimes V$ is $\chi(T)\chi(V)$, which vanishes on all non-unit x in G .

So $T \otimes V$ is free by (5.3.2). So $T \otimes V \cong V^{d(T)}$, by dimensions.

Proof of (5.5): Refer to note above. Apply (1) to M^* , where M is a simple, non-trivial irreducible module, to get:

$$|G|d((M^* \otimes V)^G) = |G| \cdot \dim \text{Hom}_{\mathbb{K}G}(M, V) = |G|s_M \cdot \dim \text{Hom}_{\mathbb{K}G}(M, M) = d(M)d(V).$$

Apply (1) with $T = \mathbb{K}$ to get: $|G| \cdot d(V^G) = d(V)$. Hence $|G|d(M)d(V^G) = |G|s_M \dim \text{Hom}(M, M)$. And $|G|d(M)d((\mathbb{K}G)^G) = |G|r_M \cdot \dim \text{Hom}(M, M)$ - (2). (2), (3) $\Rightarrow s_M = r_M d(V^G)$, $\forall M$.

Recall S3: If $M \in \mathbb{Z}G$ -proj., then $M\mathbb{Q}$ is free.

We know that $M\mathbb{Q}$ is free if it's free as a $\mathbb{Q}\langle x \rangle$ -module for all x in G . If $H \leq G$ and T is a transversal to the left cosets of H in G , then $\mathbb{Z}G = \bigoplus_{t \in T} t\mathbb{Z}H$, and this is free as a $\mathbb{Z}H$ -module. Hence any $\mathbb{Z}G$ -projective is $\mathbb{Z}H$ -projective. Hence in S3, assume G is abelian.

(5.6): If G is Abelian and if $M \in \mathbb{Z}G$ -proj. then $|G| d(M\mathbb{Q})^G = d(M\mathbb{Q})$.

Proof: Consider two cases: (i) $|G| = p^m$, p prime, (ii) $G = H \times K$, $|H| < |K|$, $(|H|, |K|) = 1$.

(5.7): If $|G| = p^n$ then $\mathbb{Z}_{(p)}G$ is local.

(5.7) $\Rightarrow M_{(p)} \in \text{proj-} \mathbb{Z}_{(p)}G$ and so $M_{(p)}$ is free and hence $M\mathbb{Q}$ is free. So case (i) follows from (5.7).

Proof of (5.7): $p \in J = \text{Jac}(\mathbb{Z}_{(p)}G)$. Let U be a simple $\mathbb{Z}_{(p)}G$ -module. Then $U_p = 0$.

Since $|U| = p^r$ and $|G| = p^n$ we get $U^G > 0$. Hence $U = U^G$ and $Ug_{(p)} = 0$.

Hence $J = (p) + g_{(p)}$ is of index p in $\mathbb{Z}_{(p)}G$.

Proof of (5.6) (ii): Consider M^K as a $\mathbb{Z}K$ -module. Provided M^K is projective we get

$$|K| \dim(M^K\mathbb{Q})^K = \dim(M^K\mathbb{Q}), \text{ and } |H| \cdot |K| \cdot \underbrace{\dim(M^K\mathbb{Q})^H}_{\dim(M\mathbb{Q})^{HK}} = |H| \underbrace{\dim(M^K\mathbb{Q})}_{{\dim(M\mathbb{Q})}^H}$$

We want:

$$\text{Giving: } |G| \cdot d(M\mathbb{Q})^G = |H| d(M\mathbb{Q})^H = d(M\mathbb{Q}), \text{ by induction.}$$

So we need: (a) M^K projective over $\mathbb{Z}K$.

$$(b) (M^K\mathbb{Q})^H = (M\mathbb{Q})^H.$$

(a) $\mathbb{Z}G = \bigoplus_{h \in H} h\mathbb{Z}H = \bigoplus_{h \in H} (\mathbb{Z}K)h$, so the elements have form $\sum_{h \in H} \sigma_h h$, $\sigma_h \in \mathbb{Z}K$.

If $\xi = \sum \sigma_h h$ is killed by all h except 1, then the σ_h is independent of h , and $\xi = \sigma_1 \sum_{h \in H} h = \sigma_1 \eta$ (say).

Hence $(\mathbb{Z}G)^H = \eta \mathbb{Z}K$, free $\mathbb{Z}K$ -module, rank 1. So (a) is true if $M = \mathbb{Z}G$.

In general, $\exists N$ with $M \oplus N \cong (\mathbb{Z}G)^F$, so $M^H \oplus N^H \cong ((\mathbb{Z}G)^F)^H \cong (\mathbb{Z}H)^F$. Hence (a).

(b) If $m/\lambda g = m/\lambda$ ($m \in M$, $\lambda \neq 0$) then $(mg - m)/\lambda = 0$. But M is torsion free over \mathbb{Z} .

So $mg = m$.

To conclude the proof S3 we need to check (5.5). Let T be any $\mathbb{Q}G$ -module.

We want $|G| \cdot d(T \otimes_{\mathbb{Q}} M\mathbb{Q})^G = d(T) d(M\mathbb{Q})$. By (3.82) $T \cong B \otimes_{\mathbb{Z}} \mathbb{Q}$ for some $\mathbb{Z}G$ -lattice B .

Note $(B \otimes_{\mathbb{Z}} \mathbb{Q}) \otimes_{\mathbb{Q}} M\mathbb{Q} \cong (B \otimes_{\mathbb{Z}} M) \otimes_{\mathbb{Z}} \mathbb{Q}$.

(5.8): $B \otimes_{\mathbb{Z}} M$ is a projective $\mathbb{Z}G$ -lattice.

Once (5.8) is done, apply (5.6) to $B \otimes_{\mathbb{Z}} M$. Left hand side is $|G| d(T \otimes_{\mathbb{Q}} M\mathbb{Q})^G$.

Right hand side is $d(B \otimes_{\mathbb{Z}} M)\mathbb{Q} = d(T) d(M\mathbb{Q})$.

Proof of (5.8): $\exists N$ such that $M \otimes N \cong (\mathbb{Z}G)^F$, so $B \otimes_{\mathbb{Z}} M \oplus B \otimes_{\mathbb{Z}} N \cong (B \otimes_{\mathbb{Z}} \mathbb{Z}G)^F$. So if we can show $B \otimes_{\mathbb{Z}} \mathbb{Z}G$ is free then we're done. We prove $B \otimes_{\mathbb{Z}} \mathbb{Z}G \cong (\mathbb{Z}G)^F$, $F = \dim(B\mathbb{Q})$.

$B \otimes_{\mathbb{Z}} \mathbb{Z}G$ is a $\mathbb{Z}G$ -module via $(b \otimes \sigma)g = bg \otimes \sigma g$. It is also a $\mathbb{Z}G$ -module, via $(b \otimes \sigma)g = b \otimes \sigma g$, and here is $\cong B_0 \otimes_{\mathbb{Z}} \mathbb{Z}G$, where B_0 is B , forgetting the action. $B_0 \otimes \mathbb{Z}G$ is $\bigoplus_{\text{basis of } B} s \otimes \mathbb{Z}G$.

We have action-preserving maps: $b \otimes g \xrightarrow{\downarrow} bg^{-1} \otimes g \xrightarrow{\uparrow} b \otimes g$, so done.

This does (5.8), hence does Swan 3.

Consider 5.6: M, N are $\mathbb{Z}_{(p)}G$ -lattices $\Rightarrow M \cong N \Leftrightarrow M\mathbb{Q} \cong N\mathbb{Q}$.

M and N are free $\mathbb{Z}_{(p)}$ -modules. We get representations α on M and β on N over $\mathbb{Z}_{(p)}$. The point is that if $x \in \mathbb{Z}_{(p)}G$ then $x\alpha, x\beta$ have the same characteristic polynomial, because $M\mathbb{Q} \cong N\mathbb{Q}$.

Also, $M \cong N \Leftrightarrow M/M_p \cong N/N_p$. We have representations $\bar{\alpha}, \bar{\beta}$ on $\bar{M} = M/M_p, \bar{N} = N/N_p$. Because the characteristic polynomials of $x\bar{\alpha}, x\bar{\beta}$ are those of $x\alpha, x\beta$ mod p , we have $x\bar{\alpha}, x\bar{\beta}$ with same characteristic polynomial $\forall x$ in $\mathbb{Z}/p\mathbb{Z}G$.

(5.9): Suppose A is a finite dimensional algebra over a field. Suppose U, V are A -modules giving rise to representations θ, φ . Suppose for all x in A , the characteristic polynomials of $x\theta$ and $x\varphi$ are the same. Then $\text{Gr } U \cong \text{Gr } V$.

Note: $0 = U_0 < U_1 < \dots < U_n = U$, a composition series (so U_{i+1}/U_i simple).

Characteristic polynomial of $x\theta$ is the same as that on $U_1 \oplus U_2/U_1 \oplus \dots \oplus U_n/U_{n-1} = \text{Gr } U$.

(5.10) (Brauer's Theorem): Suppose $A = kG$. Suppose U, V are projective A -modules.

If $\text{Gr } U \cong \text{Gr } V$ then $U \cong V$.

In our case, with $U = M/M_p, V = N/N_p$, (5.9) and (5.10) gives Swan 4.

Discussion of (5.10): U a projective A -module. $J = \text{Jac}(A)$. U/JU is an A/J -module and so $U/JU = \bigoplus_i M_i^{s_i}$, where M_1, \dots, M_m are the distinct simple A -modules. Recall end of section 1, about idempotents.

$$\begin{array}{c} \overbrace{M_1, \dots, M_m}^{\text{distinct simple } A\text{-modules}} \\ \overbrace{e_1, \bar{A}_1, \dots, e_m, \bar{A}_m}^{\text{idempotents}}, \bar{A} = A/J \\ \uparrow \qquad \uparrow \\ \overbrace{e_1, A_1, \dots, e_m, A_m}^{\text{idempotent.}} \\ P_1, \dots, P_m - \text{principal indecomposable} \\ \text{projectives.} \end{array}$$

Form $P = \bigoplus_i P_i^{s_i}$, so that $P/PJ \cong U/JU$. Because P, U are projective, we get $P \cong U$. Define $c_{ij} = \# \text{times } M_j \text{ occurs in } \text{Gr } P_i$. $C(A) = \text{matrix}(c_{ij})$ is called the Cartan Matrix.

(5.11) (Brauer): If $A = kG$ then $C(A)$ is non-singular. (Proof omitted).

Proof of (5.10): (Using (5.11)). $U = \bigoplus_{i=1}^m P_i^{s_i}, V = \bigoplus_{i=1}^m P_i^{t_i}$. Hypothesis: $\sum_{j=1}^m s_i c_{ij} = \sum_{j=1}^m t_i c_{ij}$. i.e., $(\underline{s} - \underline{t})C = 0$. (5.11) $\Rightarrow \underline{s} = \underline{t}$, i.e. $U \cong V$.

Proof of (5.9): We may as well assume $U \cong \text{Gr} U$, $V \cong \text{Gr} V$. Since $\text{Jac}(A)$ kills both U and V , we may assume A is semi-simple. Let e be a primitive idempotent in A . Then $e\theta$ is an idempotent in $\text{Hom}_A(U, U)$. If $e\theta \neq 0$, then eA occurs as a summand in U , and vice versa. But $e\theta = 0$ iff it has all its characteristic roots being zero. Hence $e\theta \neq 0 \Leftrightarrow e\varphi \neq 0$. That is, eA occurs in $U \Leftrightarrow eA$ occurs in V . Take e so that this happens.

Then $U \cong eA \oplus U'$, $V \cong eA \oplus V'$. The same hypotheses hold for U', V' and we are done by induction.

So we have shown Swan 4.

3. Relation Modules.

Group Rings and the Relation Sequence from a Presentation.

Recall we had $1 \rightarrow R \rightarrow F \xrightarrow{\pi} G \rightarrow 1$, G finite, F free of finite rank.

Quotienting $\Rightarrow 1 \rightarrow \overline{R}/R \rightarrow F/R \rightarrow G \rightarrow 1$ — object is to convert this into
($\mathbb{Z}G = \overline{R}$, a $\mathbb{Z}G$ -module)

what is called the corresponding relation sequence of $\mathbb{Z}G$ -modules:

$$1 \rightarrow \overline{R} \rightarrow (\mathbb{Z}G)^{\text{d}(F)} \xrightarrow{\text{d}(\pi)} g_F \rightarrow 0.$$

Effectively, our applications of Sections 1 and 2 will compare these for various presentations.

Slight change of notation. Let $\overline{1 \triangleleft H \trianglelefteq G}$. Consider the natural map $G \xrightarrow{\Phi} G/H$ and hence of $\mathbb{Z}G \xrightarrow{\Phi} \mathbb{Z}(G/H)$. If $G = H$, we considered this — the augmentation map, kernel g_F .

(6.1) (i): $\text{Ker } \Phi = \bar{f}$, where \bar{f} is the ideal of $\mathbb{Z}G$ generated by f .

Note: A bar $\bar{-}$ means the right ideal on what is under it.

Let $h \in H$, $x \in G$. $(h-1)x = x(h^x-1)$. ie, $\bar{f}x = x\bar{f}$. So, $\bar{f}\mathbb{Z}G = \mathbb{Z}G\bar{f}$, so right and left ideals on \bar{f} with $H \trianglelefteq G$ are the same.

$$(6.1) (ii): \bar{f}/g_F \underset{\mathbb{Z}G}{\cong} H/H'$$

$\bar{f} = \langle h-1 \rangle \xrightarrow{\Phi} \langle 1-1 \rangle = 0$, so $\bar{f} \subseteq \text{Ker } \Phi$. Let T be a transversal to the cosets of H in G . $\mathbb{Z}G = \bigoplus_{t \in T} t\mathbb{Z}H$. Then $\bar{f} = \sum_t t\sigma_t$ with σ_t in $\mathbb{Z}H$ goes under Φ to $\sum t \Phi(\sigma_t)$, and $\Phi|_{\mathbb{Z}H}$ is the augmentation map. So $\bar{f}^G = 0 \Leftrightarrow \text{all } \sigma_t^G = 0$, ie, all $\sigma_t \in \bar{f}$. Hence $\text{Ker } \Phi \subseteq \bar{f}$. This proves (ii).

Proof of (ii) (informal): $\bar{f} \trianglelefteq \mathbb{Z}G$, so $g_F \bar{f} \subseteq \bar{f}$. $g_F \bar{f}x = g_F x \bar{f} = g_F \bar{f}$ ($x \in G$). $[(h-1)x = x(h^x-1)]$. $\bar{f}/g_F \bar{f}$ — quotient of 2 ideals of $\mathbb{Z}G$.

\bar{L} is \mathbb{Z} -generated by all $x(h-1)$, $h \in H$, $x \in G$, ie $(x-1)(h-1) + (h-1) \in \text{gen } \bar{L} + (h-1)$.
 Have $\text{gen } \bar{L} + \mathbb{Z} / \text{gen } \bar{L}$. $[\text{gen } \bar{L} + (h-1)]x = \text{gen } \bar{L} + x(h^x - 1) = \text{gen } \bar{L} + (h^x - 1)$.

(Formal): \bar{L} is free \mathbb{Z} on $(h-1)$, $1 \neq h \in H$. \bar{L} is free \mathbb{Z} on generators $t(h-1)$, $t \in T$, $1 \neq h \in H$. Define a map $\psi: \bar{L} \rightarrow H/H'$ by $t(h-1) \mapsto H'h$ and extend by additivity. Notice $\text{gen } \bar{L}$ is generated by $(x-1)(h-1)$, ie, by $(t-1)(h-1)$ and $(h_i - 1)(h-1)$, $t \in T$, $h_i \in H$.

$$(t-1)(h-1) = t(h-1) - (h-1) = H'h \cdot H'h^{-1} = H'.$$

$$(h_i - 1)(h-1) = (h_i h - 1) - (h-1) - (h_i - 1) = H'h_i h \cdot H'h_i^{-1} \cdot H'h_i^{-1} = H'.$$

We get a map $\psi: \bar{L}/\text{gen } \bar{L} \rightarrow H/H'$

This has an inverse induced by $\text{gen } \bar{L} + (h-1) \longleftrightarrow h$.

$$\begin{aligned} \text{It is a } G\text{-map: } h^g &\mapsto \text{gen } \bar{L} + (h^g - 1) = \text{gen } \bar{L} + g^{-1}(h-1)g = \text{gen } \bar{L} + (h-1)g \\ &= (\text{gen } \bar{L} + (h-1))g \end{aligned}$$

(6.2): If F is a free group with basis X , then the augmentation $\tilde{\epsilon}$ is a free $\mathbb{Z}F$ -module on the $(x-1)$, $x \in X$.

(6.3): Suppose $1 \rightarrow R \rightarrow F \xrightarrow{\pi} G \rightarrow 1$ is a presentation of G with $d(F)$ finite.

Then there is an exact sequence $0 \rightarrow \bar{R} \xrightarrow{i} \mathbb{F}/\mathbb{F}\tilde{\epsilon} \xrightarrow{\tilde{\pi}} G \rightarrow 0$ of $\mathbb{Z}G$ -modules, where $\tilde{\pi}$ is induced by π ($f-1 \mapsto f^{\pi}-1$) and $(Rr)i = \mathbb{F}\tilde{\epsilon}r + (r-1)$.

Moreover, $\mathbb{F}/\mathbb{F}\tilde{\epsilon}$ is a free $\mathbb{Z}G$ -module of rank $d(F)$.

So we get: $0 \rightarrow \bar{R} \rightarrow (\mathbb{Z}G)^{d(F)} \rightarrow \mathbb{F} \rightarrow 0$. (+).

π extends to a map of group rings: $0 \rightarrow \bar{\mathbb{F}} \rightarrow \mathbb{Z}F \xrightarrow{\pi} \mathbb{Z}G \rightarrow 0$, by (6.1)(i).

(6.1) (ii) $\Rightarrow \bar{\mathbb{F}}/\mathbb{F}\tilde{\epsilon} \cong \mathbb{Z}F/\mathbb{F}$, and the map is i .

We get the sequence: $0 \rightarrow \bar{\mathbb{F}}/\mathbb{F}\tilde{\epsilon} \xrightarrow{i} \mathbb{F}/\mathbb{F}\tilde{\epsilon} \rightarrow \mathbb{F} \rightarrow 0$. $\begin{pmatrix} F/R \cong G \\ \mathbb{Z}F/\mathbb{F} \cong \mathbb{Z}G \end{pmatrix}$

(6.2) says that $\mathbb{F} = \bigoplus_{x \in X} (x-1) \mathbb{Z}F$, where X is a basis of F .

$$\begin{aligned} \mathbb{F}\tilde{\epsilon} &= \bigoplus_x (x-1) \bar{\mathbb{F}}, \text{ so } \mathbb{F}/\mathbb{F}\tilde{\epsilon} = \bigoplus \mathbb{Z}F/\bar{\mathbb{F}}, \text{ } |X| \text{ summands.} \\ &= (\mathbb{Z}G)^{d(F)}. \end{aligned}$$

(6.5): Suppose $1 \rightarrow R_1 \rightarrow F_1 \xrightarrow{\pi_1} G \rightarrow 1$, $1 \rightarrow R_2 \rightarrow F_2 \xrightarrow{\pi_2} G \rightarrow 1$ are presentations of G .

$$\text{Then } \bar{R}_1 \oplus (\mathbb{Z}G)^{d(F_2)} \cong \bar{R}_2 \oplus (\mathbb{Z}G)^{d(F_1)}.$$

Proof: We have the relation sequences $0 \rightarrow \bar{R}_1 \rightarrow (\mathbb{Z}G)^{d(F_1)} \rightarrow \mathbb{F} \rightarrow 0$
 $0 \rightarrow \bar{R}_2 \rightarrow (\mathbb{Z}G)^{d(F_2)} \rightarrow \mathbb{F} \rightarrow 0$.

(6.4) (Schanuel's Lemma): Let R be a ring, M an R -module. Suppose

$$\left. \begin{array}{l} 0 \rightarrow U_1 \rightarrow P_1 \xrightarrow{\pi_1} M \rightarrow 0 \\ 0 \rightarrow U_2 \rightarrow P_2 \xrightarrow{\pi_2} M \rightarrow 0 \end{array} \right\} \text{with } P_1, P_2 \text{ projective. Then } U_1 \oplus P_2 \cong U_2 \oplus P_1.$$

Proof: We have $T \xrightarrow{\alpha} P_1$. T is the pull-back $\downarrow \pi_1$ of $P_1 \oplus P_2$, and consists of all (p_1, p_2) with $p_1 \pi_1 = p_2 \pi_2$.

$$P_2 \xrightarrow{\pi_2} M$$

$\text{Ker } \alpha_2 = \text{all } (p_1, 0) \text{ with } p_1 \pi_1 = 0$, ie U_1 . Since P_2 is projective, it splits, so we get $T \cong P_2 \oplus U_1$. By symmetry, we are done. This finishes (6.5) for us.

A projective resolution of M is an exact sequence:

$(0 \rightarrow U \rightarrow P_n \rightarrow \dots \rightarrow P_2 \rightarrow P_1 \rightarrow P_0 \rightarrow M \rightarrow 0)$ (may be infinite, may terminate, on left).

with the P_i 's projective. Schanuel's Lemma extends to a comparison between resolutions $0 \rightarrow U_n \rightarrow P_n \rightarrow \dots \rightarrow P_0 \rightarrow M \rightarrow 0$

$$0 \rightarrow V_m \rightarrow Q_m \rightarrow \dots \rightarrow Q_0 \rightarrow M \rightarrow 0$$

Theorem RI: Hypothesis of (6.5). Then,

- (i) If $d(F_1) = d(F_2)$ then $\bar{R}_1 \vee \bar{R}_2$.
- (ii) If $d(F_1) = d(F_2) > d(G)$, then $\bar{R}_1 \cong \bar{R}_2$.

Proof: (i) comes from Bass' Cancellation Theorem.

(ii) Omitted.

RI (ii) is true, but not every module $V \bar{R}_i$ need be a relation module.

Recall: Module U over R . $\exists 0 = U_0 < U_1 < \dots < U_n = U$ - (1) of submodules with U_i simple.

$$\text{Set } \text{Gr } U = \bigoplus U_{i+1}/U_i$$

(1) is a composition series and $\text{Gr } U$ is independent of its choice.

Suppose $0 = U_0 < U_1 < \dots < U_n = U$ - (2) These have isomorphic refinements. [Schreier's Theorem].

$$0 = V_0 < V_1 < \dots < V_m = U - (3)$$

That is, for every 'gap' $U_i < U_{i+1}$ in (2), insert terms derived from (3):

$$(2'): U_i = U_i + U_{i+1} \cap V_0 \leq U_i + U_{i+1} \cap V_1 \leq \dots \leq U_i + U_{i+1} \cap V_m = U_{i+1}$$

$$(3'): V_j = V_j + V_{j+1} \cap U_0 \leq V_j + V_{j+1} \cap U_1 \leq \dots \leq V_j + V_{j+1} \cap U_n = V_{j+1}, \text{ similarly,}$$

Schreier says (2') and (3') have isomorphic quotients in some order.

Show that $\left\{ U_i + U_{i+1} \cap V_j \leq U_i + U_{i+1} \cap V_{j+1} \right\}$ have isomorphic quotients via a $V_j + V_{j+1} \cap U_i \leq V_j + V_{j+1} \cap U_{i+1}$.

Lemma (Zassenhaus'), which says that if $A \leq B$, $C \leq D$ and quotients are possible, then $\frac{A + (B \cap D)}{A + (B \cap C)} \cong \frac{C + (B \cap D)}{C + (A \cap D)} \cong \frac{B \cap D}{A \cap D + B \cap C}$. [Map $B \cap D$ onto LHS in obvious way, get kernel $(A \cap D) + (B \cap C)$].

Apply this to composition series (1). Then in (2') each term is either U_i or U_{i+1} , ie there is just one jump. The factors of the refinement (2') are precisely those of (1). So $\text{Gr } U$ is well-defined.

Splitting Up Relation Modules into Projective Parts and 'Cores'.

M a $\mathbb{Z}G$ -lattice. Then $M = M' \oplus P$, with P projective and M' has no projective direct summand, is called a 'projective excision'. M' is the corresponding core. A relation core [for G] is an \bar{R} -core, where \bar{R} is a relation module.

Theorem R2: If A and B are relation cores, then $A \vee B$.

Theorem R2*: If $A \vee B$ and B comes from a relation module, then so does A .

Proof: Omitted - hard. See Gruenberg.

(6.6): If M a $\mathbb{Z}G$ -lattice and $0 \rightarrow P \rightarrow M \rightarrow N \rightarrow 0$, and if P is projective and N is a $\mathbb{Z}G$ -lattice, then $M \cong P \oplus N$.

Proof: See questions 4,5 on example sheet 3.

(6.7): M a $\mathbb{Z}G$ -lattice. Then M has no projective summand $\Leftrightarrow M_{(G)}$ has no projective summand. (ie, having no projective summand is a 'genus property').

Proof: If $M = M' \oplus P$ with P projective, then $M_{(G)} = M'_{(G)} \oplus P_{(G)}$ and $P_{(G)}$ is projective. Conversely, suppose $M_{(G)} = P \oplus N$, P projective $\mathbb{Z}_{(G)}G$ -lattice. Now, $M \hookrightarrow M_{(G)}$, so we think of M as $\subseteq M_{(G)}$, and show $M = (M \cap P) \oplus N'$ and $M \cap P$ is projective, via (6.6), with $M \cap P$ replacing P .

$$M/M \cap P \cong (M \cap P)/P \hookrightarrow N. \text{ So } M/M \cap P \text{ is a lattice.}$$

To see $M \cap P$ is projective, we show $(M \cap P)_{(G)} \cong P$. Then use (3.12.2).

Now, we have $0 \rightarrow (M \cap P)_{(G)} \rightarrow P_{(G)} \rightarrow (P/M \cap P)_{(G)} \rightarrow 0$. Consider $P/M \cap P$.

$$\text{This is } \cong \frac{P+M}{M} \subseteq M_{(G)}/M.$$

$$\text{Hence } (M \cap P)_{(G)} \cong P.$$

(6.8): Let π be a finite set of primes containing those that divide $|G|$.

If $M_{(\pi)} \cong U \oplus N$, then $M = L \oplus V$ with $L_\pi \cong U$, $V_\pi \cong N$.

Proof: As in (6.7), and let $L = M \cap U$ and $L_\pi = U$. Consider

$0 \rightarrow M \cap U \rightarrow M \xrightarrow{f} M/M \cap U \rightarrow 0$. We show f splits by proving it does so locally.

If $p \nmid |G|$, then by 3.12, $\mathbb{Z}_{(p)}G$ -lattices are projective, so $f_{(p)}$ is split.

If $p \mid |G|$, then $p \in \pi$. Now the hypothesis says $0 \rightarrow (M \cap U)_\pi \rightarrow M_\pi \xrightarrow{f_\pi} (M/M \cap U)_\pi \rightarrow 0$ splits. Hence $f_{(p)}$ is split for these p as well.

Hence we get $M = M \cap U \oplus V$. But $M_\pi \cong (M \cap U)_\pi \oplus V_\pi \cong U \oplus N$. By Bass, we get $N \cong V_\pi$.

(6.9): Exercise: Let M be a $\mathbb{Z}G$ -lattice and M' a direct summand. Then M' is an M -core $\Leftrightarrow M'_{(G)}$ is a core of $M_{(G)}$.

(6.10): Let M and N be $\mathbb{Z}G$ -lattices with cores M' and N' . Then $M \vee N \Leftrightarrow M' \vee N'$ and $M/M' \vee N/N'$.

Proof: (\Leftarrow) $M = M' \oplus P$ } -①. This is then clear.
 $N = N' \oplus Q$

(\Rightarrow) Suppose (D). Then $M_{(G)} = M'_{(G)} \oplus P_{(G)}$, $N_{(G)} = N'_{(G)} \oplus Q_{(G)}$.

If $M \vee N$, then $M'_{(G)} \oplus P_{(G)} \cong N'_{(G)} \oplus Q_{(G)}$. By Swan 2, $P_{(G)} \cong (\mathbb{Z}_{(G)} G)^r$, $Q_{(G)} \cong (\mathbb{Z}_{(G)} G)^s$, so $M'_{(G)} \oplus (\mathbb{Z}_{(G)} G)^r \cong N'_{(G)} \oplus (\mathbb{Z}_{(G)} G)^s$.

Bass' cancellation says that if, for example, $r < s$, we get

$$M'_{(G)} \cong N'_{(G)} \oplus (\mathbb{Z}_{(G)} G)^{s-r} - \#.$$

Hence $r=s$ and $M'_{(G)} \cong N'_{(G)}$.

Let M be a $\mathbb{Z}G$ -lattice. Then $M_{(G)} = \text{Core} \oplus (\mathbb{Z}_{(G)} G)^r$, r depending only on the genus. r is called the projective rank $\text{pr}(M)$ of M .

G a finite group. Call $1 \rightarrow R \rightarrow F \rightarrow G \rightarrow 1$ a minimal presentation if $d(F) = d(G)$.

Call a corresponding relation module \bar{R} minimal. Define the presentation rank $\text{pr}(G)$ of G to be $\text{pr}(\bar{R})$.

If $G = \langle x_1, \dots, x_n \rangle$, then $\mathfrak{g}_G = (x_1, \dots, x_n) \mathbb{Z}G + \dots + (x_{n-1}) \mathbb{Z}G$. Obviously then, $d_G(\mathfrak{g}_G) = \text{minimum number of generators of } \mathfrak{g}_G \text{ as a } \mathbb{Z}G\text{-module} \leq d(G)$.

Theorem R3: $\text{pr}(G) = d(G) - d_G(\mathfrak{g}_G)$

Proof: Omitted - see Gruenberg.

Theorem R3_(G): $\text{pr}(G) = d(G) - d_G(\mathfrak{g}_{(G)})$

$\mathfrak{g}_{(G)}$ is the augmentation ideal of $\mathbb{Z}_{(G)} G$ and $d_G(\mathfrak{g}_{(G)})$ is the minimum number of generators.

Proof of R3_(G): Let $k = d_G(\mathfrak{g}_{(G)})$. Then there exists a short exact sequence

$0 \rightarrow U \rightarrow (\mathbb{Z}_{(G)} G)^k \rightarrow \mathfrak{g}_{(G)} \rightarrow 0$. -① We show $U \cong A_{(G)}$ where A is a minimal relation core.

U is a $\mathbb{Z}_{(G)} G$ -lattice, so $U \cong A_{(G)}$ for some $\mathbb{Z}G$ -lattice A .

Let $1 \rightarrow R \rightarrow F \rightarrow G \rightarrow 1$ be a minimal presentation. We get the corresponding relation sequence $0 \rightarrow \bar{R} \rightarrow (\mathbb{Z}G)^{d(G)} \rightarrow \mathfrak{g}_G \rightarrow 0$.

Hence, $0 \rightarrow \bar{R}_{(G)} \rightarrow (\mathbb{Z}_{(G)} G)^{d(G)} \rightarrow \mathfrak{g}_{(G)} \rightarrow 0$ -②, by localising.

Use Schanuel on ① and ②.

We get: $U \oplus (\mathbb{Z}_{(G)} G)^{d(G)} \cong \bar{R}_{(G)} \oplus (\mathbb{Z}_{(G)} G)^k$, so $\text{pr} U + d(G) = \text{pr} G + k$.

So, R3_(G) is equivalent to saying $\text{pr} U = 0$.

Suppose, if possible, that $\text{pr} U > 0$. Then $U = U_0 \oplus U_1$, where $U_0 \cong \mathbb{Z}_{(G)} G$.

Quotient by U_0 in ①: $0 \rightarrow U/U_0 \rightarrow (\mathbb{Z}_{(G)} G)^k/U_0 \rightarrow \mathfrak{g}_{(G)} \rightarrow 0$.

We need $T = (\mathbb{Z}_{(G)} G)^k/U_0 \cong (\mathbb{Z}_{(G)} G)^{k-1}$ - this would contradict minimality of k .

But U_0 is free and T is a lattice, so by (6.6) we get $(\mathbb{Z}_{(G)} G)^k \cong U_0 \oplus V$.

Bass again gives $V \cong (\mathbb{Z}_{(G)} G)^{k-1}$.

Theorem R4: (a) If $d(G) = 2$ then $\text{pr}(G) = 0$.

(b) If G is soluble then $\text{pr}(G) = 0$.

(c) Given any n there is a G with $\text{pr}(G) \geq n$.

Showed on example sheet that if $d(G) = 1$ then $\text{pr}(G) = 0$.

Proof of R4(a): Suppose $d(G) = 2$. Take a minimal presentation and corresponding relation sequence $0 \rightarrow \bar{R} \rightarrow (\mathbb{Z}G)^2 \rightarrow Q \rightarrow 0$. Let $R = A \oplus P$ with A a core, P projective. Move to $\mathbb{Q}G$ by localising: $0 \rightarrow \bar{R}\mathbb{Q} \rightarrow (\mathbb{Q}G)^2 \rightarrow Q\mathbb{Q} \rightarrow 0$ and hence $(\mathbb{Q}G)^2 \cong \bar{R}\mathbb{Q} \oplus Q\mathbb{Q}$. But $\mathbb{Q}G \cong Q\mathbb{Q} \oplus Q\mathbb{Q}$ trivial module. Hence $\mathbb{Q}G \oplus Q \cong A\mathbb{Q} \oplus P\mathbb{Q}$, and $P\mathbb{Q} = (\mathbb{Q}G)^{\text{pr}(G)}$. Hence $\text{pr}(G) \leq 1$.

Suppose that $\text{pr}(G) = 1$. Then $Q \cong A\mathbb{Q}$, so A is trivial.

From $R^3(G)$, $\text{pr}(G) = 1 = 2 - d_G(Q_{(G)})$, so $d_G(Q_{(G)}) = 1$.

So we have: $0 \rightarrow U \rightarrow \mathbb{Z}_{(G)}G \rightarrow Q_{(G)} \rightarrow 0$.

In the proof of $R^3(G)$, we proved that $U \cong A_{(G)}$, A a minimal relation core. So sequence is $0 \rightarrow \mathbb{Z}_{(G)} \xrightarrow{\text{trivial module}} \mathbb{Z}_{(G)}G \xrightarrow{\text{multiplication by } \frac{G}{G}} \mathbb{Q}_{(G)} \xrightarrow{\text{trivial submodule here is } (\frac{G}{G})\mathbb{Z}_{(G)}G} 0$ - (1)

Tensor (1) with the trivial module $\mathbb{Z}_{(G)}G / Q_{(G)}$. We get:

$$\mathbb{Z}_{(G)} \xrightarrow{G} \mathbb{Z}_{(G)} \xrightarrow{Q_{(G)}} \mathbb{Q}_{(G)}^2 \rightarrow 0.$$

this is $(\mathbb{Q}/Q^2)_{(G)}$ and is $\cong G/G'$.

We have $\mathbb{Z}_{(G)} \xrightarrow{G} \mathbb{Z}_{(G)} \xrightarrow{G/G'} G/G' \rightarrow 0$

So $G/G' \cong \mathbb{Z}_{(G)}/G_{(G)}\mathbb{Z}_{(G)} \cong \mathbb{Z}/G_{(G)}\mathbb{Z}$, and $G' = 1$ and G is cyclic, contradicting $d(G) = 2$. Hence $\text{pr}(G) = 0$.

Proof of (b): We find conditions for $\text{pr}(G) \geq n$. Recall: \bar{R} minimal presentation module,

$$\bar{R} = A \oplus P. \text{ Have } \bar{R}_{(G)} = A_{(G)} \oplus (\mathbb{Z}_{(G)}G)^{\text{pr}(G)}$$

projective.

(7.1): Let π be a finite set of primes. Let P, M be $\mathbb{Z}_\pi G$ -lattices. Then P is a direct summand of M iff P/P_p is a direct summand of M/M_p for all p in π .

Proof: Exercise. Refer to the proof of (4.2) and fill in the details of the following sketch: For each p_i in π , $P \xrightarrow{f_i} M$

nat. ↓ ↓ nat.

$$P/P_{p_i} \xrightarrow{g_i} M/M_{p_i}, \text{ embedding as a direct summand.}$$

$P \triangleleft \mathbb{Z}_\pi \Rightarrow \mathfrak{P} = (p), p \in \pi$. Use Chinese Remainder Theorem as in (4.2) to show that $\exists f \equiv f_i \pmod{\text{Hom}(P, M) \mathfrak{P}_i}$, $\mathfrak{P}_i = (p_i)$, and so we can assume all the f_i 's are the same, say f .

To show f is injective, localise at each p in π and show $f_{(p)}$ is injective.

Show, from the diagram $P_{(p)} \xrightarrow{f_{(p)}} M_{(p)}$ that $\text{Ker } f_{(p)} \cap P_{(p)} = \text{Ker } f_{(p)} P$, as

nat. ↓ ↓ nat. $\text{Ker } f_{(p)} \subseteq P_{(p)} P$, to get

$$P/P_p \rightarrow M/M_p \quad \text{Ker } f_{(p)} = \text{Ker } f_{(p)} P \Rightarrow \text{Ker } f_{(p)} = 0.$$

To show Pf is a direct summand, use (6.6). Show that M/Pf is projective over \mathbb{Z}_π . It is enough to show that M/Pf is torsion-free over \mathbb{Z}_π (via diagram).

(7.2): $(\mathbb{Z}_{(G)}G)^n$ is a direct summand of $\bar{R}_{(G)}$ iff for all $p \nmid |G|$, we have $(\mathbb{Z}/p\mathbb{Z}G)^n$ a direct summand of \bar{R}/\bar{R}_p .

Concentrate on a particular p .

Notation: $k = \mathbb{Z}/p\mathbb{Z}$, $J = \text{Jac}(kG)$, $kG/J = \bigoplus_{M, \text{ind}} M^{\oplus s_M}$. Want P_M to be the principal indecomposable projective with $P/PJ \cong M$.

Let $U = P_k$, k the trivial module. We have $UJ \rightarrow U \rightarrow k \rightarrow 0$. Consider $UJ/UJ^2 = \bigoplus_{M, \text{ind}} M^{\oplus s_M}$.

Let $V = \bigoplus_M P_M^{s_M}$. $V/VJ \cong \bigoplus (P_M/P_M J)^{s_M} = UJ/UJ^2$. By the previous argument we get $V \rightarrow UJ$.

Let $A = \ker(V \rightarrow UJ)$. Then we have: $0 \rightarrow A \rightarrow V \rightarrow U \rightarrow k \rightarrow 0$, and $A \leq VJ$.

(7.4) (Gaschütz): With $I \rightarrow R \rightarrow F \rightarrow G \rightarrow I$ a presentation, we have

$$A \oplus U \oplus (kG)^{d(F)} \cong \bar{R}/\bar{R}_p \oplus V \oplus kG.$$

Proof: Have $\begin{cases} (1) - 0 \rightarrow UJ \rightarrow U \rightarrow k \rightarrow 0 \\ (2) - 0 \rightarrow g_k \rightarrow kG \rightarrow k \rightarrow 0 \end{cases} \quad \left. \begin{array}{l} \text{Schanuel's lemma} \\ \Rightarrow UJ \oplus kG \cong g_k \oplus U \end{array} \right.$

Consider LHS. Have: $0 \rightarrow A \rightarrow V \rightarrow UJ \rightarrow 0$

$$\text{So: } 0 \rightarrow A \rightarrow V \oplus kG \rightarrow UJ \oplus kG \rightarrow 0. \quad - (*)$$

Consider RHS. Start with the relation sequence:

$$0 \rightarrow \bar{R} \rightarrow (\mathbb{Z}G)^{d(F)} \rightarrow g_k \rightarrow 0.$$

Tensor this with $k = \mathbb{Z}/p\mathbb{Z}$. Exactness is preserved because all terms are free \mathbb{Z} -modules.

$$\text{Get: } 0 \rightarrow \bar{R}/\bar{R}_p \rightarrow (kG)^{d(F)} \rightarrow g_k \rightarrow 0$$

$$\text{So: } 0 \rightarrow \bar{R}/\bar{R}_p \rightarrow (kG)^{d(F)} \oplus U \rightarrow g_k \oplus U \rightarrow 0 \quad - (*)$$

Schanuel on the $(*)$'s gives: $A \oplus U \oplus (kG)^{d(F)} \cong \bar{R}/\bar{R}_p \oplus V \oplus kG$.

(7.5): (i) A is non-zero.

(ii) A has no projective summands.

(iii) A is a core of \bar{R}/\bar{R}_p .

Proof: (i) Suppose A is zero. Then $V \cong UJ$ and UJ would be projective. By (6.6) with $S = k$, we get $U = UJ \oplus U_0$ ($U_0 \cong k$). By Nakayama, get $U = U_0$, ie k is projective. But this is not so, since $p \nmid |G|$.

(ii) Suppose $A = B \oplus Q$, with Q projective. Have $B \oplus Q = A \leq VJ \leq V$. We show $V = Q \oplus W$, say. For then $V = VJ \oplus W$, and Nakayama will give $V = W$ and $Q = 0$.

(6.6) applies again, to give V split over Q .

(iii) Write the modules in Gaschütz's Theorem as a direct sum of indecomposables and use Krull-Schmidt.

Take \bar{R} to be a minimal relation module, so $d(F) = d(G)$. Write $\bar{R}/\bar{R}_p = A \oplus P$, P projective. We get $U \oplus (kG)^{d(G)-1} \cong P \oplus V$. Now, $P = \bigoplus P_M^{?_M}$, $P/PJ = \bigoplus M^{?_M}$. Hence $U/UJ \oplus (kG/J)^{d(G)-1} \cong P/PJ \oplus V/VJ$.

$$\text{So: } k \oplus (kG/J)^{d(G)-1} \cong P/PJ \oplus UJ/UJ^2$$

$$\text{Define } \tau_M = \begin{cases} 1 & \text{if } M = k \\ 0 & \text{otherwise.} \end{cases}$$

$$\text{Get } \tau_M + \tau_M(d(G)-1) = ?_M + s_M. \quad (1 \geq n \geq \tau_M)$$

So we get (7.6):

(7.6): $\text{pr}(G) \geq n \Leftrightarrow$ "in all modular situations", $t_M + r_M(d(G)-1) - s_M \geq nr_M$

Hence $UJ \oplus kG \cong U \oplus \mathfrak{g}_k^r$, so $U/UJ \oplus kG/J \cong R \oplus \mathfrak{g}_k^r / \mathfrak{g}_k^r J$.

So, # times M occurs: $s_M + r_M = t_M + \alpha_M$.

So we get:

(7.7): $\text{pr}(G) \geq n \Leftrightarrow$ "in all modular situations", $r_M d(G) - n \geq \alpha_M$.

Any simple $\mathbb{Z}G$ -module is annihilated by some prime and is therefore like M above. Let $\Delta = \text{Hom}_{kG}(M, M)$. Then $\text{Hom}_{kG}(kG, M) \cong M$, but is $\cong \text{Hom}_{kG}(kG/J, M) = \Delta^{r_M}$. So $|M| = |\Delta|^{r_M}$. Also, $|\text{Hom}_{kG}(\mathfrak{g}_k^r, M)| = |\Delta|^{\alpha_M}$. From (7.7) we get $|\Delta|^{r_M d(G) - n} \geq |\Delta|^{\alpha_M}$. So we get:

(7.8) $\text{pr}(G) \geq n \Leftrightarrow |M|^{d(G) - n} \geq |\text{Hom}(\mathfrak{g}_k^r, M)|, \forall \text{ simple modules } M$.

R4(b): Let G be soluble. We show by induction on $|G|$ then $\text{pr}(G) = 0$.

Let A be a minimal normal subgroup of G . Let $H = G/A$. Suppose $\text{pr}(H) = 0$.

$A' \triangleleft A$ and A' is characteristic, so $A' \triangleleft G$. Hence $A' = 1$. Hence A is a $\mathbb{Z}G$ -module, by conjugation. So A is abelian.

By (7.8), as $\text{pr}(H) \geq 1$, \exists a simple $\mathbb{Z}H$ -module M for which $|\text{Hom}(\mathfrak{g}_k^r, M)| \geq |\text{Hom}(L, M)| > |M|^{d(H)-1}$ ($\mathfrak{g}_k^r \rightarrow L$)

If $d(G) = d(H)$ then (7.8) would give $\text{pr}(G) \geq 1$.

So we assume $d(G) > d(H)$.

(7.9): We now must have

(i) $d(G) = 1 + d(H)$.

(ii) $G \cong H \Delta A$

(iii) number of complements to A in G is $|A|^{d(H)}$

Recall that in $H \Delta A$ the number of complements to A in G is $|\text{Der}(H, A)| = |\text{Hom}(L, A)|$.

Proof of (7.9): (ii) Let $G/A = \langle Ax_1, \dots, Ax_n \rangle$. Let $1 \neq a \in A$. Then $A = a\mathbb{Z}H$, by simplicity, $= a.\mathbb{Z}\langle x_1, \dots, x_n \rangle$. Hence $G = \langle a, x_1, \dots, x_n \rangle$. So $d(G) \leq 1 + d(H)$, hence $d(G) = 1 + d(H)$. (iii) Let $X = \langle x_1, \dots, x_n \rangle$. Then $G = A.X$. But $A \cap X \trianglelefteq X$, and $A \cap X \trianglelefteq A$ (since $A' = 1$). Hence $A \cap X \trianglelefteq G$. If $A \cap X = A$, then $A \subseteq X$, and $G = X - \#$ to (i).

So $A \cap X = 1$.

(iii) We show $(a_1, \dots, a_n) \mapsto \langle a_1 x_1, \dots, a_n x_n \rangle$ from $\overbrace{A \times \dots \times A}^{n-1}$ to complements of H in G is bijective.

If $\langle a_1 x_1, \dots, a_n x_n \rangle = \langle a'_1 x_1, \dots, a'_n x_n \rangle = T$, then T contains the element $x_2^{-1} a_2^{-1} a'_2 x_2$, of A . Hence $a_2^{-1} a'_2 = 1$. So the map is 1-1.

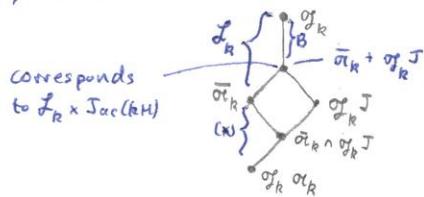
If $G = AT$ then $x_i = a_i t_i$, $a_i \in A$, $t_i \in T$. So $t_i = a_i^{-1} x_i$. So $T = \langle a_1^{-1} x_1, \dots, a_n^{-1} x_n \rangle$. \therefore onto.

We use (7.9) together with:

$$(7.10): |\text{Hom}(\mathcal{G}, A)| > |\text{Hom}(F, A)|.$$

These give: $|A|^{d(G)-1} < |\text{Hom}(\mathcal{G}, A)|$. Then (7.8) tells us $\text{pr}(G) \neq 1$.

Proof of (7.10): Let $p|G|$, $k = \mathbb{Z}/p\mathbb{Z}$. Consider kG . Let $J = \text{Jac}(kG)$. We need $\sigma_k \leq J$. If M is any simple kG -module, $|M| = p^r$, $|A| = p^s$, and we must have a fixed point of A in M . But the fixed points of A are a kG -submodule. Hence $\mu = \mu_A$, so $M\mu = 0$.



$$\begin{aligned} \text{Hom}(\mathcal{G}_k, A) &= \text{Hom}(\sigma_k / \sigma_k J, A) \\ kG / \sigma_k &\cong kH. \end{aligned}$$

$$(*) : \sigma_k / \sigma_k \sigma_k \cong A$$

$$\bar{\sigma} / \sigma \bar{\sigma} \cong A, \text{ qua } \mathbb{Z}G\text{-module.}$$

Since A is simple, either (i) $\bar{\sigma}_k = \bar{\sigma}_k \cap \sigma_k J$
or (ii) $\sigma \bar{\sigma}_k = \bar{\sigma}_k \cap \sigma_k J$.

If (i), then $\mathcal{G}_k / \sigma_k J \cong B \oplus A$.

$$\text{Hom}(\mathcal{G}, A) = \text{Hom}(F, A) \oplus \text{Hom}(A, A). \text{ Hence (7.10).}$$

Suppose (ii) were possible, then $\bar{\sigma}_k \leq \sigma_k J$.

$$\text{Now, } G = HDA, \text{ so } \mathcal{G} = F \oplus \bar{\sigma}. \text{ Hence } \sigma_k = \bar{f}_k \oplus \bar{\sigma}_k. \quad (**)$$

If $\bar{\sigma}_k \leq \sigma_k J$, we get $\sigma_k = \bar{f}_k + \sigma_k J$. Nakayama gives $\mathcal{G}_k = \bar{f}_k$.
[$X \in G$, then $X \mapsto \sigma \in \text{Jac}(kG)$ is (1-1). Get $G = H$]

$$\text{So } \bar{f}_k = \bar{f}_k kG = \bar{f}_k + \bar{f}_k \sigma_k = \bar{f}_k \oplus \underbrace{\bar{f}_k \bar{\sigma}_k}_{< \bar{f}_k + \bar{\sigma}_k = \sigma_k} < \bar{f}_k + \bar{\sigma}_k = \sigma_k. \quad \text{**}$$

$\leftarrow \bar{\sigma}_k$, by (**).

Theorem R4(c).

Theorem R5: Let $G^r = G \times \dots \times G$. $\lim_{r \rightarrow \infty} \text{pr}(G^r) = \begin{cases} \infty & \text{if } G = G' \\ 0 & \text{if } G > G'. \end{cases}$

$$(7.11): \lim_{r \rightarrow \infty} d(G^r) = \infty \text{ if } G > 1.$$

$$\text{Example: } d(A_5^{19}) = 2, \quad d(A_5^{20}) = 3.$$

(7.12) [Wiegold]: If $G > G'$ then $\exists k$ with $d(G^r) = r d[G/G']$, all $r \geq k$.

Proof: See Journal of the Australian Maths Society 20 (1975), pp. 225-9.

Proof of (7.11): Have $d(G^r) \leq d(G^{r+1}) \leq \dots$. Suppose $n = \lim d(G^r)$. Let F be free, $d(F) = n$. $|\text{Hom}(F, G)| \leq |G|^n$. Let $K = \Lambda$ kernels of homomorphisms from F to G . get $|F/K| = |G|^{|G|} = N$, say. Let $r > N$ and consider G^r .
 $F \xrightarrow{\pi} G^r \xrightarrow{\pi_i} G$, π_i = projection onto i th factor. Then $K\pi = 1$, and $|G^r| \leq |F/K|$.

Recall $\text{pr}(G^r) \geq n \Leftrightarrow \tau_M + r_M (\overbrace{d(G^r) - 1}^{\rightarrow \infty}) - s_M \geq n \cdot r_M$.

If $s_M = 0$, we are fine. Consider $s_M \neq 0$. [For notation, just write G for G^r]

Case $G = G'$: $\text{Hom}(\alpha_f, \mathbb{Z}/p\mathbb{Z}) = \text{Hom}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) = 0$, as $\mathbb{Z}/p\mathbb{Z} \cong G/G'$.

Recall $U \oplus \mathbb{Z} \cong UJ \oplus kG$, so $U/UJ \oplus \mathbb{Z}/p\mathbb{Z} \cong \frac{UJ}{UJ^2} \oplus \frac{kG}{J}$
 Count k 's: $\begin{matrix} \uparrow & \uparrow & \vdots & \uparrow \\ 1 & 0 & \dots & 0 \end{matrix}$

Examine the $s_M \neq 0$. One proves that if $D(G) = \frac{UJ}{UJ^2}$ coming from kG , $k = \mathbb{Z}/p\mathbb{Z}$.
 $= \bigoplus M^{s_M}$

(7.13): $D(G_1 \times G_2) \cong D(G_1) \oplus D(G_2)$, where G_2 acts trivially on $D(G_1)$, and G_1 acts trivially on $D(G_2)$.

Proof: Omitted.

So $D(G^r) = D(G) \oplus \dots \oplus D(G)$ (r copies), where all but the i th factor of G^r acts trivially on the i th summand.

If M is a simple G -module, write $M_{(i)} =$ the G^r -module with M in the i th summand and zeroes elsewhere.

If $D(G) = \bigoplus M^{t_M}$ then $D(G^r) = \bigoplus_{i=1}^r M_{(i)}^{t_M}$.

Hence the s_M are bounded.

Case $G > G'$: Choose p so that $d(G/G') = d(G'/G'G')$, (via Basis Theorem).
 Then you work out $|\text{Hom}(\alpha_f, \mathbb{Z}/p\mathbb{Z})|$ and use (7.8).