NON-COMMUTATIVE ALGEBRA
2015–2016

E. Jespers

Departement of Mathematics
Vrije Universiteit Brussel

Contents

Chapter 1

Groups and Rings

The basic theory of groups and rings has been dealt with in previous courses. In the first section we recall some definitions.

1.1 Basic Concepts

Definition 1.1.1. *A semigroup is a set with an associative binary operation. Sometimes this object is denoted $(S, *)$, or simply S, where S is the set and $*$ is the operation. An element θ of S is calles a zero element if $s\theta = \theta s = \theta$ for all $s \in S$.*

Definition 1.1.2. *A monoid is a semigroup S which has a unit element 1, i.e. $1s = s1 = s$ for each $s \in S$. This object is sometimes denoted $(S, *, 1)$.*

Definition 1.1.3. *A group G is a monoid in which every element is invertible. An element $g \in G$ is said to be invertible in G if there exists $g' \in G$ such that $gg' = g'g = 1$. The element g' is called the inverse of g and is denoted g^{-1}. The group G is said to be abelian, or commutative, if $gh = hg$ for all $g, h \in G$.*

Mostly we will use the multiplicative notation for groups. However, for abelian groups we will use the additive notation, with $+$ for the group operation, 0 for the unit element, and $-g$ for the inverse of g.

An element g of a group G is *torsion* (or periodic) if $g^n = 1$ for some positive integer. The group is said to be *torsion-free* if the identity element is the only torsion element.

Definition 1.1.4. *A subgroup N of a group G is normal if $gNg^{-1} = N$ for all $g \in G$. The quotient group of G by N is denoted G/N.*

Now we recall some definitions of sets with two operations.

Definition 1.1.5. *A ring is a set R together with two operations, the addition $+$ and the multiplication $.$, and two distinguished elements 0 and 1, such that the following conditions are satisfied:*

1. $(R, +, 0)$ *is an abelian group,*
2. $(R, ., 1)$ *is a monoid,*
3. *the distributive laws:* $a(b + c) = ab + ac$ *and* $(b + c)a = ba + ca$ *for all* $a, b, c \in R$.

If, moreover, $ab = ba$ *for all* $a, b \in R$*, then* R *is said to be commutative (or abelian).*

Sometimes we also will consider rings without a multiplicative identity.

The *trivial ring* is the singleton $\{0\}$. In this ring $1 = 0$. In all other rings the latter does not happen. A *subring* of a ring is a subset which is itself a ring under the induced multiplication and addition and with the same distinguished elements 1 and 0 (although sometimes one does not demand that the subring has the same 1).

A *domain* is a ring in which each product of nonzero elements is nonzero. A ring R is called a *division ring*, or *skew field*, if $(R \setminus \{0\}, ., 1)$ is a group. A commutative domain is called an *integral domain*; a commutative division ring is called a *field*.

A function $f : R \to S$ from a ring R to a ring S is said to be a *ring homomorphism* if f is a homomorphism of the abelian groups $(R, +)$ and $(S, +)$, and the monoids $(R, .)$ and $(S, .)$.

1.2 Ring constructions

We first give several natural ring constructions.

Example 1.2.1.

1. The ring of integers $\mathbb{Z}$, the fields of rational numbers $\mathbb{Q}$, real numbers $\mathbf{R}$, complex numbers $\mathbf{C}$.
2. **Matrix Rings**.
   Let R be a ring, n a positive integer. The ring of $n \times n$ matrices over the ring R, denoted $M_n(R)$, is the complete set of of all $n \times n$ arrays or matrices
   $$M = \begin{bmatrix} r_{11} & r_{12} & \dots & r_{1n} \\ r_{21} & r_{22} & \dots & r_{2n} \\ \dots & \dots & \dots & \dots \\ r_{n1} & r_{n2} & \dots & r_{nn} \end{bmatrix},$$
   or simply denoted as $M = (r_{ij})$. Addition and multiplication are given according to the rules:
   $$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}) \text{ and}$$
   $$(a_{ij})(b_{ij}) = (c_{ij}) \text{ where } c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}.$$
   Note for $n > 1$, $M_n(R)$ always is non-commutative.

3. **Upper Triangular Matrices**.
The ring of all matrices $(r_{ij}) \in M_n(R)$ *with* $r_{ij} = 0$ *for* $i > j$.

4. **Polynomial Rings**.
Let R be a ring. The polynomial ring (in one variable X) over R is the set of all formal sums

$$f(X) = r_0 + r_1X + \dots r_nX^n$$

where each $r_i \in R$. If $r_n \neq 0$, then n is called the degree of the polynomial $f(X)$, denoted $\deg(f(X))$, and r_n is called the leading coefficient of $f(X)$. The degree of the zero polynomial is by definition $-\infty$. Addition and multiplication are given according to the rules:

$$\sum_{i=1}^{n} a_iX^i + \sum_{i=1}^{n} b_iX^i = \sum_{i=1}^{n}(a_i + b_i)X^i \text{ and}$$

$$(\sum_{i=1}^{n} a_iX^i)(\sum_{j=1}^{m} b_jX^j) = \sum_{k=1}^{n+m}(\sum_{i+j=k}(a_ib_j))X^k$$

(in the latter we agree that $a_i = 0$ if $i > n$, and $b_j = 0$ if $j > m$). More generally, the polynomial ring in the variables $X_1, \dots, X_n$ is defined inductively by the rule

$$R[X_1, \dots, X_n] = (R[X_1, \dots, X_{n-1}])[X_n].$$

It follows from the definition that every element (called a polynomial) is of the form

$$f = \sum r_{i_1 \dots i_n} X_1^{i_1} \dots X_n^{i_n},$$

where the $r_{i_1 \dots i_n} \in R$ are uniquely determined as the coefficient of $X_1^{i_1} \dots X_n^{i_n}$. Note that formally the above is an infinite sum, but in fact only finitely many of the coefficients r_i are nonzero. Note also that the X_i's commute among each other and also with the coefficients.

An element of the form $m_i = X_1^{i_1} \dots X_n^{i_n}$ is called a *monomial*, and its total degree (or simply degree), denoted $\deg(m_i)$, is the sum $\sum_{k=1}^{n} i_k$.

5. **Monoid and Group Rings**.
Let R be a ring and S a monoid with identity e. The monoid ring $R[S]$ of S over R is the set of all formal finite sums

$$f = \sum_{s \in S} r_s s,$$

(so only finitely many r_s are non-zero) where each $r_s \in R$, $s \in S$. The set $\{s \in S \mid r_s \neq 0\}$ is called the support of f, and is denoted

$\mathrm{supp}(f)$. Note that, by definition, this set is always finite. Addition and multiplication are defined as follows:

$$\sum_{s\in S} a_s s + \sum_{s\in S} b_s s = \sum_{s\in S} (a_s + b_s)s$$

and

$$(\sum_{s\in S} a_s s)(\sum_{t\in S} b_t t) = \sum_{u\in S} (\sum_{st=u} a_s b_t)u,$$

where the inner sum is evaluated over all $s, t \in S$ in the respective supports such that $st = u$. The elements of $s \in S$ are identified with $1s$; and the elements $r \in R$ are identified with re. Clearly $e = 1e$ is the identity of the ring $R[S]$.

In case S is a group, then $R[S]$ is called a group ring. In case S is the free abelian monoid with free basis $X_1, \cdots, X_n$ then $R[S] = R[X_1, \cdots, X_n]$. If S is the free monoid in $X_1, \cdots, X_n$ then $R[S]$ is the polynomial ring in noncommuting variables.

6. **Contracted Semigroup Rings**.
Let S be a semigroup with zero θ. The *contracted semigroup ring* of S over a ring R is the ring $R[S]/R\theta$. This ring is denoted

$$R_0[S].$$

Thus the elements of $R_0[S]$ may be identified with the set of finite sums $\sum r_s s$ with each $r_s \in R$, $s \in S \setminus \{\theta\}$, subject to the componentwise addition and multiplication defined on the R-basis $S \setminus \{\theta\}$ as follows

$$s \circ t = \begin{cases} st & \text{if } st \neq \theta \\ 0 & \text{if } st = \theta \end{cases}$$

and then extended by distributivity to all elements.

If S does not have a zero element, then we put $R_0[S] = R[S]$.

Some important natural classes of rings may be treated as contracted semigroup rings and not as semigroup rings. For example, let $n > 1$ be an integer, and let S be the semigroup of $n \times n$ matrix units, that is,

$$S = \{e_{ij} \mid 1 \leq i, j \leq n\} \cup \{\theta\}$$

subject to the multiplication

$$e_{ij}e_{kl} = \begin{cases} e_{il} & \text{if } j = k \\ \theta & \text{if } j \neq k \end{cases}$$

Then, for any ring R,

$$R_0[S] \cong M_n(R),$$

a natural isomorphism. Now, if K is a field then $M_n(K)$ is a simple ring. But a semigroup algebra of a nontrivial semigroup is never simple as it contains the augmentation ideal, that is the ideal of all elements of the semigroup algebra of which the sum of the coefficients is zero.

This example can be extended as follows. Let R be a K-algebra. Let I, M be nonempty sets and $P = (p_{mi})_{m\in M, i\in I}$ a generalized $M \times I$ matrix with $p_{mi} \in R$. Consider the set $\mathcal{M}(R, I, M, P)$ of all generalized $I \times M$ matrices over R with finitely many nonzero entries. For any $A = (a_{im}), B = (b_{im}) \in \mathcal{M}(R, I, M, P)$, addition and multiplication are defined as follows:

$$\begin{aligned} A + B &= (c_{im}) \text{ with } c_{im} = a_{im} + b_{im}, \\ AB &= A \circ P \circ B \text{ where } \circ \text{ is the matrix multiplication} \\ kA &= (ka_{im}) \end{aligned}$$

With these operations $\mathcal{M}(R, I, M, P)$ becomes a ring, called a ring of matrix type. If each row and column of P contains an invertible element of R then we call $\mathcal{M}(R, I, M, P)$ a **Munn algebra**.

Later we will see the notion of matrix semigroup $\mathcal{M}^0(G^0, I, M, P)$ where G is a group, and P is a matrix with entries in G^0. It is then easily verified that

$$R_0[\mathcal{M}^0(G^0, I, M, P)] \cong \mathcal{M}(R, I, M, P).$$

Denote by $M_I^{row}(R)$ the ring of all $I \times I$ matrices over R with finitely many nonzero rows, subject to the natural addition and multiplication. The following is easily verified. The mapping

$$\mathcal{M}(R, I, M, P) \to M_I^{row}(R) : A \mapsto A \circ P$$

is ring homomorphism.

Another useful class of contracted semigroup algebras are the monomial algebras $K[X]/I$, where X is the free monoid on an alphabet $\{x_i \mid i \in \Omega\}$ and I is an ideal generated by an ideal J of X. So, $K[X]/I$ is a K-space with basis the Rees factor semigroup X/J (the terminology will be explained later); thus $K[X]/I \cong K_0[X/J]$.

7. **Skew Polynomial Rings**.
The notion of polynomial ring over a ring R in one variable X can be extended in such a way that the variable does not necessarily commute with the elements of R.

Let R be a ring and σ a ring homomorphism from R to R. The skew polynomial ring $R[X, \sigma]$ is, as in the case of polynomial rings, the set

of all formal sums

$$f = \sum_{i=0}^{n} r_i X^i,$$

where each $r_i \in R$. Again, if $r_n \neq 0$, then a_n is called the leading coefficient of f and the degree of f, denoted $\deg(f)$, is n. Addition and multiplication are defined by the following rules:

$$\sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{n} b_i X^i = \sum_{i=0}^{n} (a_i + b_i) X^i$$

and

$$(\sum_{i=0}^{n} a_i X^i)(\sum_{j=0}^{m} b_j X^j) = \sum_{k=0}^{n+m} (\sum_{i+j=k} a_i \sigma^i(b_j)) X^k.$$

In particular, $Xa = \sigma(a)X$.

8. **Laurent Polynomial Rings**.
Let σ be an automorphism of a ring R. Then the skew Laurent polynomial ring is

$$R[X, X^{-1}, \sigma] = \{\sum_{i=l}^{k} r_i X^i \mid l \leq k,\ l, k \in \mathbb{Z},\ r_i \in R\}.$$

The addition and multiplication is defined as in the skew polynomial ring case. Note that $R[X, X^{-1}, \sigma]$ is obtained from $R[X, \sigma]$ by "inverting" all positive powers of X.

9. **Power Series Rings**.
Let R be a ring. The ring of (formal) power series over R is the set of all sequences $f = (r_0, r_1, \dots)$, usually denoted as

$$f = \sum_{i=0}^{\infty} r_i X^i,$$

where each $r_i \in R$. Addition and multiplication are defined as follows:

$$\sum_{i=0}^{\infty} a_i X^i + \sum_{i=0}^{\infty} b_i X^i = \sum_{i=0}^{\infty} (a_i + b_i) X^i \text{ and}$$

$$(\sum_{i=0}^{\infty} a_i X^i)(\sum_{j=0}^{\infty} b_j X^j) = \sum_{k=0}^{\infty} (\sum_{i+j=k} (a_i b_j)) X^k.$$

10. **Group Graded Rings**.
Several of the above mentioned examples are actually of the following type. Let R be a ring and G a group. The ring R is said to be G-graded (or simply graded when G is clear from the context) if there exists a family of abelian subgroups of $(R, +, 0)$

$$\{R_g \mid g \in G\}$$

such that the following conditions hold:

$$R = \oplus_{g\in G} R_g \quad \text{direct sum of abelian groups}$$

and

$$R_g R_h \subseteq R_{gh}$$

for all $g, h \in G$.

11. **Crossed Products and Strongly Graded Rings.**
Let R be a ring with 1 and let G be a group. Then a crossed product $R * G$ of G over R is an associative ring which contains R and has as R-basis a set $\overline{G} = \{\bar{g} \mid g \in G\}$ that is a copy of G. Thus each element of $R * G$ can be written uniquely in the form

$$\sum_{g\in G} r_g \overline{g},$$

with each $r_g \in R$. Addition is componentwise and multiplication is defined by the following two rules:

$$\overline{g}\overline{h} = \tau(g, h)\overline{gh},$$

where $\tau : G \times G \to \mathcal{U}(R)$ (with $\mathcal{U}(R)$ the group of units of R), and

$$\overline{g}r = \sigma_g(r)\overline{g},$$

where $\sigma : G \to \mathrm{Aut}(R) : g \mapsto \sigma_g$. One can easily deduce necessary and sufficient conditions on τ and σ so that the multiplication is associative (and we thus indeed have a ring).

A crossed product is an important example of a strongly graded ring $R = \oplus_{g\in G} R_g$, that is R also satisfies the condition

$$R_g R_h = R_{gh},$$

for all $g, h \in G$.

12. **Real Quaternion Algebra**.
This is the first example of a skew field which is not commutative. This ring was introduced by W.R. Hamilton.

Let $\mathbf{H} = \mathbf{H}(\mathbf{R})$ be the subset of $M_2(\mathbf{C})$ of all matrices of the form

$$x = \begin{bmatrix} a & b \\ -\overline{b} & \overline{a} \end{bmatrix},$$

where $\mathbf{C} \to \mathbf{C} : c \mapsto \overline{c}$ is the conjugation map. One easily verifies that $\mathbf{H}$ is closed under addition and multiplication, and therefore is a ring with the identity matrix as the identity element. Further, using the inverse formula for a 2×2 matrix, it follows that each nonzero matrix in $\mathbf{H}$ is invertible. Hence $\mathbf{H}$ is a division ring. The center of this ring is the field $\mathbf{R}$ of real numbers identified with the set of all diagonal matrices

$$\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$$

$a \in \mathbf{R}$.

$\mathbf{H}$ also contains the elements:

$$\mathbf{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \ \mathbf{i} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \ \mathbf{j} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \ \mathbf{k} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

It follows that

$$x = c_0\mathbf{1} + c_1\mathbf{i} + c_2\mathbf{j} + c_3\mathbf{k}$$

for some unique $c_i \in \mathbf{R}$. The product of any two elements in $\mathbf{H}$

$$(c_0\mathbf{1} + c_1\mathbf{i} + c_2\mathbf{j} + c_3\mathbf{k})(d_0\mathbf{1} + d_1\mathbf{i} + d_2\mathbf{j} + d_3\mathbf{k})$$

is determined by the product and sum in $\mathbf{R}$, the distributivity laws and the multiplication table

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1},$$

$$\mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \ \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \ \mathbf{ki} = -\mathbf{ik} = \mathbf{j}.$$

The ring $\mathbf{H} = \mathbf{H}(\mathbf{R})$ is called the ring of real quaternions.

For any ring R one can construct a quaternion algebra $\mathbf{H}(R)$. However, even if R is a field, this ring does not have to be a skew field. For example $\mathbf{H}(\mathbf{C}) \cong M_2(\mathbf{C})$.

1.3 Group constructions

We give some well known classes of groups.

1. **Abelian groups**.
   The structure of finitely generated abelian groups is well known. Indeed, up to isomorphism these groups are the direct product of cyclic groups. The number of infinite cyclic factors is called the torsion-free rank of the group. So a finitely generated abelian group contains a free abelian group of finite index.

2. **Nilpotent groups and Solvable groups**.
   Examples of nilpotent groups are subgroups of a linear group consisting of the upper triangular matrices over a field with diagonal elements all equal to one. The dihedral group of order $2m$ is the group with presentation:

   $$\mathcal{D}_{2m} = \langle g, h \mid g^m = 1,\ h^2 = 1,\ hgh^{-1} = g^{-1} \rangle,\ m > 2.$$

   The generalized quaternion group of order $2m$ is the group with presentation:

   $$\mathcal{Q}_{2m} = \langle g, h \mid g^m = 1,\ h^2 = g^{m/2},\ hgh^{-1} = g^{-1} \rangle,\ m > 2,\ 2|m.$$

   These groups are of course nilpotent if m is a power of 2. Otherwise, they are not necessarily nilpotent, but they are always solvable. For example D_6 (which is isomorphic with the symmetric group S_3 of degree 3) is solvable but not nilpotent.

3. **Finite groups and simple groups**.
   Simple groups are groups in which the only normal subgroups are the trivial subgroups. Finite simple groups have been classified.

4. **Free groups**.
   A concrete representation of a free group of rank 2 is the subgroup of $SL_2(\mathbb{Z})$ generated by the matrices:

   $$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}.$$

5. **Polycyclic-by-finite groups**.
   A subnormal series of subgroups of a group G is a chain of subgroups

   $$G_0 = \{1\} \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

   so that each G_i is normal in G_{i+1}.

   A group G is said to be polycyclic if it has a subnormal series so that each factor G_{i+1}/G_i in the series is cyclic. We say G is poly-infinite cyclic if it has a subnormal series with each factor infinite cyclic. A group G is said to be polycyclic-by-finite (or virtually polycyclic) if it has a subgroup of finite index that is polycyclic.

1.4 Finite completely 0-simple semigroups

An important class of semigroups are the completely 0-simple semigroups. In this section we characterize finite semigroups of this type. But before we do this we need some general background on semigroups.

If S is a semigroup then we denote by S^1 the smallest monoid (i.e. semigroup with identity) containing S. So $S^1 = S$ if S already has an identity element. Otherwise, $S^1 = S \cup \{1\}$, a disjoint union, with $s1 = 1s = s$ for all $s \in S^1$. Similarly we denote by S^0 the smallest semigroup with a zero containing S. So $S^0 = S$ if S already has a zero element. Otherwise $S^0 = S \cup \{\theta\}$, with $s\theta = \theta s = \theta$ for all S^0.

A left ideal in a semigroup S is a nonempty subset L of S so that $S^1 L \subseteq L$. Similarly one defines right and twosided ideals in S.

Next we introduce some important congruence relations on a semigroup S. An equivalence relation ρ on S is called a *congruence* relation if for all $a, b, c \in S$ the following property holds:

$$a\rho b \text{ implies } ac\rho bc \text{ and } ca\rho cb.$$

If only the former is satisfied then we call ρ a *right congruence relation* (similarly one has a left congruence relation). For such a congruence we denote by S/ρ the set of the equivalence classes. This set becomes a semigroup for the the following operation:

$$\overline{a}\overline{b} = \overline{ab},$$

where $\overline{a}$ denotes the equivalence class containing the element a (sometimes we also denote this class as $a\rho$). We call S/ρ the *factor* semigroup of S modulo ρ. Clearly there is a natural semigroup homomorphism

$$S \to S/\rho : a \mapsto \overline{a}.$$

Congruence relations on groups correspond with normal subgroups.

If I is an ideal of S then we define the *Rees congruence modulo* I on S as follows:

$$a\rho b \text{ if and only if either } a = b \text{ or } a, b \in I.$$

We write S/I for S/ρ and call this the Rees factor semigroup of S modulo I. Thus as a set S/I is $S \setminus I$ together with one element θ (that identifies all elements of I). Note that $\overline{a}\theta = \theta\overline{a} = \theta$, so it is a zero element. So the nonzero elements of S/I correspond with $S \setminus I$ and we will usually denote them also as a (with $a \in S \setminus I$).

We now define the *Green relations* $\mathcal{L}$, $\mathcal{R}$, $\mathcal{D}$ and $\mathcal{J}$ on a semigroup S. For $a, b \in S$,

1. $a\mathcal{L}b$ if and only if $S^1 a = S^1 b$; this is a right congruence and the $\mathcal{L}$ class containing a is denoted L_a;

2. $a\mathcal{R}b$ if and only if $aS^1 = bS^1$; this is a left congruence and the $\mathcal{R}$ class containing a is denoted R_a;

3. $\mathcal{D} = \mathcal{L} \circ \mathcal{R} = \mathcal{R} \circ \mathcal{L}$; i.e. $a\mathcal{D}b$ if and only if there exists $c \in S$ so that $a\mathcal{L}c$ and $c\mathcal{R}b$; the $\mathcal{D}$ class containing a is denoted D_a. $\mathcal{D}$ is the smallest equivalence relation containing both $\mathcal{L}$ and $\mathcal{R}$.

We show that indeed $\mathcal{L} \circ \mathcal{R} \subseteq \mathcal{R} \circ \mathcal{L}$. Suppose that $a, b \in S$ with $a(\mathcal{L} \circ \mathcal{R})b$, i.e., there exists $c \in S$ so that $a\mathcal{L}c$ and $c\mathcal{R}b$. So there exist $u, v \in S^1$ with $a = uc$ and $b = cv$. Let

$$d = av = ucv = ub.$$

Since $\mathcal{L}$ is a right congruence, $a\mathcal{L}c$ implies $av\mathcal{L}cv$. So $d\mathcal{L}b$. Since $\mathcal{R}$ is a left congruence, $c\mathcal{R}b$ implies $uc\mathcal{R}ub$. Thus $a\mathcal{R}d$. Hence $a(\mathcal{R} \circ \mathcal{L})b$; as required.

4. $a\mathcal{J}b$ if and only if $S^1aS^1 = S^1bS^1$; J_a denotes the class of a (so it is the set of generators of $J(a) = S^1aS^1$, and the set of non generators of $J(a)$ as a twosided ideal is denoted I_a. The set of $\mathcal{J}$-classes is partially ordered for the relation $J_a \leq J_b$ if $S^1aS^1 \subseteq S^1bS^1$ (that is, $a \in J(b)$).

5. $\mathcal{H} = \mathcal{L} \cap \mathcal{R}$, an equivalence relation; the class of a is denoted by H_a.

Lemma 1.4.1. *For $a, b \in S$, $a\mathcal{D}b$ if and only if $R_a \cap L_b \neq \emptyset$.*

Proof. Clearly $a\mathcal{D}b$ if and only if there exists $c \in S$ so that $a\mathcal{R}c$ and $c\mathcal{L}b$, or equivalently there exits $c \in S$ with $c \in R_a$ and $c \in L_b$. Hence the result follows. □

A semigroup S is left simple (i.e. the only left ideal is the semigroup itself) if and only if S consists of a single $\mathcal{L}$-class. S is simple (only one twosided ideal) if and only if S consists of a single $\mathcal{J}$-class.

Lemma 1.4.2. *If $a\mathcal{R}b$ and $as = b$ and $bs' = a$ for some $s, s' \in S^1$, then the mappings*

$$\sigma : L_a \to L_b : x \mapsto xs$$

and

$$\sigma' : L_b \to L_a : x \mapsto xs'$$

are mutually inverses preserving $\mathcal{R}$ classes.

Proof. If $x \in L_a$ then $x\mathcal{L}a$ and thus $xs\mathcal{L}as$. As $as = b$ this gives $xs \in L_b$. So the range of σ is indeed contained in L_b.

Suppose $x \in L_a$ and thus $x = ta$ for some $t \in S^1$. Then $x\sigma\sigma' = xs\sigma' = xss' = tass' = tbs' = ta = x$. So $\sigma\sigma' = 1_{L_a}$. Similarly $\sigma'\sigma = 1_{L_b}$.

Finally, let $y = x\sigma = xs$. Then $ys' = xss' = x$. Thus $y\mathcal{R}x$. Thus σ preserves $\mathcal{R}$-classes (similarly, so does σ'). □

If a semigroup has a zero element θ then clearly $\{\theta\}$ is a twosided ideal in S. A semigroup (not necessarily having a zero element) is called 0-*simple* if it has no nonzero proper ideals and it is not a semigroup with zero multiplication and of cardinality two.

The class of 0-simple semigroups has an important subclass of *completely 0-simple semigroups*. These are the 0-simple semigroups that have a primitive idempotent, that is, a nonzero idempotent that is minimal with respect to the natural order in the set $E(S)$ of (nonzero) idempotents given by $e \leq f$ if and only if $e = ef = fe$ for $e, f \in E(S)$.

We now restrict our attention to a finite semigroup S. If $s \in S$, then consider the cyclic semigroup generated by s:

$$\langle s \rangle = \{s^n \mid n = 1, 2, 3, \ldots\}.$$

Since S is finite, there exist positive integers n and k such that $s^{n+k} = s^n$. Hence $s^{n+vk} = s^n$ for any positive integer v. In particular, $s^{n(1+k)} = s^n$. So the semigroup $\langle s \rangle$ contains an element a with

$$a^m = a$$

for some integer $m \geq 2$. If $m = 2$ then a is an idempotent. Otherwise $a^{m-1}, a^{m-2} \in \langle s \rangle$ and

$$(a^{m-1})^2 = a^{m-1}a^{m-1} = (a^{m-1}a)(a^{m-2}) = a^m a^{m-2} = aa^{m-2} = a^{m-1}.$$

So we have shown the following.

Lemma 1.4.3. *Any cyclic semigroup $\langle s \rangle$ in a finite semigroup S contains an idempotent.* □

If S is a finite semigroup then it contains only finitely many ideals. Their product is also an ideal, which is contained in any ideal of S. So S contains an ideal M contained in any ideal, we call this the *core* of S. Note that $M = SMS^1 = S^1MS = SMS$. We now show that M as a semigroup is itself a 0-simple semigroup. Indeed, let J be a nonzero ideal of the semigroup M. Then MJM is an ideal of S contained in M. So $M = MJM \subseteq J$ and thus $J = M$. Clearly, if S also has a zero element θ then $M = \{\theta\}$; on the other hand if S does not have a zero element then M^0 is an ideal that is minimal amongst the non-zero ideals.

More general, let S be a semigroup with a zero element θ. A non-zero ideal that does not properly contain a non-zero ideal is called a 0-minimal ideal. Since S is finite, it easily is seen that S contains such an ideal (provided $S \neq \{\theta\}$). In the following lemma we prove that such an ideal either is null or (completely) 0-simple.

Lemma 1.4.4. *Let S be a finite semigroup with zero θ and suppose $S \neq \{\theta\}$. Let M be a 0-minimal ideal of S. Then, M is a completely 0-simple semigroup or it is null semigroup, that is, a semigroup with zero multiplication. In the former case, for every $x \in M$ there exist idempotents $e, f \in M$ such that $x = exf$.*

Proof. As M^2 is an ideal of S contained in M and because M is a 0-minimal ideal of S, it is clear that either $M^2 = \{\theta\}$ or $M^2 = \{\theta\}$. In the former case M has zero multiplication.

Suppose now the other case holds, that is, $M^2 = M \neq \{\theta\}$. Let $\theta \neq x \in M$. Then $Mx \neq \{\theta\}$, for otherwise $M = MM = MM^1xM^1 = MxM^1 = \{\theta\}$, a contradiction. Similarly $xM \neq \{\theta\}$. (Note that this also implies that M is 0-simple as a semigroup.) Hence $M = M^1xM = M^1MxM = MxM$ and thus $x \in MxM$. So

$$x = x_1xx_2$$

for some $x_1, x_2 \in M$. Hence

$$x = x_1^n x x_2^n,$$

for any positive integer n. Clearly $x_1^n, x_2^n \neq \theta$. Let n be such that $e = x_1^n$ and $f = x_2^n$ are idempotents in $\langle x_1 \rangle$ and $\langle x_2 \rangle$ respectively. Then it follows that M contains the nonzero idempotent e. It follows therefore that M is completely 0-simple; and the lemma follows. □

From now on let M be a finite completely 0-simple semigroup with zero element θ. From the previous proof we know that for any $x \in M$ there exist idempotents $e, f \in M$ so that $exf = x$ and thus $Mx = M^1x$, and similarly $xM = xM^1$.

Lemma 1.4.5. *The semigroup M is the θ-disjoint union of the 0-minimal left ideals (that is, a left ideal which does not contain proper nonzero left ideals). Also, M is the disjoint union of the 0-minimal right ideals.*

Proof. As seen above, if $\theta \neq x \in M$, then $Mx = M^1x$. So the 0-minimal left ideals are of the form Mx. Note that

$$M = MxM = \cup_{y \in M} Mxy.$$

If $y, z \in M$ then either $Mzxy = \{\theta\}$ or

$$M^1zxy = Mzxy = Mxy.$$

It follows that Mxy is also a 0-minimal left ideal. The result therefore follows. □

Thus it follows that each nonzero element belongs to a unique minimal left ideal. Hence every nonzero principal left ideal is a 0-minimal left ideal. Therefore the nonzero $\mathcal{L}$-classes adjoined with θ are precisely the 0-minimal left ideals. Similarly the nonzero $\mathcal{R}$-classes together with θ are the 0-minimal right ideals of M. Note that two nonzero minimal left ideals are either θ-disjoint or equal. Moreover, we have shown that for each nonzero element $x \in M$ there exists idempotents $e, f \in M$ so that $x = ex$ and $x = xf$. Thus the nonzero $\mathcal{L}$-classes are generated by an idempotent.

Lemma 1.4.6. *If e is a nonzero idempotent then the nonzero elements in eMe form a group with identity e.*

Proof. First note that for any $\theta \neq exe \in eMe$,

$$exeM = eM$$

and thus

$$(exe)(eMe) = (exeM)e = eMe.$$

Hence there exists $eye \in eMe$ so that $(exe)(eye) = e$. Similarly there exists $eze \in eMe$ so that $(eze)(exe) = e$. It follows that the nonzero elements of eMe are multiplicatively closed, have identity e and have left and right inverses. So the lemma follows. □

Let us now introduce some notation. Let $L_1, \cdots, L_n$ be the different nonzero $\mathcal{L}$-classes each adjoined with θ and $R_1, \cdots, R_m$ the different nonzero $\mathcal{R}$-classes together with θ. Then

$$M = \cup_{1 \leq i \leq n} \cup_{1 \leq j \leq m} L_i \cap R_j.$$

Thus the $H_{ij} = (L_j \cap R_i) \setminus \{\theta\}$ are the nonzero $\mathcal{H}$-classes. Clearly, $(L_j \cap R_i) \setminus \{\theta\}$ is an $\mathcal{H}$-class if non-empty. So we only have to show this set actually is non-empty. Well, for each $1 \leq i \leq n$ take $\theta \neq x_{1i} \in L_i$ and for each $1 \leq j \leq m$ take $\theta \neq x_{j1} \in R_j$. Then

$$L_i = Mx_{1i} \text{ and } R_j = x_{j1}M.$$

Thus

$$\{\theta\} \neq x_{j1}Mx_{1i} \subseteq R_j \cap L_i = H_{ji}.$$

So we can represent the nonzero elements of M as the union of the following blocks:

H_{11}	H_{12}	$\cdots$	H_{1n}
H_{21}	H_{22}	$\cdots$	H_{2n}
$\vdots$			$\vdots$
H_{m1}	H_{m2}	$\cdots$	H_{mn}

.

Lemma 1.4.6 implies that each $\mathcal{H}$-class which contains a nonzero idempotent e is a group with e as an identity. Renumbering the sets we may assume H_{11} contains an idempotent, say e. Thus $L_1 = Me$ and $R_1 = eM$.

Now, notice that

$$H_{ij}H_{kl} \subseteq H_{il}^0.$$

Also for $x_{i1} \in H_{i1}$ we have $H_{i1} \subseteq R_i = x_{i1}M$ and thus

$$H_{i1}M \subseteq x_{i1}M = x_{i1}eM.$$

As $H_{i1} = H_{i1}e$ we get

$$H_{i1} \subseteq x_{i1}eMe \setminus \{\theta\} \subseteq x_{i1}H_{11}.$$

Since $\theta \notin x_{i1}H_{11}$ it follows that

$$H_{i1} = x_{i1}H_{11}.$$

Similarly

$$H_{1j} = H_{11}x_{1j}.$$

Hence, in general,

$$H_{ij} \subseteq x_{i1}M = x_{i1}eM$$

and thus

$$H_{ij} \subseteq x_{i1}H_{1j} = x_{i1}H_{11}x_{1j}.$$

So (note that $\theta \notin x_{i1}H_{1j}$. Indeed for otherwise $\theta = x_{i1}h_{1j}M = x_{i1}R_1$ for some $h_{1j} \in H_{1j}$. This is impossible as $e \in R_1$ is a right identity for x_{i1})

$$H_{ij} = x_{i1}H_{11}x_{1j}.$$

Hence we have shown that each nonzero element of M can be written uniquely (verify the uniqueness) in the form

$$x_{i1}h_{11}x_{1j}$$

with $h_{11} \in H_{11}$. The multiplication of two such elements is as follows:

$$(x_{i1}h_{11}x_{1j})(x_{k1}h'_{11}x_{1l}) = (x_{i1}h_{11}p_{jk}h'_{11}x_{1l})$$

with

$$p_{jk} = x_{1j}x_{k1} \in H_{11}^{\theta}.$$

Let us denote H_{11} as G and let

$$P = (p_{ji}),$$

a generalized $n \times m$ matrix over G^0, that is, every entry (defined as above) lies in G^0. Further let $\mathcal{M}^0(G^0, m, n, P)$ be the set of all generalized $m \times n$ matrices over G^0 with at most one nonzero entry, and with multiplication defined by the rule

$$AB = A \circ P \circ B,$$

where $\circ$ denotes the usual multiplication of matrices. Any nonzero element of $\mathcal{M}^0(G^0, m, n, P)$ is uniquely determined by its nonzero entry, and so it may be denoted by (g, i, j), where $g \in G$ and $1 \leq i \leq m$, $1 \leq j \leq n$. Therefore $\mathcal{M}^0(G^0, m, n, P)$ maybe treated as the set of all such triples with multiplication given by

$$(g, i, j)(h, k, l) = (gp_{jk}h, i, l).$$

If P is a matrix over G then the nonzero matrices in $\mathcal{M}^0(G^0, m, n, P)$ form a semigroup which we denote by $\mathcal{M}(G^0, m, n, P)$.

So we have shown part of the following theorem.

Theorem 1.4.7. *Let S be a finite semigroup with nonzero multiplication. If $\theta \in S$, then S is 0-simple if and only if S is isomorphic to a semigroup of matrix type $\mathcal{M}^0(G^0, m, n, P)$ (with G a finite group) such that for every $1 \leq i \leq m$ there exists $1 \leq j \leq m$ so that $p_{ji} \neq \theta$, and for every $1 \leq k \leq n$ there exists $1 \leq l \leq m$ with $p_{kl} \neq \theta$.*

If $\theta \notin S$, then S is (0-)simple if and only if S is isomorphic to a semigroup of matrix type $\mathcal{M}(G^0, m, n, P)$ (with G a finite group) such that P is a matrix over G (so P has no nonzero entries).

Proof. To prove the result, it is easily seen that we may assume that $\theta \in S$. That the conditions are necessary has been proven. The converse is an easy exercise. □

In general one can extend the above result as follows.

Theorem 1.4.8. *A semigroup S (with zero) is completely 0-simple if and only if S is isomorphic to a matrix semigroup of matrix type $\mathcal{M}^0(G, I, J, P)$, with G a group and I, J indexing sets and P a sandwich matrix over G, so that each row and column of P contains a nonzero element.*

We list a few properties of semigroups of the type $\mathcal{M}^0(G^0, m, n, P)$.

Lemma 1.4.9. *Let $S = \mathcal{M}^0(G^0, m, n, P)$ be a semigroup of matrix type which is completely 0-simple Then*

1. *$\{(g, i, j) \mid p_{ji} \neq \theta,\ g = p_{ji}^{-1}\}$ is the set of nonzero idempotents.*
2. *if $p_{ji} \neq \theta$ then $\{(g, i, j) \mid g \in G\}$ is a maximal subgroup of S (that is, it is a subgroup that is not contained in a properly larger subgroup).*
3. *S is regular, that is, for every $s \in S$ there exists $x \in S$ so that $sxs = s$.*

A regular semigroup is called an *inverse semigroup* if the idempotents of S commute; or, equivalently, for every $s \in S$ there exists a unique $x \in S$ with $sxs = s$ and $xsx = x$. One can show that a completely 0-simple semigroup is an inverse semigroup if and only if the sandwich matrix P has precisely one nonzero entry in each row and column. It follows that P is a square matrix and we may assume it is the identity matrix.

1.5 Structure of finite semigroups.

Let I be an ideal in a semigroup S. Then the natural mapping

$$S \to S/I : s \mapsto \overline{s}$$

is a homomorphism of semigroups. It defines a one-to-one correspondence between the ideals of S/I and the ideals of S that contain I.

Theorem 1.5.1. *A finite semigroup S has series of subsets*

$$S_0 \subseteq S_1 \subseteq \cdots \subseteq S_n = S,$$

so that

1. *$S_0 = \{\theta\}$ if S has a zero element θ, otherwise $S_0 = \emptyset$,*
2. *each S_i $(1 \leq i \leq n)$ is an ideal in S, and there are no ideals strictly between S_i and S_{i+1},*
3. *the Rees factors S_i/S_{i-1} are either null semigroups or completely 0-simple semigroups. (We agree that $S_1/S_0 = S_1$ if $S_0 = \emptyset$.) The factors S_i/S_{i-1} are called the principal factors of S.*

Proof. Without loss of generality we may assume that S contains a zero element θ. If $S = \{\theta\}$ then the result is obvious. So we may assume that $S \neq \{\theta\}$. From the previous section we know that a 0-minimal ideal $S_1 = I$ of S is either a null semigroup or a completely 0-simple semigroup.

If $S = S_1$ then we are finished. If $S \neq S_1$, then consider the semigroup $T = S/S_1$. So now T is again a semigroup with zero element. Let J be a 0-minimal ideal in T. It corresponds in S with an ideal K of S that properly contains S_1. Moreover $K/S_1 \cong J$, as semigroups. From a previous Lemma we thus know that either $J^2 = \{\theta\}$ or J is completely 0-simple. Put $S_2 = K$. If $S_2 = S$ then we are finished. If not, then we repeat the above argument on S/S_2. The conclusion then follows by a repeated argument. □

One can show that the principal factors are uniquely determined by the semigroup.

1.6 Structure of linear semigroups.

We now consider an important class of completely 0-simple semigroups arising from skew linear semigroups. Let D be a division ring. Let $M_n(D)$ be the $n \times n$ matrix ring over D. We can treat this matrix ring as the ring of endomorphisms of the left D-module D^n with fixed standard basis. If $a \in M_n(D)$, then we define the rank $\rho(a)$ of a as the dimension of the subspace $(D^n)a$ of D^n (we have written the endomorphism a on the right of the argument). For $0 \leq j \leq n$, put

$$I_j = \{a \in M_n(D) \mid \rho(a) \leq j\}.$$

It is easily seen that each I_j is an ideal of $M_n(D)$, treated as semigroup under multiplication of matrices.

Theorem 1.6.1. *For any division algebra D and any integer $n \geq 1$, the ideals listed in the chain*

$$I_0 \subseteq I_1 \subseteq \cdots \subseteq I_n = M_n(D)$$

are the only ideals of the multiplicative semigroup of the algebra $M_n(D)$. Moreover, every Rees factor I_j/I_{j-1}, $1 \leq j \leq n$, is a completely 0-simple semigroup, the maximal subgroups of which are isomorphic to the full skew linear groups of the corresponding algebras $M_j(D)$.

Proof. Let $a, b \in M_n(D)$ be such that $\rho(a) = \rho(b) = j \geq 1$. Then $(D^n)a$ and $(D^n)b$ are isomorphic as left D-linear spaces. So there exists an invertible matrix $x \in M_n(D)$ such that

$$(D^n)ax = (D^n)b.$$

Since ax maps D^n onto $(D^n)b$, we get that for any e_i in the standardbasis $e_1, \ldots, e_n$ of D^n, there exists $f_i \in D^n$ such that

$$(f_i)ax = (e_i)b.$$

Then

$$yax = b,$$

where $y \in M_n(D)$ is such that

$$(e_i)y = f_i$$

for any $1 \leq i \leq n$. Hence $b \in M_n(D)aM_n(D)$. Since a, b are arbitrary elements of $I_j \setminus I_{j-1}$, this shows that $I_j \setminus I_{j-1}$ is a $\mathcal{J}$-class of the multiplicative semigroup of $M_n(D)$. Thus I_j/I_{j-1} is a 0-simple semigroup (note that it does not have zero multiplication as this semigroup contains a nonzero idempotent). Since $M_n(D)$ has finite dimension it is readily verified that this semigroup does not have an infinite descending chain of idempotents (for the natural order). Hence I_j/I_{j-1} is a completely 0-simple semigroup.

Moreover, for $e = e^2 \in I_j \setminus I_{j-1}$, the algebra $eM_n(D)e$ is the endomorphism algebra of the left D space $(D^n)e$. Thus we have an isomorphism of algebras $eM_n(D)e \cong M_j(D)$. Now every invertible element c of $eM_n(D)e$ is of the form

$$c = e(ece)e,$$

where $ece \in I_j \setminus I_{j-1}$. Since $e(I_j/I_{j-1})e$ is a maximal subgroup of I_j/I_{j-1} with the zero adjoined, the properties of completely 0-simple semigroups imply that $e(I_j/I_{j-1})e$ is isomorphic to the group of invertible matrices in $M_j(D)$ with the zero adjoined. Hence the result follows. □

Chapter 2

Semisimplicity Problems

2.1 Background

We first recall some structural results. Let us first recall the notion of prime ring.

Definition 2.1.1. *A ring R is is said to be prime if $AB \neq \{0\}$ for all $\{0\} \neq A, B \lhd R$.*

Proposition 2.1.2. *Let R be a ring. The following conditions are equivalent:*

1. *R is prime;*
2. *$Ann_R(L) = \{0\}$ for every nonzero left ideal L of R;*
3. *if $a, b \in R$ and $aRb = \{0\}$, then $a = 0$ or $b = 0$.*

Definition 2.1.3. *A ring R is (left) primitive if and only if it has a faithful simple left R-module.*

Example 2.1.4. *Let F be a field and σ an automorphism of F of infinite order. Then $F[X, X^{-1}, \sigma]$ is a primitive ring without minimal left ideals.*

Proof. Consider the skew Laurent polynomial ring $R = F[X, X^{-1}, \sigma]$. Recall that

$$(aX^i)(bX^j) = (a\sigma^i(B))X^{i+j},$$

$a, b \in F$ and that R is the F-vectorspace with basis $\{X^i \mid i \in \mathbb{Z}\}$.

We now from the exercises that all ideals of $F[X, \sigma]$ are generated by a monomial X^i. Since the latter are invertible in R, every nonzero ideal of R (which clearly intersects $F[X, \sigma]$ in a nonzero ideal) is equal to R. Hence R is a simple ring and therefore a primitive ring.

With standard techniques one easily verifies that R is not a division ring, hence $soc(R) = \{0\}$. So R is without minimal left ideals. $\square$

Proposition 2.1.5. *A simple ring R is primitive. A primitive ring R is prime.*

Not every primitive ring is simple and not every prime ring is primitive. Indeed a commutative ring is primitive if and only if the ring is a field.

We now turn to internal characterizations of primitive rings.

Definition 2.1.6. *Let L be a left ideal of a ring R. The core of L, denoted $core(L)$, is the largest twosided ideal of R contained in L. The the core of L is the sum of all ideals of R contained in L.*

Proposition 2.1.7.

1. *Let L be a left ideal of a ring R. Then $core(L) = Ann_R(R/L)$.*
2. *If L is a maximal left ideal of R, then $R/core(L)$ is a primitive ring.*
3. *R is a primitive ring if and only if R has a maximal left ideal L whose core is $\{0\}$.*

There is another related internal characterization of primitive rings.

Definition 2.1.8. *A left ideal L of a ring R is said to be comaximal with all ideals if $L + I = R$ for all $\{0\} \neq I \lhd R$.*

Lemma 2.1.9. *Let R be a ring with maximal left ideal L. Then $core(L) = \{0\}$ if and only if L is comaximal with all ideals of R.*

Proposition 2.1.10. *R is a primitive ring if and only if R has a left ideal L comaximal with all ideals.*

Proposition 2.1.11. *If R is a prime ring with minimal left ideal L, then L is faithful simple in $R - \mathcal{MOD}$, implying R is primitive. Moreover, every faithful simple R-module M is isomorphic to L, implying $End_R(M) \cong End_R(L)$.*

Definition 2.1.12. *An ideal P of a ring R is prime if R/P is a prime ring.*

If A, B are (left) ideals of a ring R, then AB denotes the (left) ideal $\{\sum_{i=1}^{n} a_i b_i \mid a_i \in A,\ b_i \in B,\ n \in \mathbf{N}\}$.

Proposition 2.1.13. *Let R be a ring and $P \lhd R$. The following conditions are equivalent.*

1. *P is a prime ideal.*
2. *Let $A, B \lhd R$. If $AB \subseteq P$, then $A \subseteq P$ or $B \subseteq P$.*
3. *If $P \subset A$ and $P \subset B$, A, B ideals of R, then $AB \not\subseteq P$.*
4. *If $aRb \subseteq P$, $a, b \in R$, then $a \in P$ or $b \in P$.*

It is also useful to "decompose" a ring starting from an infinite set of ideals. Therefore the following definition.

Definition 2.1.14. *Let $\{A_i \mid i \in I\}$ be a set of ideals of a ring R. The ring R is said to be a subdirect product of $\{R/A_i \mid i \in I\}$ if the natural mapping $\phi : R \to \prod_{i\in I} R/A_i$ is injective (or equivalently $\cap_{i\in I} A_i = \{0\}$).*

Subdirect products are rings that can be studied in terms of direct products of homomorphic images. Note that subdirect products are much more general than direct products. For example, $\mathbb{Z}$ is the subdirect product of the finite fields $\mathbf{Z}_p$, where p runs over all prime numbers. The polynomial ring $F[X]$ of a field F is the subdirect product of the fields $F[X]/(f)$, where f runs over the irreducible polynomials and $(f) = F[X]f$. Note that $F[X]/(f_1 \dots f_n) \cong \prod_{i=1}^{n} F[X]/(f_i)$, where the f_i's are distinct irreducible monic polynomials.

Definition 2.1.15. *A ring R that is the subdirect product of prime rings is said to be semiprime. So R is semiprime if and only if the intersection of all prime ideals of R is $\{0\}$.*

The class of semiprime rings has a central role in the structure theory. Before we state the main reason for this, we need a technical lemma and the following notion. Let R be a ring and S a subset of nonzero elements of R. The set S is called an $m - set$ if for every $s_1, s_2 \in S$ there exists $r \in R$ with $s_1 r s_2 \in S$. Complements of prime ideals are examples of m-sets.

Lemma 2.1.16. *If R is a ring and S an m-set in R, then $R \setminus S$ contains a prime ideal.*

Proof. The zero ideal intersects S trivially. Hence by Zorn's Lemma there exits an ideal P in R maximal with respect to the condition $P \cap S = \emptyset$. We claim P is prime. Indeed if $A, B \lhd R$ and $P \subset A$, $P \subset B$, then there exist $s_1 \in (S \cap A)$ and $s_2 \in (S \cap B)$. Hence, for some $r \in R$, $s_1 r s_2 \in (S \cap AB)$. Therefore $AB \not\subseteq P$. □

Definition 2.1.17. *Let R be a ring. A (left) ideal I of R is nilpotent if $I^n = \{0\}$ for some nonzero n. The smallest such n is called the nilpotency index of I.*

Let C_2 be the cyclic group of order 2 generated by the element g. Then, in the group algebra $R = \mathbb{Z}_2[C_2]$, the ideal $\omega = R(1 - g)$ has nilpotency index 2. However, in the group ring $T = \mathbf{Q}[C_2]$ the ideal $T(1 - g)$ is not nilpotent.

Proposition 2.1.18. *Let R be a ring. The following conditions are equivalent.*

1. *R is semiprime.*

2. R has no nonzero nilpotent left ideals.

3. R has no nonzero nilpotent ideals.

4. R has no nonzero nilpotent ideals of nilpotency index 2.

2.2 Structural Results: revisited

If R has a faithful simple module M then by Schur's Lemma $D = End_R(M)$ is a division ring. Furthermore, M is a left D-module. By means of the (left) regular representation, one can consider $R \subseteq End_D(M)$.

Definition 2.2.1. *Let R be an arbitrary subring of $End_D(M)$, where M is left D-module over the division ring D. View $M \in R - \mathcal{MOD}$ by the given action of R on M. The ring R is said to be dense if for every $n \in \mathbf{N}$ and every D-independent set $\{m_1, \ldots, m_n\}$ in M we have $R(m_1, \ldots, m_n) = M^{(n)}$; i.e. given $v_1, \ldots, v_n$ in M there exists $r \in R$ such that $rm_i = v_i$ for $1 \leq i \leq n$. Another equivalent way of stating this is: for every $f \in End_D(M)$ and $m_1, \ldots, m_n$ in M, there exists $r \in R$ such that $f(m_i) = rm_i$.*

Note that every dense subring R of $End_D(M)$ is primitive. Indeed, it is obvious that M is faithful in $R - \mathcal{MOD}$ and by the definition of dense for $n = 1$, it is also clear that M is a simple R-module. That the converse also holds is proved in the following theorem

Theorem 2.2.2 (Jacobson's density theorem)**.** *Suppose the ring R has a faithful simple module M. If $D = End_R(M)$, then R is dense in $End_D(M)$.*

One can also formulate these results in terms of matrices.

Proposition 2.2.3. *Let R be a dense subring of $End_D(M)$, where M is a left D-module over the division ring D. If $dim_D(M) = n < \infty$, then $R \cong M_n(D)$.*

Proposition 2.2.4. *Let R be a dense subring of $End_D(M)$, where M is a left D-module over the division ring D. If $dim_D(M)$ is infinite, then for every $n \in \mathbf{N}$ there is a subring of R with $M_n(D)$ as a homomorphic image.*

Theorem 2.2.5 (Wedderburn-Artin)**.** *If R is a left Artinian primitive ring , then $R \cong M_n(D)$ for some division ring D. Hence, any left Artinian simple ring is isomorphic with a matrix ring over a division ring. In particular, any left Artinian simple ring is also right Artinian.*

Definition 2.2.6. *The elements 0 and 1 are called trivial idempotents in any ring. Idempotents e and e' of a ring R are said to be orthogonal if $ee' = e'e = 0$. Note that if e is an idempotent, then $1 - e$ is an idempotent orthogonal to e. An idempotent e of a ring R is said to be primitive if e cannot be written as the sum of two non-trivial orthogonal idempotents.*

Lemma 2.2.7. *An idempotent e of a ring R is primitive if and only if there is no nonzero idempotent e_1 such that $Re_1 \subset Re$. In fact, if $Re_1 \subset Re$, then there is an idempotent e_1' such that $Re_1 = Re_1'$ and $e_1', e - e_1'$ are orthogonal.*

Theorem 2.2.8. *Let R be a left Artinian ring.*

1. *Every proper prime ideal of R is a maximal proper ideal. In particular, if R is prime then R is simple.*

2. *R has only finitely many distinct proper prime ideals $P_1, \ldots, P_n$, and $R/\cap_{i=1}^n P_i \cong \prod_{i=1}^n R/P_i$, a direct product of simple Artinian rings.*

Definition 2.2.9. *The socle of an R-module M, denoted $soc(M)$, is the sum of the simple submodules of M if M has simple submodules; otherwise $soc(M) = \{0\}$. M is said to be completely reducible if $soc(M) = M$.*

Theorem 2.2.10. *The following conditions are equivalent for a ring R.*

1. *R is a finite direct product of simple Artinian rings.*

2. *$R = soc(R)$.*

3. *R is semiprime and left Artinian.*

Definition 2.2.11. *A ring R satisfying the conditions of Theorem 2.2.10 is called a semisimple Artinian ring, or just simply semisimple ring.*

Note that the conditions for a ring to be semisimple are left-right symmetric.

Theorem 2.2.12. *Let $R = \prod_{i=1}^n R_i$ be a semisimple Artinian ring, where each $R_i = M_{n_i}(D_i)$ form some division rings D_i. The R_i are called the simple components of R. Let $e_i = (0, \ldots, 0, 1, 0 \ldots, 0)$, i.e. a 1 appears in the i-th position and zeros elsewhere.*

1. *Then each e_i is a central idempotent of R, and $\sum_{i=1}^n e_i = 1$. The $M_i = Re_i$ are the unique minimal ideals of R, and each M_i is a ring with multiplicative identity e_i. Further, $R_i \cong M_i$ as rings.*

2. *Any simple R-module is isomorphic to Re for some primitive idempotent e of R.*

3. *Every primitive idempotent e of R lies in some M_i. Two primitive idempotents e, e' are in the same component M_i if and only if $Re \cong Re'$ (as modules), or equivalently $eRe' \neq \{0\}$.*

4. *There are precisely n isomorphic classes of simple R-modules, one for each simple component.*

Definition 2.2.13. *Let N be a submodule of an R-module M. We say N has a complement if there exits a submodule N' of M such that $M = N \oplus N'$. The module M is said to be complemented if every nonzero submodule has a complement.*

Proposition 2.2.14. *Let R be a ring and $M \in R - \mathcal{MOD}$. Then, M is completely reducible if and only if M is complemented.*

Theorem 2.2.15. *Let R be a ring. The following conditions are equivalent.*

1. *R is semisimple Artinian.*
2. *R is completely reducible in $R - \mathcal{MOD}$.*
3. *Every R-module is completely reducible.*
4. *Every R-module is complemented*

Corollary 2.2.16. *Let R be a ring. R is semisimple Artinian if and only if every R-module is projective.*

2.3 The Jacobson Radical

Because of the Jacobson density Theorem, primitive rings are an important class of rings. Using subdirect products one is then able to study subdirect products of primitive rings. The following definition is therefore useful.

Definition 2.3.1. *An ideal P of a ring R is primitive if R/P is a primitive ring. And a ring R is semiprimitive if the intersection of all primitive ideals of R is trivial, or equivalently, R is the subdirect product of primitive rings.*

Since a primitive ring is prime, any primitive ideal is a prime ideal. Further, an ideal P is primitive if and only if P is the annihilator of a simple R-module M (which is equivalent with, M is a faithful simple R/P-module).

Examples of primitive ideals are maximal ideals. The reason being that simple rings are primitive. So any ring contains primitive ideals.

The Jacobson radical "measures" the obstruction to being semiprimitve. Using this ideal we give another characterization of semisimple Artinian rings.

Definition 2.3.2. *The Jacobson radical of a ring R, denoted $J(R)$, is the intersection of the primitive ideals of R; or equivalently, $J(R)$ is the intersection of the annihilators of the simple R-modules.*

Theorem 2.3.3. *A ring R is semisimple Artinian if and only if R is semiprimitive Artinian.*

Proposition 2.3.4. *Let R be a ring and I an ideal of R. The following statements hold.*

1. $(J(R) + I)/I \subseteq J(R/I)$.
2. *If $I \subseteq J(R)$, then $J(R/I) = J(R)/I$.*
3. $J(R/J(R)) = \{0\}$, *i.e. $R/J(R)$ is semiprimitive.*

Proof. Let $\overline{R} = R/I$. Let $\overline{P} = P/I$ be an ideal of $\overline{R}$, where P is an ideal of R containing I. Since $\overline{R}/\overline{P} \cong R/P$, the ideal P is a primitive ideal of R if and only if $\overline{P}$ is a primitive ideal of $\overline{R}$. Hence

$$J(\overline{R}) = \bigcap\{\overline{P} \mid P \text{ a primitive ideal of } R \text{ containing } I\}.$$

So (1) follows. If $I \subseteq J(R)$, then any primitive ideal of R contains I. Therefore (2) follows. (3) is a special case of (2). □

Note that Proposition 2.3.4.(1) says that a ring epimorphism maps the Jacobson radical in the Jacobson radical, in particular, $f(J(R)) = J(f(R))$ for any ring isomorphism f.

Proposition 2.3.5. *The Jacobson radical of a ring R is the intersection of all maximal left ideals of R.*

Proof. Let L be a maximal left ideal of R. By Proposition 2.1.7, L contains a primitive ideal of R. Hence $J(R) \subseteq L$, and thus $J(R)$ is contained in the intersection of all maximal left ideals. For the converse inclusion, let P be a primitive ideal of R. Then for some simple R-module M,

$$P = Ann_R(M) = \bigcap_{0 \neq m \in M} Ann_R(m).$$

Now for $0 \neq m \in M$, $R/Ann_R(m) \cong Rm = M$. Hence $Ann_R(m)$ is a maximal left ideal of R. Therefore

$$\bigcap\{\text{maximal left ideals of } R\} \subseteq \bigcap_{0 \neq m \in M} Ann_R(m) \subseteq P.$$

Since P is an arbitrary primitive ideal of R, the result follows. □

The Jacobson radical can also be described elementwise.

Definition 2.3.6. *Let R be a ring. An element $r \in R$ is left quasi regular if $1 - r$ is left invertible in R; and r is right quasi regular if $1 - r$ is right invertible in R. If r is left and right quasi regular, then r is said to be quasi regular. A subset of R is (left, right) quasi regular if each element is (left, right) quasi regular.*

Nilpotent elements are examples of quasi regular elements. Indeed if $r \in R$ and $r^n = 0$ (with $n > 0$) then

$$(1-r)(1+r+\cdots+r^{n-1}) = 1,$$

so that $1-r$ is invertible. Any element $1 \neq r$ in a division ring is quairegular. So not every quasi regular element is nilpotent.

Lemma 2.3.7. *Let R be a ring $r \in R$. Then, r is left (resp. right) quasi regular if and only if $1-r \notin L$ for every maximal left (resp. right) ideal of R.*

Proof. Note that an element $r \in R$ is not left invertible if $Rr \neq R$, or equivalently Rr is contained in a maximal left ideal. Hence an element is left quasi invertible if and only if $R(1-r)$ is not contained in any maximal left ideal. □

Proposition 2.3.8. *Let R be a ring.*

$$\begin{aligned} J(R) &= \{r \in R \mid rx \text{ is right quasi regular for all } x \in R\} \\ &= \{r \in R \mid yr \text{ is left quasi regular for all } y \in R\} \\ &= \{r \in R \mid yrx \text{ is quasi regular for all } x, y \in R\} \end{aligned}$$

Proof. Let

$$\begin{aligned} A &= \{r \in R \mid rx \text{ is right quasi regular for all } x \in R\}, \\ B &= \{r \in R \mid yr \text{ is left quasi regular for all } y \in R\}, \\ C &= \{r \in R \mid yrx \text{ is quasi regular for all } x, y \in R\}. \end{aligned}$$

If $r \in J(R)$, then $1-r$ cannot be in any maximal left ideal of R. For if, say, $1-r \in L$, L a maximal left ideal, then $1 = (1-r)+r \in L$, a contradiction. Hence r is left quasi regular. Since $J(R)$ is a twosided ideal, it follows that $J(R) \subseteq B$. Also $J(R) \subseteq \{r \in R \mid yrx \text{ is left quasi regular for all } x, y \in R\} = D$.

Clearly D is a twosided ideal. We claim that every element $r \in D$ is quasi regular. Since $r \in D$, there exists $d' \in R$ so that

$$r'(1-r) = 1$$

and thus $-r'r \in D$ is left quasi regular. Therefore

$$r' = 1 + r'r = 1 - (-r'r)$$

has a left invers, i.e. there exists $r'' \in R$ so that

$$r''r' = 1.$$

Hence r' is invertible with inverse $1 - r = r''$. Thus $1 - r$ is invertible. So r is quasi regular.

So $D = C$ and thus $J(R) \subseteq C$.

We now show that $B \subseteq J(R)$. Let $r \in B$. Then Rr is a left ideal contained in B. Suppose, $Rr \not\subseteq J(R)$, i.e. $Rr \not\subseteq L$ for some maximal left ideal L of R. Hence $Rr + L = R$, and thus $1 = a + b$ for some $a \in Rr$ and $b \in L$. Consequently, $b = 1 - a \in L$ is left invertible, a contradiction. Thus $B = J(R)$ and thus

$$J(R) = B \subseteq C \subseteq B = J(R).$$

So $J(R) = C = B$.

Now C is left-right symmetric. So by symmetry it follows that the intersection of all right ideals equals $J(R)$ and also equals A. □

Proposition 2.3.9. *Let R be a ring. Then $J(R)$ is a quasi invertible ideal which contains all left (resp. right) quasi regular left (resp. right) ideals.*

Proof. Because of Proposition 2.3.8, $J(R)$ is a quasi invertible (twosided) ideal. The proof that it contains all left ideals that are quasi invertible is as in the last part of Proposition 2.3.8. □

In Proposition 2.3.8 we have shown that $J(R)$ is independent of "left" and "right" notions. Hence we obtain:

Corollary 2.3.10. *The intersection of the maximal left ideals of a ring equals the intersection of the maximal right ideals.* □

Theorem 2.3.11. *Let R be a right Artinian ring, then $J(R)$ is nilpotent.*

Proof. Let $J = J(R)$. Dan

$$J \supseteq J^2 \supseteq J^3 \supseteq \cdots$$

Since each J^n is a twosided ideal and because R is right artinian there exists $n > 0$ so that $J^n = J^{n+1}$. Let $N = J^n$. Dan $N^2 = N$. It is now sufficient to show that $N = 0$.

Suppose $N \neq \{0\}$. Then $NN = N \neq \{0\}$. Let K be a right ideal which is minimal for the condition that $KN \neq \{0\}$. Let $k \in K$ so that $kN \neq \{0\}$. Then kN is a right ideal contained in K and

$$(kN)N = kN^2 = kN \neq \{0\}.$$

So by the minimality of K we obtain that $kN = K$. Hence there exists $x \in N$ so that $kx = k$. Hence $k(1 - x) = 0$. Because $x \in N \subseteq J$, the element $1 - x$ is invertible. Therefore $x = 0$ and thus $xN = \{0\}$, a contradiction. □

2.4 Group algebras

It is clear from the above that the Jacobson radical is an important ideal. In particular it is crucial to know when the Jacobson radical of some relevant classes of rings is zero.

Amazingly the following is still an open problem (after more than 50 years of research):

Problem 1: Let K be a field and G a group. When is $J(KG) = \{0\}$? Presumably this is the case if K has zero characteristic.

For finite groups the answer is well known.

Theorem 2.4.1. *(Maschke's Theorem) If G is a finite group of order n and K is a field, then $J(KG) = \{0\}$ (i.e. KG is semisimple) if and only if $charK \not| n$.*

Proof. Since G is finite, the group algebra KG is right artinian and thus $J(KG)$ is nilpotent.

If $x \in J(KG)$, then the right multiplication

$$KG \to KG : a \mapsto ax$$

is a K-linear transformation. Suppose $|G| = n$. Let $G = \{g_1, \ldots, g_n\}$ and let $M(x)$ denote the matrix of this transformation with respect to this (ordered) basis G of KG. Thus the (i, j)-entry of $M(x)$ is the coefficient of g_j in $g_i x$.

Because $((a)x)y = a(xy)$ and $a(x + y) = ax + ay$, for $a, x, y \in KG$, we obtain that M is a ring homomorfismen

$$M : KG \to M_n(K).$$

Thus if x is a nilpotent element in KG then $M(x)$ is a nilpotent matrix.

Let

$$t : KG \to K : x \to tr(M(x)),$$

where $tr(M(x))$ is the trace of the matrix $M(x)$. Clearly t is a K-linear map. We recall that the trace of a nilpotent matrix in $M_n(K)$ is zero.

Thus if $x = \sum_{g \in G} x_g g \in J(KG)$ (each $x_g \in K$) then $t(x) = 0$. Note that also

$$t(x) = \sum_{g \in G} x_g t(g).$$

As $t(g) = 0$ if $g \neq 1$ and $t(1) = n$ we obtain that

$$0 = t(x) = t(\sum_{g \in G} x_g g) = n x_1.$$

Now assume that $0 \neq n \in K$. Then $x_1 = 0$. So the coefficient of 1 of any element in $J(KG)$ is zero. So if $x \in J(KG)$ then the coefficient of 1 of all xg^{-1} is zero ($g \in G$). But this implies $x = 0$, as required.

Conversely, suppose $0 = n \in K$. Let $x = \sum_{g \in G} g$. Then

$$xg = x$$

for all $g \in G$ and thus

$$x^2 = nx = 0.$$

So the ideal Kx is nilpotent. Hence $0 \neq Kx \subseteq J(KG)$. So $J(KG) \neq \{0\}$. □

Note that as a consequence of Maschke's Theorem, we get that KG is not a simple ring (if $char(K) \not| |G|$ and $|G| > 1$). Indeed, because $\frac{1}{|G|} \sum_g g$ is a central and non trivial idempotent.

Actually, that KG is not simple is valid for any non trivial group G and field K. Indeed let

$$\omega : KG \to K : \sum_g k_g g \mapsto \sum_g k_g,$$

this is called the *augmentation* mapping. It is easily verified that this is an algebra homomorphism with kernel:

$$\ker \omega = \{\sum_g k_g(g-1) \mid k_g \in K\}.$$

So

$$KG/\ker \omega \cong K$$

and thus the nonzero ideal $\ker \omega$ is a maximal ideal.

Definition 2.4.2. *For any group G and any commutative ring R we define the (Kaplansky) trace map*

$$tr : R[G] \to R$$

as follows:

$$tr((\sum_g r_g g) = r_1.$$

In case K is a field and G is a finite group, this trace differs from the trace map associated with the regular representation by a factor $|G|$.

Note that $tr(\alpha\beta) = tr(\beta\alpha)$.

Lemma 2.4.3. *Let R be a commutative ring and G a group. Suppose $\alpha = \sum r_g g \in RG$. If $char(R) = p$ is prime and q is a power of p, then*

$$tr(\alpha^q) = \sum_{g \in G, g^q = 1} r_g^q.$$

Proof. It is enough to show that that $tr(\alpha^q) = tr(\sum r_g^q g^q)$. Now the terms in α^q are of the form

$$r_{g_1} \cdots r_{g_q} g_1 \cdots g_q.$$

When two g_i are distinct, then we also have the terms

$$r_{g_1} \cdots r_{g_q} g_j \cdots g_q g_1 \cdots g_{j-1}$$

for each $j \leq q$. Since

$$tr(g_j \cdots g_q g_1 \cdots g_{j-1}) = tr(g_1 \cdots g_q)$$

and because $char(R) = p$ (and thus $q = 0$ in R) we obtain that

$$tr(\alpha^q) = tr(\sum r_g^q g^q).$$

□

Proposition 2.4.4. *Suppose R is a commutative domain. Suppose $\alpha = \sum r_g g \in RG$ is a nilpotent element. If either $char(R) = 0$, or $char(R) = p \neq 0$ and $supp(r)$ does not have non-identity elements of order a power of p, then $tr(\alpha) = 0$.*

Proof. Suppose $\text{char}(R) = p > 0$. Let q be a large enough power of p so that $\alpha^q = 0$. Because of the hypothesis, $g^q \neq 1$ for every $1 \neq g \in \text{supp}(\alpha)$. So

$$0 = tr(0) = tr(r^q) = \sum_{g \in G,\, g^q = 1} r_g^q = r_1^q.$$

Hence $r_1 = tr(\alpha) = 0$, as required.

The zero characteristic case follows by applying the previous to "enough" rings of the form $(S/P_p)G$, where P_p is a prime ideal in a finitely generated $\mathbb{Z}$-algebra (contained in R) and P_p contains a prime integer p. The fact that enough such primes exist is guaranteed by the Nullstellensatz. □

Theorem 2.4.5. *Let K be a field and G a group. If G does not have elements of order $char(K)$, then KG does not have nil left ideals.*

Proof. Suppose L is a nil left ideal of KG. Let $x = \sum k_g g \in L$. Then, for each $g \in \text{supp}(x)$, $g^{-1}x \in L$. So by Proposition 2.4.4, $k_g = tr(g^{-1}x) = 0$. Hence $x = 0$ and it follows that $L = \{0\}$. □

Theorem 2.4.6. *(Rickart) If G is a group, then $J(\mathbf{C}G) = \{0\}$.*

Proof For $\alpha = \sum c_g g \in \mathbf{C}G$ we denote

$$|\alpha| = \sum |c_g|.$$

It is clear that

$$|\alpha + \beta| \leq |\alpha| + |\beta|.$$

Further $|\alpha g| = |\alpha|$. Hence, for $\beta = \sum r_g g$,

$$|\alpha\beta| = |\sum \alpha r_g g| \leq \sum |\alpha r_g| = \sum |\alpha||r_g|.$$

So

$$|\alpha\beta| \leq |\alpha||\beta|.$$

Let now $\alpha \in J(\mathbf{C}G)$. Then, for all $c \in \mathbf{C}$, $1 - c\alpha$ is invertible. Consider the map

$$f : \mathbf{C} \to \mathbf{C} : c \mapsto tr(1 - c\alpha)^{-1},$$

where tr is the trace map on the group algebra. We show that f is an entire function and we will give its Taylor series about the origin.

Set $g(c) = (1 - c\alpha)^{-1}$. Thus $f(c) = tr(g(c))$. Because all the $g(c) \in \mathbf{C}G$ commute, we get for $c, d \in \mathbf{C}$,

$$\begin{aligned} g(c) - g(d) &= (1 - c\alpha)^{-1} - (1 - d\alpha)^{-1} \\ &= [(1 - d\alpha) - (1 - c\alpha)](1 - c\alpha)^{-1}(1 - d\alpha)^{-1} \\ &= (c - d)\alpha g(c)g(d). \end{aligned}$$

We now first show that $|g(c)|$ is bounded in a neighborhood of c. Since

$$g(d) = g(c) - (c - d)\alpha g(c)g(d)$$

we get that

$$|g(d)| \leq |g(c)| + |c - d||\alpha g(c)|\,|g(d)|.$$

So

$$|g(d)|(1 - |c - d|||\alpha g(c)|) \leq |g(c)|.$$

So if d is sufficiently close to c then we can make the term $(\dots)$ larger than $\frac{1}{2}$, and thus $|g(d)| \leq 2|g(c)|$.

Now we show that f is an entire function. From the previous formulas we get that

$$g(c) - g(d) = (c - d)\alpha g(c)\left(g(c) - (c - d)\alpha g(c)g(d)\right).$$

Divide this equation by $c - d$ and take traces. So we obtain

$$\frac{f(c) - f(d)}{c - d} - tr(\alpha g(c)^2) = -(c - d)tr(\alpha^2 g(c)^2 g(d)).$$

Because $|tr\gamma| \leq |\gamma|$ we conclude from the boundedness of $|g(d)|$ in a neighborhood of c that

$$\lim_{d \to c} \frac{f(c) - f(d)}{c - d} = tr(\alpha g(c)^2).$$

Hence $f(c)$ is an entire function with $f'(c) = tr(\alpha g(c)^2)$.

Now we compute the Taylor series for f about the origin. Because $f(c) = tr(1-c\alpha)^{-1}$ we expect that for small c we can write $(1-c\alpha)^{-1}$ as the sum of an appropriate geometric series and then obtain f by taking traces. Indeed, set

$$s_n(c) = \sum_{i=0}^{n} c^i tr(\alpha^i).$$

Then

$$\begin{aligned} f(c) - s_n(c) &= tr\left\{ g(c) - \sum_{i=0}^{n} c^i \alpha^i \right\} \\ &= tr\left(g(c) \left\{ 1 - (1-c\alpha) \sum_{i=0}^{n} c^i \alpha^i \right\} \right) \\ &= tr\left(g(c) c^{n+1} \alpha^{n+1} \right). \end{aligned}$$

Because $g(c)$ is bounded in a neighborhood of zero, we obtain for c sufficiently small that

$$\lim_{n\to\infty} s_n(c) = f(c).$$

So

$$f(c) = \sum_{i=0}^{\infty} c^i tr(\alpha^i)$$

is the Taylor series expansion for $f(c)$ in a neighborhood of the origin. But f is an entire function. So it follows from a well known theorem of complex analysis that the series describes $f(c)$ and converges for all c. In particular,

$$\lim_{n\to\infty} tr(\alpha^n) = 0$$

and this holds for all $\alpha \in J(\mathbf{C}G)$.

We now conclude the proof by showing that if $J(\mathbf{C}G) \neq \{0\}$ then there exists an element $\alpha \in J(\mathbf{C}G)$ that does not satisfy the foregoing; hence yielding a contradiction. Indeed, suppose $0 \neq \beta \in J(\mathbf{C}G)$. Let $\beta = \sum c_g g$ and let $\overline{\beta} = \sum \overline{c_g} g^{-1}$. Further let $\|\beta\| = \sqrt{\sum |c_g|^2}$. Put

$$\alpha = \frac{1}{\|\beta\|^2}(\beta\overline{\beta}).$$

Then $\alpha \in J(\mathbf{C}G)$. Furthermore $\alpha = \overline{\alpha}$ and

$$tr(\alpha) = \|\beta\|^{-2} tr(\beta\overline{\beta}) = \|\beta\|^{-2}\|\beta\|^2 = 1.$$

Now also $\alpha^m = \overline{\alpha^m}$ for any positive integer m. So for all such m we get

$$\begin{aligned} tr(\alpha^{2^{m+1}}) &= tr(\alpha^{2^m}\overline{\alpha^{2^m}}) \\ &= \|\alpha^{2^m}\|^2 \\ &\geq |tr(\alpha^{2^m})|^2. \end{aligned}$$

Hence, by induction

$$tr(\alpha^{2^m}) \geq 1$$

for all $m \geq 0$. But this contradicts the fact that $tr(\alpha^{2^m}) \to 0$. Thus $J(\mathbf{C}G) = \{0\}$. $\square$

Some of the best known results to date are the following.

Theorem 2.4.7. *(Amitsur) Let K be a field of characteristic zero that is not algebraic over $\mathbf{Q}$ then $J(KG) = \{0\}$ for all groups G.*

Theorem 2.4.8. *(Passman) Let K be a field of characteristic $p > 0$ that is not algebraic over its prime subfield. If G is a group without elements of order p then $J(KG) = \{0\}$.*

2.5 Semigroup Algebras

In this section we investigate when a semigroup algebra $K[S]$ is semisimple.

We first mention that Zelmanov (1977) proved the following result.

Theorem 2.5.1. *If a semigroup algebra $K[S]$ is right artinian, then S is finite. The converse holds if S is a monoid.*

This result was proved earlier for group algebras by Connell (1963).

If S is finite but not a monoid (or, more generally, $K[S]$ does not have a right identity), then $K[S]$ can have infinite descending chains of right ideals. For example this is the case if S has zero multiplication and $K = \mathbf{Q}$. Indeed in this case any subgroup containing $K\theta$ is an ideal. Since $\mathbf{Q}$ has an infinite descending chain of subgroups, we get an infinite descending chain of ideals in $K[S]$. So $K[S]$ is not artinian.

We now describe when a semigroup algebra is semisimple. By the previous the semigroup has to be finite and we also know that such an algebra necessarily contains an identity element.

We first need a few lemmas. Recall that an element a in a ring R is a right zero divisor if there exists $0 \neq b \in R$ with $ba = 0$. Similarly one defines left zero divisor.

Lemma 2.5.2. *Let R be a finite dimensional algebra over a field K. If $a \in R$ is not a right (resp. left) zero divisor, then R contains a right (resp. left) identity element e. Furthermore, in this case, there exists $x \in R$ with $ax = xa = e$.*

Proof. Assume a is not a right zero divisor. Let n be the least positive integer so that a, $a^2, \cdots, a^n$ are linearly dependent. It is clear that $n \geq 2$. So there exits $k_1, \ldots, k_n \in K$ so that

$$k_1 a + k_2 a^2 + \cdots + k_n a^n = 0,$$

and $k_n \neq 0$. Since a is a not a right zero divisor, and because of the minimality of n, we get that $k_1 \neq 0$. Let

$$e = -k_1^{-1}(k_2a + \cdots + k_na^{n-1}).$$

Then

$$ea = a.$$

Let $b \in R$. Then

$$(be - b)a = bea - ba = b(ea - a) = 0,$$

so that

$$be = b.$$

Thus e is a right identity for R.

Further,

$$\begin{aligned} & a\left(-k_1^{-1}(k_2e + k_3a + \cdots + k_na^{n-2})\right) \\ &= -k_1^{-1}(k_2ae + k_3a^2 + \cdots + k_na^{n-1}) \\ &= -k_1^{-1}\left(k_2(-k_1^{-1}(k_2a^2 + \cdots + k_na^n)) + k_3a^2 + \cdots + k_na^{n-1}\right) \\ &= -k_1^{-1}\left(k_2(-k_1^{-1})(-k_1a) + k_3a^2 + \cdots + k_na^{n-1}\right) \\ &= -k_1^{-1}(k_2a + k_3a^2 + \cdots + k_na^{n-1}) \\ &= e \end{aligned}$$

and

$$\begin{aligned} -k_1^{-1}(k_2e + k_3a + \cdots + k_na^{n-2})a &= -k_1^{-1}(k_2a + \cdots + k_na^{n-1}) \\ &= e. \end{aligned}$$

So this proves the result. □

Corollary 2.5.3. *Let R be a finite dimensional algebra over a field K. If $a \in R$ is neither a left nor a right zero divisor, then R contains an identity element e, and a is a unit (i.e. $ax = xa = e$ for some $x \in R$.*

Proof. This follows at once from Lemma 2.5.2 and the fact that if R has a left and right identity then R has an identity (equal to this left and right identity). □

Corollary 2.5.4. *Let R be a finite dimensional algebra over a field K and n a positive integer. If $P \in M_n(R)$ is neither a left nor a right zero divisor in $M_n(R)$, then R has an identity and P is invertible.*

Proposition 2.5.5. *Let R be a finite dimensional algebra over a field K and let $P \in M_{n,m}(R)$ (n and m positive integers).*

1. *If $n > m$ then there exists a nonzero matrix $A \in M_{m,n}(R)$ so that $A \circ P = 0$.*

2. *If $m > n$ then there exists a nonzero matrix $B \in M_{m,n}(R)$ so that $P \circ B = 0$.*

Proof. We only prove the case $n > m$. Let

$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix}$$

with $P_1 \in M_m(R)$ and $P_2 \in M_{n-m,m}(R)$. If P_1 is a right zero divisor in $M_m(R)$, then there exists $0 \neq A_1 \in M_m(R)$ with $A_1 \circ P_1 = 0$. Let then $A = (A_1\ 0)$. It follows that $A \circ P = 0$.

If P_1 is not a right zero divisor in $M_m(R)$, then by Lemma 2.5.2 the algebra $M_m(R)$ contains a right identity element E and

$$P_1 \circ Q_1 = Q_1 \circ P_1 = E$$

for some $Q_1 \in M_m(R)$. Let

$$A = (-A_2 \circ P_2 \circ Q_1 \quad A_2),$$

with $0 \neq A_2 \in M_{m,n-m}$. Then

$$A \circ P = -A_2 \circ P_2 \circ Q_1 \circ P_1 + A_2 \circ P_2 = -A_2 \circ P_2 \circ E + A_2 \circ P_2 = 0,$$

because $A_2 \circ P_2 \in M_m(R)$ and E is a right identity in $M_m(R)$. □

Lemma 2.5.6. *Let R be a finite dimensional algebra over a field K. Then the following conditions are equivalent for any algebra of matrix type $\hat{R} = \mathcal{M}(R, I, M, P)$:*

1. *$\hat{R}$ has an identity,*

2. *I, M are finite sets of the same cardinality, and P is an invertible matrix in $M_{|I|}(R)$.*

Furthermore, if these conditions are satisfied, then the mapping

$$\hat{R} \to M_{|I|}(R) : A \mapsto A \circ P$$

is an isomorphism of algebras.

Proof. Suppose E is an identity of $\hat{R}$. Then

$$AE = A \circ P \circ E = A$$

and

$$EA = E \circ P \circ A = A$$

for all $A \in \hat{R}$. This implies that the nonzero rows of A can only be those for which E has nonzero rows. Since E has only finitely many nonzero rows it follows that $|I| = n < \infty$. Similarly $|M| = m < \infty$. We claim $n = m$. Indeed, for if $n > m$ then by Lemma 2.5.2 there exists a nonzero $A \in M_{m,n}(R)$ with $A \circ P = 0$, which contradicts with $A \circ P \circ E = A$. Similarly $n < m$ leads to a contradiction with $E \circ P \circ A = A$.

¿From the above mentioned equalities it also follows that P is not a left nor a right zero divisor in $M_n(R)$. So by Corollary 2.5.4, R contains an identity element and P is invertible in $M_n(R)$.

Conversely, assume that condition (2) hold. Let P^{-1} be the inverse of P in $M_n(R)$. Then

$$AP^{-1} = A \circ P \circ P^{-1} = A$$

and

$$P^{-1}A = P^{-1} \circ P \circ A = A,$$

for all $A \in \hat{R}$. Thus P^{-1} is the identity in $\hat{R}$.

Assume $\hat{R}$ has an identity and let P^{-1} be the inverse of P in $M_n(|I|)$. Consider the following mapping:

$$f : \hat{R} \to M_{|I|}(R) : A \mapsto A \circ P.$$

Clearly $f(A + B) = f(A) + f(B)$ and

$$f(AB) = f(A \circ P \circ B) = A \circ P \circ B \circ P = f(A) \circ f(B),$$

for all $A, B \in \hat{R}$. It follows that f is an algebra homomorphism. Since P is invertible in $M_n(R)$ it follows easily that this mapping is bijective, and hence is an isomorphism. □

Proposition 2.5.7. *Let R be a finite dimensional algebra over a field K. Then the following conditions are equivalent for any algebra of matrix type $\hat{R} = \mathcal{M}(R, I, M, P)$:*

1. *$\hat{R}$ is semisimple,*
2. *$|I| = |M| < \infty$, P is invertible in $M_n(R)$ and R is semisimple.*

Proof. If $\hat{R}$ is semisimple then $\hat{R}$ contains an identity. So $|I| = |M| < \infty$ and $\hat{R} \cong M_n(R)$. It is well known $J(M_n(R)) = M_n(J(R))$. Hence $M_n(R)$ is semisimple if and only of R is semisimple. The result now follows. □

Lemma 2.5.8. *Let $S = \mathcal{M}^0(G^0, I, M, P)$ be a semigroup of matrix type, with G a finite group. Then the following conditions are equivalent:*

1. *$K_0[S]$ has an identity,*
2. *I, M are finite sets of the same cardinality, and P is an invertible matrix in $M_{|I|}(K[G])$.*

Proof. Because of the previous results it is sufficient to show that

$$K_0[S] \cong \mathcal{M}(K[G], I, M; P).$$

For this define the mapping

$$f : S \to \mathcal{M}(K[G], I, M; P)$$

by

$$f((g, i, m)) = (a_{jn}),$$

where $a_{jn} = g$ if $j = i$, $n = m$, and , otherwise $a_{jn} = 0$. From the definitions, it follows that f is a homomorphism into the multiplicative semigroup of the algebra $\mathcal{M}(K[G], I, M; P)$. Since the images of the nonzero elements of S are linearly independent, it is clear that the extension of f to a homomorphism of K-algebras $K_0[S] \to \mathcal{M}(K[G], I, M; P)$ is an isomorphism. □

Corollary 2.5.9. *Let $S = \mathcal{M}^0(G^0, I, M, P)$ be a semigroup of matrix type, with G a finite group, and let K be a field. Then, $K_0[S]$ is semisimple if and only if $K[G]$ is semisimple, $|I| = |M| < \infty$ and P is invertible in $M_n(K[G])$.*

Proof. We know that $K_0[S] \cong \mathcal{M}^0(G^0, I, M, P)$. Therefore the result follows from Proposition 2.5.7. □

Lemma 2.5.10. *Let R be a ring and I an ideal in the semigroup S. Then $K_0[S/I] \cong K[S]/K[I]$.*

Proof. It is easily verified that the natural mapping $K[S] \to K_0[S/I]$ is a ring epimorphism with kernel $K[I]$. Hence the result follows. □

Theorem 2.5.11. *Let K be a field and S a finite semigroup. Then $K[S]$ is semisimple if and only if S has a series of ideals*

$$S_0 = \emptyset \subseteq S_1 \subseteq \cdots \subseteq S_n = S,$$

with each factor $S_i/S_{i-1} \cong \mathcal{M}^0(G_i, n_i, n_i, P_i)$ a completely 0-simple square matrix semigroup with G_i a finite group so that $char(K) \not| |G_i|$ and P_i is invertible in the matrix ring $M_{n_i}(K[G])$.

Proof. We first show that if a finite dimensional K-algebra R has subalgebras R_i so that

$$R = R_1 \supseteq R_2 \supseteq \cdots \supseteq R_{n+1} = \{0\}$$

with each R_i an ideal in R_{i+1}, then R is semisimple if and only if each factor R_{i+1}/R_i is semisimple. By induction it is sufficient to show this result for $n = 2$.

So suppose $n = 2$, $R_3 = \{0\}$ and R_2 and R_1/R_2 are semisimple. If N is a nilpotent ideal of R, then $N + R_2 = R_2$, as R_1/R_2 is semiprime. So $N \subseteq R_2$. Since R_2 is semiprime and N is a nilpotent ideal in R_2, it

follows that $N = \{0\}$. Hence R is semiprime and finite dimensional. So R is semisimple.

Conversely, if R is semisimple, then by the Wedderburn-Artin theorem

$$R = I_1 \oplus \cdots \oplus I_k,$$

the direct product of simple rings R. Then, $R_2 = I_{j_1} \oplus \cdots \oplus I_{j_l}$ and $R_1/R_2 \cong I_{j_1} \oplus \cdots \oplus I_{j_n}$. So both R_2 and R_1/R_2 are semisimple.

Now, form the structure theorem of finite semigroups we know that S has a series of ideals

$$S_0 \subseteq S_1 \subseteq \cdots \subseteq S_n = S,$$

with $S_0 = \emptyset$ or $S_0 = \{\theta\}$, and each Rees factor S_{i+1}/S_i is null or completely 0-simple. So, in the latter case, $S_{i+1}/S_i \cong \mathcal{M}^0(G^0, n, m; P)$ (G a finite group). With this corresponds a series of ideals in $K[S]$:

$$\{0\}K[S_0] \subseteq K[S_1] \subseteq \cdots \subseteq K[S_n] = K[S].$$

By Lemma 2.5.10, if $S_{i+1}/S_i \cong \mathcal{M}^0(G^0, n, m; P)$ then $K[S_{i+1}]/K[S_i] \cong K_0[S_{i+1}/S_i]$. So, by the first part of the proof, $K[S]$ is semisimple if and only if there are no null factors and each $K_0[S_{i+1}/S_i]$ is semisimple. The result now follows from Corollary 2.5.9 and Maschke's theorem. □

2.6 Crossed Products

For some classes of infinite groups one can reduce problems of their group algebras to problems of group algebras of some "nicer" subgroups and crossed products (or graded rings) of finite groups.

Recall that we denoted by $T = R * G$ a crossed product of a group G over a ring R. Note that T is a G-graded ring,

$$T = \oplus_{g \in G} T_g \text{ with } T_g = R\overline{g}.$$

It is easily seen that each $\overline{g}$ is a unit in T. Conversely any G-graded ring $T = \oplus_{g \in G} T_g$ that contains a unit in each T_g is a crossed product.

We first show that group algebras easily yield examples of crossed products.

Lemma 2.6.1. *Let N be a normal subgroup in a group G and let K be a field. Then*

$$KG \cong (KN) * (G/N),$$

a crossed product of the group G/N over the ring KN.

Proof. Let $R = KN$ and $H = G/N$. For each $h \in H$ let $\overline{h} \in G$ be a fixed inverse image. Then, since $G = \cup_{h \in H} N\overline{h}$,

$$KG = \oplus_{h \in H} (KN)\overline{h}.$$

Furthermore

$$(KN)\overline{h_1}(KN)\overline{h_2} = (KN)\overline{h_1h_2}.$$

Thus KG is a H-graded ring with homogeneous components $(KN)\overline{h}$, $h \in H$. Since each $\overline{h}$ is invertible we get that indeed $KG = (KN) * H$, a crossed product. $\square$

Thus the lemma relates problems of KG to problems of group algebras of subgroups and crossed products.

Recall that a group G is polycyclic-by-finite if it has a sugroup of finite index that is polycyclic. If $\{1\} = G_0 \lhd G_1 \lhd \cdots G_n = G$ is a subnormal series with G_{i+1}/G_i either finite or cyclic, then $\{1\} \lhd G_1 \cap H \lhd \cdots G_n \cap H = H$ is a subnormal series of H and

$$G_{i+1} \cap H/G_i \cap H \cong (H \cap G_{i+1})G_i/G_i \subseteq G_{i+1}/G_i,$$

so these factors are also finite or cyclic. In particular, if G is poly-infinite cyclic, then so is H.

Lemma 2.6.2. *Let G be a finitely generated group and $n \geq 1$ an integer. Then G has only finitely many subgroups of index at most n.*

Proof. Let H be a subgroup of G of index $m \leq n$. Then G permutes the right cosets of H by right multiplication. So we obtain a homomorphism

$$\sigma : G \to S_m \subseteq S_n.$$

Clearly, $\ker(\sigma) \subseteq H$. Thus $H = \sigma^{-1}(W)$ for some subgroup W of S_n. Now there are only finitely many possible subgroups W and there are only finitely many possible maps σ (because σ is determined by the images of the finite number of generators of G). Thus there are only finitely many possibilities for H. $\square$

Lemma 2.6.3. *A group G is polycyclic-by-finite if and only if G has a subnormal series with factors either finite or cyclic. Moreover, in this case, G has a characteristic subgroup of finite index that is poly-infinite cyclic.*

Proof. We first note the following. Suppose L is a group, N is a finite normal subgroup of L, and L/N is infinite cyclic. If $L = \langle N, x\rangle$, then, for some $t \geq 1$, x^t centralises both N and x (as conjugation by x defines an automorphism of finite order on N). Therefore x^t is central in L. So $\langle x^t\rangle$ is a normal infinite cyclic subgroup of L with $[L : \langle x^t\rangle] < \infty$.

Now let $\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ be a given subnormal series for G with quotients that are either cyclic or finite. We show, by induction on i, that G_i has a characteristic subgroup H_i of finite index that is poly-infinite cyclic. This is trivial for $i = 0$.

Suppose now that H_i exists. Because $G_i \lhd G_{i+1}$ and H_i is characteristic in G_i, we get that $H_i \lhd G_{i+1}$. We first show that G_{i+1} has a normal poly-infinite cyclic subgroup of finite index. This is clear if G_{i+1}/G_i is finite. Thus we may assume that that this quotient is infinite cyclic. Then $L = G_{i+1}/H_i$ has a finite normal subgroup $N = G_i/H_i$ with $L/N \cong G_{i+1}/G_i$ infinite cyclic. Thus by the foregoing remark, L has a normal infinite cyclic subgroup of finite index. The inverse image in G_{i+1} of this group is then a normal poly-infinite cyclic subgroup of G_{i+1} of finite index.

Suppose M is this subgroup of G_{i+1} of finite index which is poly-infinite cyclic. Because G_{i+1} is a finitely generated group, it follows from Lemma 2.6.2 that G_{i+1} has only finitely many subgroups of index equal to $[G_{i+1} : M]$. Let H_{i+1} be their intersection. Then it follows easily that H_{i+1} is a characteristic subgroup of G_{i+1} of finite index. Furthermore, as a subgroup of a poly-infinite cyclic group, H_{i+1} is itself poly-infinite cyclic. Hence this induction step is proved. Because $G = G_n$, the result follows. □

So to study the Jacobson radical of group algebras of polycyclic-by-finite groups we should investigate crossed products of finite groups and (Laurent) polynomial rings.

We begin with a classical version of Maschke's Theorem.

Theorem 2.6.4. *Let G be a finite group and $R * G$ a crossed product. Let $W \subseteq V$ be $R * G$ submodules with no $|G|$-torsion and let $V = W \oplus U$, where U is a complementary R-submodule. Then there exists an $R * G$-submodule U' of V so that $V|G| \subseteq W \oplus U'$.*

Proof. First we show that G permutes the R-submodules of V. Indeed, let U be an R-submodule of V and $g \in G$. Then $U\overline{g}$ is an R-submodule isomorphic with the conjugate module U^{σ_g}. The latter is the module with underlying set U but with multiplication defined by

$$ur = u\sigma_g(r),$$

for $u \in U$ and $r \in R$.

Now $V = W \oplus U$. Then for all $g \in G$,

$$V = W\overline{g} \oplus U\overline{g} = W \oplus U\overline{g}$$

and let

$$\pi_g : V \to W$$

be the natural R-homomorphism defined by this decomposition. If $v = w + u\overline{g}$, then $v\overline{h} = w\overline{h} + u\overline{g}\overline{h}$. So

$$\pi_{gh}(v\overline{h}) = w\overline{h} = \pi_g(v)\overline{h}.$$

It follows that $\pi = \sum_{g\in G} \pi_g : V \to W$ is an $R * G$-homomorphism because

$$\begin{aligned} \pi(v\overline{h}) &= \sum_{g\in G} \pi_g(v\overline{h}) \\ &= \sum_{g\in G} \pi_{gh}(v\overline{h}) \\ &= \sum_{g\in G} \pi_g(v)\overline{h} \\ &= \pi(v)\overline{h} \end{aligned}$$

for all $v \in V$ and $h \in G$. Set $U' = \ker(\pi)$. Then U' is an $R * G$-submodule of V.

Now if $w \in W$, then $\pi(w) = w|G|$. Thus, $W \cap U' = \{0\}$ because V has no $|G|$-torsion. Finally, if $v \in V$, then $v|G| - \pi(v) \in \ker(\pi)$ and hence $v|G| \in W \oplus U'$, as required. □

Lemma 2.6.5. *(Nakayama) Let R be a ring and V a finitely generated right R-module. If $V = VJ(R)$ then $V = \{0\}$.*

Proof. Suppose $v_1, \cdots, v_n$ are generators for V as an R-module. Then $v_n \in VJ(R)$. Thus

$$v_n = v_1 r_1 + \cdots v_n r_n$$

with $r_i \in J(R)$. Hence

$$v_n = \sum_{i=1}^{n-1} v_i r_i (1 - r_n)^{-1}.$$

Consequently, V is generated by $v_1, \cdots, v_{n-1}$. Continuing this way obtain that $V = \{0\}$. □

Let $R \subseteq S$ be rings with the same 1. If $M = M_S$ is a right S-module, we let $M_{|R}$ denote the module M but considered as right R-module.

If V_R is a right R-module, we let $V^{|S}$ denote the induced S-module

$$V^{|S} = V_R \otimes_R S.$$

The S-module structure on the latter module is given by

$$(v \otimes s)t = v \otimes st$$

for all $v \in V$ and $s, t \in S$.

We give some elementary properties.

Lemma 2.6.6. *Let $R \subseteq S$ be rings. The following properties hold.*

1. *If V_R is finitely generated, then so is $V^{|S}$.*
2. *Induction commutes with direct sums.*
3. *$R^{|S} \cong S$ and hence if V_R is projective or free, then so is $V^{|S}$.*
4. *If M is an S-module, then there is an S-module epimorphism*
$$(M_{|R})^{|S} \to M : m \otimes s \mapsto ms.$$
5. *If $S \subseteq T$ and V is an R-module, then*
$$(V^{|S})^{|T} \cong V^{|T}.$$

Note that if R is the ring of integers and S the rationals, then for any periodic abelian group V, $V_R \neq \{0\}$ but $V^{|S} = \{0\}$.

Lemma 2.6.7. *Let $S = R * G$ be a crossed product and V an R-module. Then*
$$V^{|S} = \oplus_{g \in G} V \otimes \overline{g}$$
is an R-module direct sum with $V \otimes \overline{g} \cong V^{\sigma_g}$.

Proof. Since S is a free left R-module with basis $\overline{G}$ we have $V^{|S} = V \otimes R = \oplus_R V \otimes_R (R * G) = \oplus_{g \in G} V \otimes \overline{g}$, a direct sum of additive abelian groups. Furthermore, for $v \in V$, $g \in G$ and $r \in R$,
$$(v \otimes \overline{g})r^{\sigma_{g^{-1}}} = v \otimes (\overline{g} r^{\sigma_{g^{-1}}}) = v \otimes (r\overline{g}) = (vr) \otimes \overline{g}.$$
Hence
$$(v \otimes \overline{g})r = (vr^{\sigma_g}) \otimes \overline{g}.$$
So $V \otimes \overline{g}$ is an R-module isomorphic with V^{σ_g}. □

Theorem 2.6.8. *Let $R*G$ be a crossed product with G a finite group. Then*
$$J(R * G)^{|G|} \subseteq J(R) * G \subseteq J(R * G).$$
Furthermore if $|G|^{-1} \in R$, then $J(R * G) = J(R) * G$.

Proof. Let V be an irreducible $R * G$-module. Then V is a cyclic $R * G$-module and hence $V_{|R}$ is finitely generated. It follows from Nakayama's Lemma that $VJ(R)] \neq V$. But it is easily verfied that $VJ(R)$ is a $R * G$-submodule of V, so $VJ(R) = \{0\}$. Hence $J(R) \subseteq J(R * G)$ and thus $J(R) * G \subseteq J(R * G)$.

For the other inclusions, let W be an irreducible R-module and form the induced $R*G$-module $V = W^{|R*G}$. By Lemma 2.6.7, $V_{|R} = \oplus_{g \in G} W \otimes \overline{g}$, the direct sum of $n = |G|$ irreducibles R-submodules. Thus V has composition

length at most n and $VJ(R*G)^n = \{0\}$. Now let $\alpha = \sum_{g\in G} r_g\overline{g} \in J(R*G)^n$. Then for any $w \in W$,

$$0 = (w \otimes 1)\alpha = \sum_{g\in G} wr_g \otimes \overline{g}.$$

So $wr_g = 0$ and $Wr_g = 0$. Since this holds for all W, we have that $r_g \in J(R)$. Hence $J(R * G)^n \subseteq J(R) * G$.

Finally, if $|G|^{-1} \in R$, then since $V_{|R}$ is completely reducible it follows from Theorem 2.6.4 that V is completely reducible. Hence, in this case $VJ(R*G) = \{0\}$ for all W. The above argument then yields that $J(R*G) \subseteq J(R) * G$. $\square$

Let K be a field. If G is a polycyclic-by-finite group and H is a poly-infinite cyclic normal subgroup of G, then $KG = (KH) * (G/H)$ is ring graded by the finite group G/H. If $|G/H|$ is invertible in K, then it follows from the above result that

$$J(KG) = J(KH) * (G/H).$$

Now H has a subnormal series

$$H_0 = \{1\} \lhd H_1 \lhd \cdots \lhd H_n = H$$

with $H_{i+1}/H_i \cong \langle X_i\rangle \cong \mathbb{Z}$ for every $0 \leq i \leq n-1$. Furthermore

$$KH_{i+1} \cong (KH_i) * (H_{i+1}/H_i) = \oplus_{j\in\mathbb{Z}}(KH_i)X_i^j$$

and conjugations by X_i defines an automorphism σ_i on KH_i. It follows that

$$KH_{i+1} \cong (KH_i)[X_i, X_i^{-1}, \sigma_i],$$

a skew Laurent polynomial ring. Now, consider a skew Laurent polynomial ring. In the next section we will prove that $J(R[X, X^{-1}, \sigma]) = \{0\}$ if $J(R) = \{0\}$. Hence the following result follows easily.

Corollary 2.6.9. *Let G be a polycyclic-by-finite group with a normal poly-infinite cyclic subgroup H of finite index. If $|G/H|$ is invertible in the field K then $J(KG) = \{0\}$.*

2.7 Polynomial rings and graded rings

Before handling the Jacobson radical of polynomial rings we consider a very useful and important result on the radical of a $\mathbb{Z}$-graded ring R. Recall that a ring R is graded by a group G if

$$R = \oplus_{g\in G} R_g$$

and

$$R_g R_h \subseteq R_{gh}$$

for all $g, h \in G$. An (left, right, two-sided) ideal I of R is said to be *graded* if

$$I = \oplus_{g \in G}(I \cap R_g),$$

that is, if $r_{g_1} + \cdots r_{g_n} \in I$ (with $r_{g_i} \in R_{g_i}$ and $g_i \neq g_j$ for $i \neq j$) then $r_{g_i} \in I$.

Lemma 2.7.1. *Let $R \subseteq S$ be an extension of rings.*

1. *If $S = R \oplus U$, where U is a complementary R-submodule of S, then $J(S) \cap R \subseteq J(R)$.*
2. *Suppose S is a finitely generated right R-module and that $J(R)S \subseteq SJ(R)$, then $J(R) \subseteq J(S)$.*
3. *If R is a G-graded ring and H is a subgroup of G, then $J(R) \cap R_H \subseteq J(R_H)$, where $R_H = \oplus_{h \in H} R_h$, an H-graded ring.*

Proof. (1) Suppose $r \in R$ has an inverse $s \in S$. Write $s = r' + u \in R \oplus U$. Then

$$1 = sr = r'r + ur$$

implies that $ur = 0$ and thus $u = 0$. Hence $s \in R$. It now follows that $J(S) \cap R$ is a quasi-regular ideal of R and hence is contained in $J(R)$.

(2) Let V be an irreducible S-module. Then $V_{|S}$ is cyclic and, since $S_{|R}$ is finitely generated, V is a finitely generated R-module. By Nakayama's Lemma, $VJ(R) \subset V$. In addition, $J(R)S \subseteq SJ(R)$ implies that $VJ(R)$ is an S-submodule of V. Thus, since V is irreducible, we have that $VJ(R) = \{0\}$. Hence $J(R) \subseteq J(S)$.

(3) Observe that

$$R = R_H \oplus R_{G \setminus H}$$

and thus

$$R_{G \setminus H} = \oplus_{g \in (G \setminus H)} R_g$$

is a complementary R_H-submodule of R. So (1) applies. □

Theorem 2.7.2. *(Bergman) Let R be a $\mathbb{Z}$-graded ring. Then $J(R)$ is a graded ideal and $J(R) \cap R_n$ is nilpotent for all $n \neq 0$.*

Proof. We first prove that $J(R)$ is graded. So let $r = r_{n_1} + \cdots + r_{n_k} \in J(R)$, with $r_{n_i} \in R_{n_i}$ and $n_i \neq n_j$ for $i \neq j$. We prove by induction on k (the number of nonzero terms of r) that $r_{n_i} \in J(R)$. If $k = 0$ or 1 then this is clear. So assume $k \geq 2$.

Choose a prime integer $p > |n_k - n_1|$ and form the ring extension $S = R[\xi]/(1 + \xi + \cdots + \xi^{p-1})$ of R. Let η denote the image of ξ in S. The η commutes with R and $1 + \eta + \cdots + \eta^{p-1} = 0$. Thus $\eta^p = 1$. Furthermore

$$S = R \oplus R\eta \oplus \cdots + R\eta^{p-2}.$$

So by Lemma 2.7.1

$$J(R) = J(S) \cap R.$$

Note that S is also $\mathbb{Z}$-graded with

$$S_i = R_i \oplus R_i\eta \oplus \cdots \oplus R_i\eta^{p-2}.$$

Thus $r = r_{n_1} + \cdots + r_{n_k} \in J(S)$ and r_{n_i} is also a homogeneous component of S.

Now the map

$$f : S \to S : s_i \mapsto s_i\eta^i,$$

for $s_i \in S_i$, defines an automorphism of S. Since $J(S)$ is a characteristic ideal of S, we get that

$$\sum_i r_{n_i}\eta^{n_i} = f(r) \in J(S).$$

Furthermore

$$s = \sum_i r_{n_i}\eta^{n_i} - \eta^{n_1}\sum_i r_{n_i} \in J(S)$$

and this element has less nonzero homogeneous terms than r. By induction we conclude that

$$s_{n_k} = (\eta^{n_k} - \eta^{n_1})r_{n_k} \in J(S).$$

So,

$$(1 - \eta^{(n_1 - n_k)})r_{n_k} \in J(S).$$

By the choice of p we know that p does not divide $n_1 - n_k$. It follows that

$$pr_{n_k} = \prod_{j=1}^{p-1}(1 - \eta^j)r_{n_k} \in J(S).$$

Therefore

$$pr_{n_k} \in J(S) \cap R = J(R).$$

Because the latter is true for at least two distinct primes p we get that

$$r_{n_k} \in J(R),$$

as required.

For the second part, let $r_m \in J(R) \cap R_m$ and assume for convenience that $m > 0$. Then $1 - r_m$ is invertible in R, with inverse $a = \sum_{i=k}^{k+l} a_i$, and say $a_k \neq 0$. Now the lowest degree term in

$$1 = (1 - r_m)a$$

is

$$1.a_k = a_k.$$

It follows that $k = 0$ and $a_0 = 1$. Furthermore, because

$$r_m a_i = a_{i+m}$$

and because $a_0 = 1$ we conclude by induction that

$$a_{jm} = r_m^j.$$

Since $a_{jm} = 0$ for j large enough, it follows that r_m is nilpotent. $\square$

One can extend Bergman's result to any ring graded by a torsion free abelian group. So if R is a ring graded by a torsion free abelian group S then

$$J(R) = \oplus_{a \in A}(J(R) \cap R_a).$$

Furthermore for a ring R graded by a finite abelian group B one can show that

$$\text{if } \sum_{b \in B} r_b \in J(R), \text{ then } |B| r_b \in J(R),$$

for all $b \in B$.

For a ring R we denote by $P(R)$ the intersection of all prime ideals. Now $P(R)$ is a nil ideal. Indeed, suppose $r \in P(R)$ is not nilpotent. By Zorn's lemma there exits an ideal P maximal with respect to the condition that $P \cap \{r^n \mid n \in \mathbf{N}\} = \emptyset$. It follows easily that P is a prime ideal. However this yields a contradiction as $r \notin P$ and $r \in P(R)$.

Theorem 2.7.3. *$J(R[X]) = (J(R[X]) \cap R)[X]$ and*

$$J(R[X, X^{-1}]) = (J(R[X, X^{-1}]) \cap R)[X, X^{-1}].$$

Further $J(R[X]) \cap R = J(R[X, X^{-1}]) \cap R$. We denote the ideal $J(R[X]) \cap R$ by $J_1(R)$. For commutative rings, $J_1(R) = P(R)$.

Proof. Since a polynomial ring and a Laurent polynomial ring are $\mathbb{Z}$-graded, it follows from Bergman's result that the Jacobson radical of $J(R)[X]$ and $J(R[X, X^{-1}])$ are homogeneous for this gradation. Now let $\psi : R[X] \to R[X]$ be the R-linear ring automorphism defined by $X \mapsto X + 1$. Then

$$\psi(J(R[X])) = J(R[X]).$$

Hence if $rX^n \in J(R[X])$, then also

$$r(X + 1)^n \in J(R[X]).$$

Again by Bergman's result we therefore obtain $r \in J(R[X]) \cap R$. So it follows that

$$J(R[X]) \subseteq (J(R)[X] \cap R)[X].$$

The converse inclusion is obvious. It also follows from Bergman's result that $(J(R[X]) \cap R)X$ consists of nil elements. Hence the ideal $J(R[X]) \cap R$ is a nil ideal of R.

Similarly one proves that $J(R[X, X^{-1}]) = (J(R[X, X^{-1}]) \cap R)[X, X^{-1}]$.

Now, because $X^2 = (X + X^{-1})X - 1$

$$R[X, X^{-1}] = R[X + X^{-1}] + R[X + X^{-1}]X.$$

So $R[X, X^{-1}]$ is a free $R[X+X^{-1}]$-module with basis $\{1, X\}$, two central elements. Furthermore $R[X+X^{-1}] \cong R[Y]$, a polynomial ring in one variable. Because of Lemma 2.7.1,

$$J(R[X, X^{-1}]) \cap R[X + X^{-1}] = J(R[X + X^{-1}]).$$

By the above we therefore obtain that

$$\big(J(R[X, X^{-1}]) \cap R\big)\, [X, X^{-1}] \cap R[X+X^{-1}] = (J(R[X+X^{-1}]) \cap R)[X+X^{-1}].$$

Thus

$$J(R[X, X^{-1}]) \cap R = J(R[X + X^{-1}]) \cap R = J(R[X]) \cap R.$$

Finally, if R is a commutative ring, then $P(R)$ is a sum of nilpotent ideals. Hence $P(R)[X]$ is a sum of nilpotent ideals and thus contained in $J(R[X])$. Hence $P(R) \subseteq J_1(R)$. Since $J_1(R)$ is a nil ideal we get $P(R) = J_1(R)$. $\square$

With a bit of work one can extend the result as follows.

Corollary 2.7.4.

$$J(R[X_1, \cdots, X_n]) = J_n(R)[X_1, \cdots X_n]$$

where $J_n(R) = J(R[X_1, \cdots, X_n]) \cap R$ *(and* n *is finite or infinite). Moreover,*

$$J(R) = J_0(R) \supseteq J_1(R) \supseteq J_2(R) \supseteq \cdots \supseteq J_\infty(R) = \cap_{n=0}^{\infty} J_n(R),$$

and if n *is infinite then* $J_n(R) = J_\infty(R)$*. Moreover* $J_1(R)$ *is a nilideal.*

One also has the following.

Corollary 2.7.5.

$$J(R[X_1, X_1^{-1}, \cdots, X_n, X_n^{-1}]) = J_n(R)[X_1, X_1^{-1}, \cdots X_n, X_n^{-1}].$$

For algebras R over a non-denumerable field, Amitsur has shown that $J_1(R)$ is the largest nil ideal $N(R)$ (that is, the sum of all nil ideals). In general one does not have a description for $J_1(R)$. Actually, Krempa has shown that "$J_1(R) = N(R)$ for all rings R" is equivalent with

Problem 2: *the Koethe conjecture:* if a ring R contains a one-sided nil ideal L, then $L \subseteq N(R)$.

In case R is noetherian, then this conjecture holds.
Krempa showed the following nice result.

Theorem 2.7.6. *The following conditions are equivalent:*

1. *the Koethe conjecture holds;*
2. *the sum of two nil left ideals is necessarily nil;*
3. $N(M_n(R)) = M_n(N(R))$ *for all rings* R *and for all* n*;*
4. $J(R[X]) = N(R)[X]$ *for all rings* R*.*

In 1981, Beidar constructed an example of a finitely generated algebra over a field for which the Jacobson radical and the nil radical are different. In 1979, Amitsur and Krempa posed the question whether $R[X]$ necessarily is a nil ring if R is a nil ring. Only in 1999, Agata Soktunowicz constructed an example that gave a negative answer to this question. In 2000, Puczylowski and Somktunowicz constructed a ring R so that $R[X]$ is not nil but $R[X]$ is Jacobson.

This result on the Jacobson radical of polynomial rings and Laurent polynomial rings can be generalised to a description of the Jacobson radical of the semigroup ring of any subsemigroup of an abelian group without nontrivial periodic elements. Using this one can obtain a description of $J(R[S])$ for any commutative semigroup S.

The same techniques as use above can also be applied to, for example, skew polynomial rings. This was done by Bedi and Ram.

Chapter 3

Noetherian Characterization Problem

A problem of general interest is to construct many classes of Noetherian rings. In this chapter we look at Noetherian group algebras.

3.1 Group Algebras

In this section we investigate when a group algebra KG is noetherian.

We first note that for group algebras, left and right noetherian are equivalent.

Lemma 3.1.1. *Let K be a field and G a group. The K-linear mapping*

$$* : K[G] \to K[G] : \alpha \mapsto \alpha^*$$

defined by

$$g^* = g^{-1} \quad (\textit{for } g \in G)$$

is an involution. It follows that $K[G]$ is left noetherian if and only if $K[G]$ is right noetherian.

Proof. Clearly $(gh)^* = h^*g^*$ and hence it follows easily that the mapping $*$ is an involution. It follows that a subset L of $K[G]$ is a left ideal if and only if L^* is a right ideal. Furthermore, if L_1, L_2 are left ideals of $K[G]$ then $L_1 \subseteq L_2$ if and only if $L_1^* \subseteq L_2^*$. Hence the last statement follows. □

To deal with the Noetherian property of skew polynomial rings, we prove the following more general property.

Proposition 3.1.2. *(Generalised Hilbert Basis Theorem) Suppose that a ring T is generated (as a ring) by a subring R and an element a so that $R + aR = R + Ra$. If R is left Noetherian then also T is left Noetherian.*

Proof. Let L be a left ideal of T. We have to show that L is finitely generated as a left T-module. Define, for each integer $n \geq 0$,

$$L_n = \{r \in R \mid \text{ there exists } w(r) = \sum_{i=0}^{n} a^i r_i \in L, \text{ each } r_i \in R \text{ and } r_n = r\}.$$

Because $R + aR = R + Ra$ it is easily verified that each L_n is a left ideal. Indeed,

$$R + aR + \cdots + a^n R = R + Ra + \cdots + Ra^n$$

and thus, with notations as in the definition of L_n, for $r' \in R$,

$$a^n r' = b_0 + b_1 a + \cdots + b_n a^n,$$

with all $b_i \in R$. Hence

$$b_n w(r) = b_n(w(r) - a^n r) + b_n a^n r.$$

Now $b_n(w(r) - a^n r) \in R + aR + \cdots + a^{n-1}R$ and

$$b_n a^n r = (a^n r' - b_0 - \cdots - b_{n-1}a^{n-1})r.$$

Thus

$$b_n a^n r = a^n r' r + \alpha$$

with $\alpha \in R + aR + \cdots + a^{n-1}R$. So it indeed follows that $r'r \in L_n$, and thus L_n is a left ideal.

So we obtain an ascending chain of left ideals of R,

$$L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots$$

Because R is left Noetherian we get that, for some n,

$$L_i = L_{i+1}$$

for all $i \geq n$. Write

$$L_i = \sum_{j=1}^{t(i)} Rs_{ij}$$

and let

$$L' = \sum_{i=0}^{n} \sum_{j=1}^{t(i)} Tw(s_{ij}),$$

where $w(s_{ij}) \in T$ is such that it "leading coefficient" is s_{ij}. So

$$L' \subseteq L.$$

We now show that $L' = L$, and thus L is finitely generated. For this we show by induction on k that if $w = \sum_{u=0}^{k} a^u r_u \in L$ (with all $r_u \in R$) then $w \in L'$. First suppose $k \leq n$. Write $r_k = \sum_j r_{kj} s_{kj}$. Note that

$$a^k r_{kj} \in r'_{kj} a^k + \sum_{v,\, v<k} a^v R$$

for suitable $r'_{kj} \in R$. Thus

$$w - \sum_j r'_{kj} w(s_{kj}) \in L$$

and has "degree" less than k. Hence this element is in L' by induction on k. Thus $w \in L'$.

Hence we may assume $k > n$. Now $r_k \in L_k = L_n$. As in the previous paragraph r_k appears as the "leading coefficient" of an element $w' \in L'$ of degree n. Thus r_k is the "leading coefficient" of $a^{k-n}w'$, and $w - a^{k-n}w'$ has "degree" less than k. By induction $w - a^{k-n}w' \in L'$. So $w \in L'$. □

Proposition 3.1.3. *If R is a left noetherian ring and σ an automorphism of R,. Then the skew polynomial ring $R[X, \sigma]$ and the skew Laurent polynomial ring $R[X, X^{-1}, \sigma]$ are also left noetherian.*

Proof. Since $RX = XR$ the first part follows at once from Proposition 3.1.2. For the second part. Let L be a left ideal of $R[X, X^{-1}, \sigma]$. Then

$$L = R[X, X^{-1}, \sigma](L \cap R[X, \sigma]).$$

Since $L \cap R[X, \sigma]$ is a finitely generated left $R[X, \sigma]$-module we get that L is a finitely generated left $R[X, X^{-1}, \sigma]$-module. So the second statement follows. □

Corollary 3.1.4. *Let K be a field and G a polycyclic-by-finite group. Then a crossed product $K * G$ is left noetherian. In particular, a group algebra of a polycyclic-by-finite group is noetherian.*

Proof. Let H be a poly-infinite cyclic subgroup of finite index in G. Then $K * G$ is a finitely generated left $K * H$-module. So to prove the result it is sufficient to show that $K * H$ is a (left) Noetherian ring. In the previous section we have mentioned (for group rings, the proof for crossed products is similar) that

$$K * H \cong (K * A)[X, X^{-1}, \sigma]$$

where A is a normal subgroup of H, and A is poly-infinite cyclic but it has a subnormal series with less infinite cyclic factors than H. So by induction we get that $K * A$ is left Noetherian. Hence by Proposition 3.1.3, $K * H$ is Noetherian. □

Since group algebras of polyclic-by-finite groups are the only known noetherian group algebras one has the following question.

Problem 3 Characterise noetherian group algebras $K[G]$! Is G necessarily polycyclic-by-finite if $K[G]$ is noetherian?

Let us deduce some properties of noetherian group algebras. Let K be a field and H a group. Recall that we denote by

$$\omega(K[H])$$

the augmentation ideal of $K[H]$. That is, the ideal generated by the elements $h-1$ with $h \in H$.

Proposition 3.1.5. *If $K[G]$ is a noetherian group algebra then G has no infinite chain*

$$H_1 \subset H_2 \subset \cdots$$

of subgroups. In particular, G is finitely generated.

Proof. Consider the ascending chain of left ideals of $K[G]$:

$$K[G]\omega(K[H_1]) \subseteq K[G]\omega(K[H_2]) \subseteq \cdots$$

Since $K[G]$ is left Noetherian we get that, for some m,

$$K[G]\omega(K[H_n]) = K[G]\omega(K[H_{n+1}]),$$

for all $n \geq m$. Hence $h_{n+1} - 1 \in K[G]\omega(K[H_n])$. Now let

$$\pi_{H_n} : K[G] \to K[H_n]$$

defined by

$$\pi_{H_n}(\sum_{g\in G} k_g g) = \sum_{h_n \in H_n} k_{h_n} h_n.$$

Then π_{H_n} is an $K[H_n]$-left module morphism. Hence

$$\pi_{H_n}(h_{n+1} - 1) \in \pi_{H_n}(\omega(K[H_n])) = \omega(K[H_n]).$$

Since $-1 \notin \omega(K[H_n])$ we get that $h_{n+1} \in H_n$. Thus $H_n = H_{n+1}$, a contradiction. □

Lemma 3.1.6. *Let R be a subring of T and suppose that $T = R \oplus N$, for some right R-submodule N. Then, for any left ideal L of R, $R \cap TL = L$.*

Proof Clearly $L \subseteq (R \cap TL)$. Conversely, let

$$r = \sum t_i l_i \in TL \cap R,$$

with $t_i \in T$ and $l_i \in L$. Write $t_i = r_i + n_i$, with $r_i \in R$ and $n_i \in N$. So

$$r = \sum r_i l_i + \sum n_i l_i,$$

with $\sum r_i l_i \in L$ and $\sum n_i l_i \in N$. So $r = \sum r_i l_i \in L$. □

Proposition 3.1.7. *Let K be a field and G a solvable group. If $K[G]$ is noetherian, then G is polycyclic*

Proof. Take a subnormal series of G with each factor G_i/G_{i+1} abelian. Since $K[G]$ is a free right $K[G_i]$-module, we get from the previous lemma that also $K[G_i]$ is Noetherian. Hence $K[G_i/G_{i+1}]$ is Noetherian. By Proposition 3.1.5 we therefore get that the abelian group G_i/G_{i+1} is finitely generated. Hence each G_i/G_{i+1} is polycyclic. So G is polycyclic. □

We give a few more properties of polycyclic-by-finite groups and more generally of finitely generated groups. Recall that a subgroup H and a quotient group of a polycyclic-by-finite group G are again polycyclic-by-finite. Moreover, if G is poly-infinite-cyclic then so is H.

The infinite factors give an important invariant.

Also recall that in a finitely generated group G there are only finitely many subgroups of index n in G, for a given number n. In particular, any subgroup of finite index contains a characteristic subgroup of finite index.

Definition 3.1.8. *The Hirsch number $h(G)$ of a polycyclic-by-finite group G is the number of the infinite cyclic factors in a subnormal series each of whose factors is infinite cyclic or finite.*

Proposition 3.1.9. *Suppose G is polycyclic-by-finite. Then $h(G)$ is well-defined. Moreover, $h(G) = 0$ if and only if G is finite. If N is a normal subgroup of G, then*

$$h(G) = h(N) + h(G/N).$$

Proof. Suppose

$$\{1\} = G_m \lhd G_{m-1} \lhd \cdots \lhd G_1 \lhd G$$

and

$$\{1\} = H_n \lhd H_{n-1} \lhd \cdots \lhd H_1 \lhd G$$

are two subnormal series whose factors all are either finite or infinite cyclic. If all factors in one series are finite then G is a finite group, hence all factors in the other series are finite as well. So suppose G is not finite, that is, not all factors are finite.

Now let $k \geq 1$ be the smallest index so that $[G : G_k]$ is infinite. Similarly let $l \geq 1$ be the smallest index so that $[G : H_l]$ is infinite. Then consider the subgroup $D = G_k \cap H_l$.

Now G_k has subnormal series with the number of infinite cyclic factors one less than the number of infinite cyclic factors of the form G_i/G_{i+1}. Similarly H_l has subnormal series with the number of infinite cyclic factors one less than the number of infinite cyclic factors of the form H_i/H_{i+1}. So by induction on the number of cyclic factors we may assume that the Hirsch number is well defined for G_k and H_l. Furthermore, we have the series:

$$H_l \cap G_k = D \lhd H_{l-1} \cap G_k \lhd \cdots \lhd H_1 \cap G_k \lhd G_k,$$

and

$$D \lhd G_{k-1} \cap H_l \lhd \cdots \lhd G_1 \cap H_l \lhd H_l.$$

At most the last factors can be infinite cyclic. If they both are then

$$h(G_k) = h(D) + 1.$$

Similarly

$$h(H_l) = h(D) + 1.$$

It follows that the number of infinite cyclic factors in both series of G is the same. On the other hand if one of the factors, say $H_{l-1} \cap G_k/D$ is finite, as in Lemma 2.6.3 we can construct a series

$$D \lhd D_1 \lhd G$$

with D_1/D infinite cyclic and G/D_1 is finite. Hence for any $g \in G$ which is of infinite order modulo D we get that $\langle D, g\rangle$ is of finite index in G. So it follows that also the factor $G_{k-1} \cap H_l/D$ is finite. Thus in this case

$$h(G_k) = h(D) = h(H_l).$$

Hence the number of infinite cyclic factors in both series is

$$h(D) + 1.$$

To prove the last assertion one just has to put together the subnormal series of N and G/N. □

Definition 3.1.10. *A group G is residually finite if there is a set $\{N_i \mid i \in I\}$ of normal subgroups such that each G/N_i is finite and $\cap_{i\in I} N_i = \{1\}$.*

Proposition 3.1.11. *Any polycyclic-by-finite group G is residually finite.*

Proof. We know that G has a characteristic subgroup H that is poly-infinite cyclic. Then the second last subgroup A in the derived series of H is a characteristic subgroup of G that is torsion-free and abelian. So $A \neq \{1\}$. Let $A^i = \{a^i \mid a \in A\}$. Then

$$h(G/A^i) = h(G) - h(A^i) \leq h(G) - 1.$$

So, by induction, G/A^i is residually finite. Since $\cap A^i = \{1\}$ we conclude that G is residually finite. □

Of course one can extend the noetherian problem to more general ring constructions, such as semigroup algebras and graded rings. In both cases results have been obtained.

For example Chin and Quinn showed the following.

Theorem 3.1.12. *Let R be a ring graded by a polycyclic-by-finite group G and let $M = \oplus_{g\in G} M_g$ be a graded left R-module. That is, $R_{g_1} M_{g_2} \subseteq M_{g_1 g_2}$. Then M is left Noetherian if and only if M is graded left Noetherian, that is, M satisfies the ascending chain condition on graded submodules N (so $N = \oplus_{g\in G} M_g \cap N$).*

Corollary 3.1.13. *Let S be a submonoid of a polycyclic-by-finite group. Then $K[S]$ is right Noetherian if and only if S satisfies the ascending chain condition on right ideals. Moreover, in this case, S is finitely generated.*

In general, the following remains an unsolved problem.

Problem 4: Let S be an arbitrary semigroup. Is S necessarily finitely generated if the semigroup algebra $K[S]$ is right Noetherian.

Gilmer proved the following result.

Theorem 3.1.14. *Let S be an abelian monoid and K a field. Then the monoid algebra $K[S]$ is Noetherian if and only if S is finitely generated.*

In case $K[S]$ is left and right Noetherian then Okninski showed that Problem 4 also has an affirmative answer.

In the case of submonoids S of polycyclic-by-finite groups one can completely characterize when the semigroup algebra $K[S]$ is left and right Noetherian. This result was obtained recently by Jespers and Okninski.

Theorem 3.1.15. *Let S be a submonoid of a polycyclic-by-finite group. The following conditions are equivalent.*

1. *$K[S]$ is left and right Noetherian.*
2. *S satisfies the ascending chain condition on left and right ideals.*
3. *S has a group of quotients $G = \{st^{-1} \mid s, t \in S\}$ which contains a normal subgroup H of finite index and a normal subgroup $F \subseteq H$ such that $S \cap H$ is a finitely generated semigroup, $F \subseteq S$ and H/F is Abelian.*

Chapter 4

The zero divisor problem

4.1 Group Algebras

We consider the problem of when a group algebra $K[G]$ is a domain.

First we note the following.

Lemma 4.1.1. *Let G be a group and K a field. If $K[G]$ is a domain, then G is torsion-free, that is, every non-trivial element of G has infinite order.*

Proof. Let $g \in G$ be an element of finite order n. Then,

$$0 = 1 - g^n = (1 - g)(1 + g + \cdots + g^{n-1}).$$

Since $K[G]$ is a domain, we get that $1 - g = 0$ or $1 + g + \cdots + g^{n-1} = 0$. The latter is impossible, because the order of g is n and thus $g^i \neq g^j$ for $1 \leq i, j \leq n - 1$ and $i \neq j$. Thus $1 - g = 0$ and so $1 = g$. Hence the only element of finite order in G is the identity. So G is torsion-free. □

So the problem is whether the converse holds.

Problem 5: Let K be a field. Is the group algebra of a torsion-free group a domain?

This problem has been tackled in several stages. The first step is the purely group theoretic approach. One may ask if the torsion-free assumption on G implies other properties of G which are more relevant to the zero divisor problem.

Definition 4.1.2. *A group G is said to have the unique product property if for any two non-empty finite subsets $A, B \subseteq G$ there is at least one uniquely represented element of the form ab with $a \in A$ and $b \in B$. One can show that any such group is a two unique product group, that is, there are two uniquely represented elements of the form ab (assuming $|A| + |B| > 2$)*

Examples of such groups are ordered groups.

Definition 4.1.3. *A group G is said to be an ordered group if the elements of G are linearly ordered with respect to a relation $<$ such that for all $g, h, x \in G$, $g < h$ implies that $xg < xh$ and $gx < hx$.*

It is an immediate consequence of the definition that if $g < h$ and $g' < h'$ then $gg' < hh'$. Indeed, $g < h$ implies that $gg' < hg'$ and $g' < h'$ implies that $hg' < hh'$. The transitivity of $<$ now yields the result.

An important subset of such a group is the so-called *positive cone*, namely

$$P = P(G) = \{g \in G \mid 1 < g\}.$$

Lemma 4.1.4. *Let G be a group. If G is ordered with positive cone P, then P has the following properties.*

1. *P is a subsemigroup of G, that is, P is multiplicatively closed.*
2. *$G = P \cup \{1\} \cup P^{-1}$ is a disjoint union.*
3. *P is a normal subset of G, that is $g^{-1}Pg = P$ for all $g \in G$.*

Conversely, suppose G has a subset P satisfying these conditions. If we define $g < h$ to mean that $hg^{-1} \in P$, then G becomes an ordered group with positive cone.

Proof. Suppose G is an ordered group with positive cone P. Let $g, h \in P$, and let $x \in G$. Then $1 < g$, $1 < h$ implies that $1 < gh$ and $1 = x^{-1}1x < x^{-1}gx$. Thus $gh \in P$ and $x^{-1}gx \in P$. This yields parts (1) and (3). Moreover, if $y \in G$, then either $1 < y$, $1 = y$ or $y < 1$. Because the latter condition is equivalent to $1 = yy^{-1} < 1.y^{-1} = y^{-1}$, also condition (2) holds.

Conversely, suppose $P \subseteq G$ satisfies conditions (1), (2) and (3). Define $g < h$ to mean that $hg^{-1} \in P$. Now, if $g < h$ and $h < k$, then $kh^{-1}, hg^{-1} \in P$. Thus (1) yields that $kg^{-1} = (kh^{-1})(hg^{-1}) \in P$ and so $g < k$. Furthermore, if $g, h \in G$, then by (2), precisely one of the following three possibilities holds: $hg^{-1} \in P$, $hg^{-1} = 1$ or $gh^{-1} \in P$. Hence either $g < h$, $g = h$ or $h < g$, and $<$ is a linear ordering on G. Finally, suppose $g < h$ and $x \in G$. Then $hg^{-1} \in P$, so that by (3) we have

$$(hx)(gx)^{-1} = hg^{-1} \in P$$

and

$$(xh)(xg)^{-1} = x(hg^{-1})x^{-1} \in P.$$

Hence $gx < hx$ and $xg < xh$. Thus G is an ordered group. Because $h1^{-1} = h \in P$ if and only if $1 < h$, we get that the positive cone for this ordering is the set P. □

We note that the class of ordered groups is not particularly large. Indeed this class of groups is not even closed under extensions of groups. For example, let

$$G = \langle x, y \mid y^{-1}xy = x^{-1} \rangle.$$

This is an infinite extension of the infinite cyclic group $\langle x \rangle$ by the infinite cyclic group $\langle y \rangle$, and both $\langle x \rangle$ and $\langle y \rangle$ are ordered groups. But G is not ordered, because $x \in P$ would imply $x^{-1} = y^{-1}xy \in P$, and $x^{-1} \in P$ would imply that $x = y^{-1}x^{-1}y \in P$.

A weaker condition is that of left orderability.

Definition 4.1.5. *A group G is said to be left ordered if G has a total order $\leq$ such that for all $g \in G$,*

$$g_1 \leq g_2 \text{ implies } gg_1 \leq gg_2.$$

Again we can characterise left ordered groups via the positive cone.

Lemma 4.1.6. *If G is left ordered then $P(G) = \{g \in G \mid g \geq 1\}$ is a submonoid of G satisfying $P \cap P^{-1} = \{1\}$ and $P \cup P^{-1} = G$. Conversely, given any submonoid P of G with $P \cap P^{-1} = \{1\}$ and $P \cup P^{-1} = G$, then G is left ordered such that $P = P(G)$.*

Proof. The proof is similar to that of ordered groups. We leave it to the reader to verify the details. □.

Note that the mentioned conditions on P are left-right symmetric. Thus a left ordered group is also right ordered, but not necessarily under the same ordering. Indeed, if $<$ is a left ordering for G, then $<<$ defined by $g << h$ if and only if $h^{-1} < g^{-1}$ yields a right ordering with the same positive cone.

We now consider the extension properties of these groups.

Lemma 4.1.7. *Let N be a normal subgroup of a group G. If N and G/N are both left ordered groups, then so is G. Furthermore, if N and G/N are both ordered groups and if N is central in G, then G is an ordered group.*

Proof. Let $\pi : G \to G/N$ denote the natural homomorphism. Let $P(N)$ be the positive cone of N and $P(G/N)$ the positive cone of G/N. Define

$$P(G) = \{g \in G \mid \pi(g) \in P(G/N) \text{ or } g \in P(N)\}.$$

It is then easily verified that $P(G)$ is multiplicatively closed and that $G = P(G) \cup \{1\} \cup P(G)^{-1}$ is a disjoint union. Thus G is a right ordered group.

If G/N and N are ordered groups, then $\{g \in G \mid \pi(g) \in P(G/N)\}$ is easily seen to be a normal subset of G. If, furthermore N is central, then $P(N)$ is also normal in G. Hence, in this case G is an ordered group. □

Proposition 4.1.8. *If a group G has a subnormal series whose factors are left ordered then G is left ordered. In particular, if G has a subnormal series each of whose factors is torsion-free abelian then G is left ordered.*

Proof. The first part of the statement is an immediate consequence of Lemma 4.1.7. For the second statement it is sufficient to prove that if A is a torsion-free abelian group, then A is ordered. So let A be such a group and let $\mathcal{S}$ denote the family of all subsets S of A that satisfy the condition $s, t \in S$ implies $st \in S$ and also $1 \notin S$. Because of Zorn's Lemma $\mathcal{S}$ contains a maximal member S. We show that S satisfies conditions (1), (2) and (3) of Lemma 4.1.4. Clearly (1) is satisfied and (3) holds because A is abelian. We consider (2). Let $1 \neq a \in A$ and suppose by way of contradiction that neither a nor a^{-1} belongs to S. Put

$$T = S \cup \{sa^n \mid s \in S,\ n \geq 1\} \cup \{a^n \mid n \geq 1\}.$$

Clearly $S \subset T$ and T is multiplicatively closed. By the maximality of S we have $T \notin \mathcal{S}$. Hence $1 \in T$. Since A is torsion-free we have that $1 \notin \{a^n \mid n \geq 1\}$. Hence $1 = sa^n$ for some $s \in S$ and $n \geq 1$. Thus $a^{-n} \in S$. Replacing a by a^{-1} in this argument, we also obtain that $a^m \in S$ for some $m \geq 1$. Because S is multiplicatively closed we obtain that $1 = (a^m)^n(a^{-n})^m \in S$, a contradiction. Thus A is ordered. □

Lemma 4.1.9. *Let G be a unique product group and K a field. Then $K[G]$ is a domain.*

Proof. Let $\alpha = \sum_{i=1}^{n} a_i g_i$ and $\beta = \sum_{j=1}^{m} b_j h_j$ be nonzero elements in $K[G]$ (each $a_i, b_j \in K$, $0 \neq a_i$, $0 \neq b_j$, and $g_i, h_j \in G$). Since G is a unique product group there is a uniquely represented element in the product $\{g_1, \cdots, g_n\}\,\{h_1, \cdots, h_m\}$, say $g_1 h_1$. Hence $a_1 b_1 g_1 h_1$ is a term in

$$\alpha\beta = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j g_i h_j$$

that cannot be cancelled with any other term. Thus $\alpha\beta \neq 0$. □

This approach was brought to an end by the following example.

Example 4.1.10. *(Promislow)*
Let G be the group

$$G = \langle x, y \mid x^{-1}y^2x = y^{-2},\ y^{-1}x^2y = x^{-2} \rangle.$$

Then G is a torsion-free abelian-by-finite group which does not have the unique product property.

Proof. Set $z = xy$, $a = x^2$, $b = y^2$ and $c = z^2$. Then $D = \langle a, b, c \rangle$ is abelian and

$$a^z = a^{-1} \text{ and } b^z = b^{-1}.$$

Moreover

$$(xy)^{-1} = y^{-1}x^{-1} = y^{-2}yx^{-2}x = y^{-2}x^2yx = b^{-1}ayx$$

and thus

$$\begin{aligned} c^{-1} &= (xy)^{-2} \\ &= b^{-1}ayxb^{-1}ayx \\ &= b^{-1}aybxayx \\ &= b^{-1}abyxayx \\ &= b^{-1}abyaxyx \\ &= b^{-1}aba^{-1}yxyx \\ &= yxyx \end{aligned}$$

So

$$\begin{aligned} c^{-1} &= yxyx \\ &= x^{-1}(xyxy)x \\ &= c^x \end{aligned}$$

and

$$\begin{aligned} c^{-1} &= yxyx \\ &= y(xyxy)y^{-1} \\ &= c^{y^{-1}} \end{aligned}$$

Therefore D is an abelian normal subgroup of G. Furthermore G/D is generated by the elements $\overline{x} = xD$ and $\overline{y} = yD$ with $\overline{x}^2 = \overline{y}^2 = (\overline{xy})^2 = 1$. Hence $|G/D| \leq 4$.

We now show that D is a free abelian group of rank 3 and that $|G/D| = 4$. Consider therefore the following matrices in $\mathrm{GL}_4(\mathbf{Q})$:

$$X = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1/2 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ and } Y = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 \\ 0 & 1/2 & 0 & 0 \end{pmatrix}$$

One easily verifies that

$$X^{-1}y^2X = Y^{-2} \text{ and } Y^{-1}X^2Y = X^{-2}.$$

Hence there is a well defined group epmimorphism

$$\sigma : G \to \langle X, Y \rangle$$

given by

$$\sigma(x) = X \text{ and } \sigma(y) = Y.$$

Set $Z = XY$. Then

$$\begin{array}{rclcl} \sigma(a) & = & X^2 & = & \mathrm{diag}(2,2,1/2,1/2), \\ \sigma(b) & = & Y^2 & = & \mathrm{diag}(2,1/2,2,1/2), \\ \sigma(c) & = & Z^2 & = & \mathrm{diag}(2,1/2,1/2,2), \end{array}$$

and these matrices generate a free abelian group of rank 3. Also, as $\sigma(D)$ is diagonal and $1, X, Y, Z$ are not diagonal multiples of each other, we have $|G/D| \geq 4$ and hence G/D is the Klein Four Group.

Next we show that G is torsion free. So let $g \in G$ be an element of finite order. As $g^2 \in D$ and D is torsion free, we get that $g^2 = 1$. Suppose $g \in Dx$. Write $g = dx$ with $d \in D$. Then

$$1 = g^2 = dxdx = dd^x x^2 = dd^x a.$$

However $dd^x = a^{2n} b^{2m} c^{2k}$ for some $n, m, k \in \mathbb{Z}$ and thus

$$1 = a^{2n+1} b^{2m} c^{2k}.$$

But as $\{a, b, c\}$ is a free abelian basis for D this is impossible. Thus $g \notin Dx$. Similarly $g \notin Dy$ and $g \notin Dz$. Thus $g \in D$. As D is torsion free we get $g = 1$.

Finally we show that G does not have the unique product property. Let

$$S = Ax \cup By \cup C \subseteq G$$

with

$$A = \{1, a^{-1}, a^{-1}b, b, a^{-1}c^{-1}, c\},$$
$$B = \{1, a, b^{-1}, b^{-1}c, c, ab^{-1}c\}$$

and

$$C = \{c, c^{-1}\}.$$

Then $|S| = 14$ and $S^2 = S \cdot S$ has no unique product. For the latter, observe that $A, B, C \subseteq D$ and that D is commutative. Thus the intersection of S^2 with the four cosets of D are given by

$$S^2 \cap Dx = AxC \cup CAx = (AC^x \cup AC)x,$$

$$S^2 \cap Dy = ByC \cup CBy = (BC^y \cup BC)y,$$

$$S^2 \cap Dz = AxBy \cup ByAx = (AB^x \cup A^y Ba^{-1}bc^{-1})z,$$

$$S^2 \cap D = AxAx \cup ByBy \cup C^2 = AA^x a \cup BB^y b \cup C^2.$$

Because $C^x = C^y = C$, the elements in $S^2 \cap Dx$ and $S^2 \cap Dy$ all occur with even multiplicities; and are thus not uniquely represented. For the other two cosets one has to chech by hand or computer that the respective 72 and 76 products are not uniquely represented. $\square$

One can show that if G is the group in the example of Promislow than the group algebra $K[K]$ is a domain.

In the next stage in the investigations of the zero divisor problem one introduced some ring theoretic machinery. For this we introduce some definitions.

Definition 4.1.11. *A projective resolution $\mathcal{P}$ of a left R-module M is an exact sequence of the form*

$$\cdots \to \xrightarrow{f_n} P_{n-1} \to \cdots P_1 \xrightarrow{f_1} P_0 \xrightarrow{\epsilon} M \to 0$$

where each P_i is a projective left R-module. One says $\mathcal{P}$ is f.g. if each P_i is finitely generated; $\mathcal{P}$ is free if each P_i is a free left R-module. The smallest n for which $P_{n+1} = \{0\}$ is called the length of the resolution $\mathcal{P}$.

Lemma 4.1.12. *Every module M has a free resolution. Every finitely generated module over a left noetherian ring has a f.g. free resolution.*

Proof. Let $f_0 : F_0 \to M$ be a module epimorfism with F_0 a free module. Inductively, given $f_{i-1} : F_{i-1} \to F_{i-2}$ define a module morphism $f_i : F_i \to F_{i-1}$ with F_i free and $f_i(F_i) = \ker(f_{i-1})$. It follows that the sequence

$$\cdots F_2 \xrightarrow{f_2} F_1 \xrightarrow{f_1} F_0 \to 0$$

is an exact sequence of free modules.

If in the above M is finitely generated then we could take F_0 finitely generated. In case R is left Noetherian we obtain that $\ker(f_0)$ is finitely generated as well. Continuing by induction we may assume that each F_i is finitely generated. □

We note that every exact sequence

$$\cdots \to M'' \xrightarrow{f} M \xrightarrow{g} M' \to \cdots$$

can be cut at g to produce exact sequences

$$\to M'' \xrightarrow{f} M \to gM \to 0$$

and

$$0 \to \ker g \to M \xrightarrow{g} M' \to \cdots$$

In particular any projective resolution $\mathcal{P}$ can be cut at f_n to yield

$$0 \to K \to P_n \xrightarrow{f_n} P_{n-1} \to \cdots \to P_0 \to M \to 0.$$

The module $K = \ker f_n$ is called the n-th syzygy of M. If $\mathcal{P}$ has length $n+1$ then $K \cong P_{n+1}$ is projective. Conversely, if K is projective then we have obtained a new projective resolution of length $n+1$. We now compare these two projective resolutions in the following proposition.

Proposition 4.1.13. *(Schanuel's lemma) Assume*

$$0 \to K_1 \to P_1 \stackrel{g_1}{\to} M \to 0$$

and

$$0 \to K_2 \to P_2 \stackrel{g_2}{\to} M \to 0$$

are exact sequences. If P_1 and P_2 are projective, then

$$P_1 \oplus K_2 \cong P_2 \oplus K_1.$$

Proof. Identify K_i with $\ker(g_i)$. Consider the diagram

$$\begin{array}{ccccc} & & P_1 & & \\ & & \downarrow g_1 & & \\ P_2 & \stackrel{g_2}{\to} & M & \to & 0 \end{array}$$

Because P_1 is projective there exists a module morphism $h : P_1 \to P_2$ so that $g_1 = g_2 h$. Define

$$f : P_1 \oplus K_2 \to P_2 : (x, y) \mapsto hx - y.$$

We claim that f is an epimorphism. Indeed, let $x' \in P_2$. Then since g_1 is surjective, there exists $x \in P_1$ so that $g_1(x) = g_2(x')$. Hence $g_2(h(x) - x') = g_1(x) - g_2(x') = 0$. Thus $h(x) - x' \in K_2$ and $f(x, hx - x') = x'$.

Since f is an epimorphism onto the projective P_2, the morphism f splits. Thus $P_1 \oplus K_2 \cong P_2 \oplus \ker(f)$. Now

$$\begin{array}{rcl} \ker(f) & = & \{(x, y) \in P_1 \oplus K_2 \mid h(x) = y \in K_2\} \\ & = & \{(x, h(x)) \mid x \in P_1,\ h(x) \in K_2\} \\ & = & \{(x, h(x)) \mid x \in P_1,\ g_2 h(x) = 0\} \\ & = & \{(x, h(x)) \mid x \in P_1,\ g_1(x) = 0\} \\ & \cong & K_1 \end{array}$$

Thus the result follows. □

Proposition 4.1.14. *(generalised Schanuel's lemma) Assume*

$$0 \to K \to P_n \stackrel{f_n}{\to} P_{n-1} \to \cdots \to P_1 \stackrel{f_1}{\to} P_0 \stackrel{\epsilon}{\to} M \to 0$$

and

$$0 \to K' \to P'_n \stackrel{g_n}{\to} P'_{n-1} \to \cdots \to P'_1 \stackrel{g_1}{\to} P'_0 \stackrel{\epsilon'}{\to} M \to 0$$

are exact sequences. If each P_i and P'_i is projective, then

$$K \oplus P'_n \oplus P_{n-1} \oplus P'_{n-2} \oplus \cdots \cong K' \oplus P_n \oplus P'_{n-1} \oplus P_{n-2} \oplus \cdots$$

Proof. We cut the sequence at f_1 to get

$$0 \to K \to \cdots \to P_2 \to P_1 \to \ker \epsilon \to 0$$

and

$$0 \to \ker \epsilon \to P_0 \to M \to 0$$

Cutting at g_1 we get

$$0 \to K' \to \cdots \to P_2' \to P_1' \to \ker \epsilon' \to 0$$

and

$$0 \to \ker \epsilon' \to P_0' \to M \to 0$$

Applying Schanuel's Lemma to the two short exact sequences we obtain

$$M' \cong P_0' \oplus \ker \epsilon \cong P_0 \oplus \ker \epsilon'$$

We then can modify the two other sequences to get

$$0 \to K \to \cdots \to P_2 \to P_1 \oplus P_0' \stackrel{f_1 \oplus 1}{\to} M' \to 0$$

and

$$0 \to K' \to \cdots \to P_2' \to P_1' \oplus P_0 \stackrel{f_1 \oplus 1}{\to} M' \to 0$$

By induction on the length we get the desired conclusion. □

Definition 4.1.15. *Two modules N, N' are projectively equivalent if there are projective modules P, P' such that $N \oplus P \cong N' \oplus P'$. If, furthermore, P, P' are finitely generated free then N, N' are stably equivalent. One says N is stably free if N is stably equivalent to a free module, i.e. $N \oplus R^n$ is free for some n.*

Note that any stably free module is projective. Also the n-th syzygies of any two projective resolutions of a module M are projectively equivalent. The n-th syzygies of any two f.g. free resolutions of M are stably equivalent.

We mention the following important result. It shows that there do not exist stably free nonfree modules over Noetherian commutative polynomial algebras.

Theorem 4.1.16. *(Quillen-Suslin) Let K be a field. Each projective module over $K[X_1, \cdots, X_n]$ is free.*

We mention the following example. Let $R = \mathbf{R}[X, Y, Z]/(X^2 + Y^2 + Z^2 - 1]$. Then R has a stably free nonfree module P with $P \oplus R \cong R^3$. Other examples over commutative Noetherian rings are

$$k[X_1, \cdots, X_n, Y_1, \cdots, Y_n]/(\sum_{i=1}^{n} X_i Y_i - 1),$$

with k a field of characteristic zero and $n \geq 2$.

We now introduce a new dimension in module theory.

Definition 4.1.17. *A module M has projective dimension n (denoted $pd(M) = n$) if n is the smallest integer so that M has a projective resolution of length n. If no such number exists then we say M has infinite projective dimension.*

Note that $\mathrm{pd}(M) = 0$ if and only if M is projective.

Proposition 4.1.18. *Let M be an R-module. The following conditions are equivalent:*

1. *$pd(M) \leq n + 1$,*
2. *The n-th syzygy of any projective resolution of M is projective,*
3. *any projective resolution $\mathcal{P}$ of M can be cut at f_n to form a projective resolution of length $n + 1$.*

Proof. (1) $\Rightarrow$ (2) The n-th syzygies of any two projective resolutions of M are projectively equivalent. Because of (1) M has a projective resolution with n-th syzygy a projective module. Thus any n-th syzygy is projective.
(2) $\Rightarrow$ (3) This is clear.
(3) $\Rightarrow$ (1) This is clear from the definition of projective dimension. □

Proposition 4.1.19. *Let M be an R-module. The following conditions are equivalent:*

1. *M has a f.g. free resolution of length $\leq n + 1$,*
2. *The n-th syzygy of any f.g. free resolution of M is stably free,*
3. *any f.g. free resolution of M can be cut and modified to form a a f.g. free resolution of length $n + 1$.*

Proof. (3) $\Rightarrow$ (1) $\Rightarrow$ (2) is clear. We prove (2) $\Rightarrow$ (3). For this it is sufficient to note that if $P \oplus R^{(n)}$ is free and $0 \to P \to F \to F'$ is exact with F, F' free, then the sequence of free modules

$$0 \to P \oplus R^{(n)} \to F \oplus R^{(n)} \to F'$$

is exact. □

We now give some elementary properties of projective dimension. To do so we first need to prove several lemmas concerning diagrams of modules. We assume all rows and columns are exact.

Lemma 4.1.20. *(The five lemma) Consider the following diagram*

$$\begin{array}{ccccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D & \xrightarrow{j} & E \\ \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \downarrow \delta & & \downarrow \epsilon \\ A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \xrightarrow{h'} & D' & \xrightarrow{j'} & E \end{array}$$

If every vertical arrow but γ is an isomorphism then γ is also an isomorphism.

Proof. □

Lemma 4.1.21. *Suppose the following diagram is given*

$$\begin{array}{ccc} M & \stackrel{\beta}{\to} & N \\ \downarrow f & & \downarrow g \\ M'' & \stackrel{\gamma}{\to} & N'' \end{array}$$

Then f restricts to a map

$$\tilde{f} : \ker\beta \to \ker\gamma$$

and g induces a map

$$\overline{g} : coker\beta \to coker\gamma$$

yielding the commutative diagram

$$\begin{array}{ccccccccccc} 0 & \to & \ker\beta & \to & M & \stackrel{\beta}{\to} & N & \to & coker\beta & \to & 0 \\ & & \downarrow \tilde{f} & & \downarrow f & & \downarrow g & & \downarrow \overline{g} & & \\ 0 & \to & \ker\gamma & \to & M'' & \stackrel{\gamma}{\to} & N'' & \to & coker\gamma & \to & 0 \end{array}$$

If f and g are isomorphisms then $\tilde{f}$ and $\overline{g}$ are also isomorphisms.

Proof. Suppose $x \in \ker\beta$, that is, $\beta x = 0$. Then

$$\gamma f x = g\beta x = 0.$$

Hence $f(\ker\beta) \subseteq \ker(\gamma)$ and thus f restricts to a map

$$\tilde{f} : \ker\beta \to \ker\gamma : m \mapsto f(\beta).$$

On the other hand ,

$$g(\beta M) = \gamma f M \subseteq \gamma M''.$$

Thus g induces a map

$$\overline{g} : \mathrm{coker}\beta = N/\beta M \to N''/\gamma M'' = \mathrm{coker}\gamma : n + \beta M \mapsto g(n).$$

The commutativity of the ensuing diagram is easy to verify.

The last assertion is a special case of the five lemma. Indeed, adding 0 at the right so that $\overline{g}$ is in the middle of the appropriate diagram (with f at the left side) shows that $\overline{g}$ is an isomorphism. Adding 0 at the left so that $\tilde{f}$ is in the middle shows that $\tilde{f}$ is an isomorphism. □

Lemma 4.1.22. *(Snake Lemma) Suppose the following diagram is given*

$$\begin{array}{ccccccc} & & M' & \stackrel{f'}{\to} & M & \stackrel{f}{\to} & M'' \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma \\ 0 & \to & N' & \stackrel{g'}{\to} & N & \stackrel{g}{\to} & N'' \end{array}$$

Then

1. $\ker\alpha \xrightarrow{\tilde{f'}} \ker\beta \xrightarrow{\tilde{f}} \ker\gamma$ *is exact (where the maps are obtained as in Lemma 4.1.21).*

2. *If f is an epimorphism then there is an exact sequence*

$$\ker\alpha \xrightarrow{\tilde{f'}} \ker\beta \xrightarrow{\tilde{f}} \ker\gamma \xrightarrow{\delta} coker\ \alpha \xrightarrow{\overline{g'}} coker\ \beta \xrightarrow{\overline{g}} coker\ \gamma$$

where δ is defined in the proof and the other maps are as in Lemma 4.1.21.

Proof. (1) Because $f\ f' = 0$ we certainly get that $\tilde{f}\ \tilde{f'} = 0$. Hence $Im(\tilde{f'}) \subseteq \ker(\tilde{f})$. On the other hand, if $z \in \ker\beta$ and $fz = \tilde{f}z = 0$, then $z = f'x'$ for some $x' \in M'$. Hence

$$0 = \beta z = \beta f' x' = g'\alpha x'.$$

As g' is injective we get that $\alpha x' = 0$ and thus $x' \in \ker\alpha$. Hence $z \in Im(\tilde{f'})$.

(2) Define δ as follows. Suppose $x'' \in \ker\gamma$. Since f is onto, by assumption, there exits $x \in M$ so that $fx = x''$. Then $g\beta x = 0$, and thus $\beta x \in \ker g = g'N'$. So there exists $y' \in N'$ with $g'y' = \beta x$. Define

$$\delta x'' = y' + \alpha M'.$$

We now show that δ is well defined. So suppose $x_1 \in M$ with $fx_1 = x''$ and $y_1' \in N'$ with $g'y_1' = \beta x_1$. Then

$$f(x_1 - x) = 0$$

so that

$$x_1 - x \in f'M'.$$

Hence

$$g'(y_1' - y_1) = \beta(x_1 - x) \in \beta f'M' = g'\alpha M'.$$

Consequently, since g' is injective,

$$y_1' - y_1 \in \alpha M'$$

and thus

$$y_1' + \alpha M' = y' + \alpha M'.$$

We now show that that $\ker\alpha \xrightarrow{\tilde{f'}} \ker\beta \xrightarrow{\tilde{f}} \ker\gamma \xrightarrow{\delta} \text{coker}\ \alpha$ is exact (the other part we leave to the reader). In view of (1) we need only show $\ker\beta \xrightarrow{\tilde{f}} \ker\gamma \xrightarrow{\delta} \text{coker}\ \alpha$ is exact. We use throughout the notation of the previous paragraph. First note that if $x'' \in \tilde{f}(\ker\beta)$ then in the definition of δ we could take $x \in \ker\beta$. So $g'y' = \beta x = 0$ and thus $y' = 0$. This shows that $\delta\tilde{f} = 0$. On the other hand, if $\delta x'' = 0$ then $y' \in \alpha M'$. So $y' = \alpha x'$ for some $x' \in M'$. Hence $\beta f' x' = g'\alpha x' = g'y' = \beta x$, and thus $x - f'x' \in \ker\beta$. Consequently, $\tilde{f}(x - f'x') = f(x - f'x') = fx = x''$, so that $x'' \in \tilde{f}(\ker\beta)$. □

Lemma 4.1.23. *(The nine lemma) Suppose the following diagram is given*

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & A' & & A & & A'' & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & B' & \xrightarrow{f} & B & \to & B'' & \to & 0 \\
 & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\
0 & \to & C' & \to & C & \to & C'' & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

One can then complete the diagram as follows

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & A' & \to & A & \to & A'' & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & B' & \xrightarrow{f} & B & \to & B'' & \to & 0 \\
 & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\
0 & \to & C' & \to & C & \to & C'' & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Proof. From the snake lemma we obtain the following exact sequence.

$$\ker \alpha \xrightarrow{\tilde{f}} \ker \beta \to \ker \gamma \xrightarrow{\delta} \text{coker } \alpha = 0$$

Since f is a monomorphism this gives the short exact sequence

$$0 \to \ker \alpha \xrightarrow{\tilde{f}} \ker \beta \to \ker \gamma \xrightarrow{\delta} \text{coker}\alpha = 0$$

Hence the result follows. □

Lemma 4.1.24. *(The horseshoe lemma) If P and P' are projective, then the following diagram*

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
0 & \to & K' & \xrightarrow{\alpha'} & P' & \xrightarrow{\beta'} & M' & \to & 0 \\
 & & & & & & \downarrow f' & & \\
 & & & & & & M & \to & 0 \\
 & & & & & & \downarrow f & & \\
0 & \to & K'' & \xrightarrow{\alpha''} & P'' & \xrightarrow{\beta''} & M'' & \to & 0 \\
 & & & & & & \downarrow & & \\
 & & & & & & 0 & &
\end{array}$$

can be completed as follows

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & K' & \stackrel{\alpha'}{\to} & P' & \stackrel{\beta'}{\to} & M' & \to & 0 \\
 & & \downarrow & & \downarrow \mu & & \downarrow f' & & \\
0 & \to & K & \to & P' \oplus P'' & \stackrel{\beta}{\to} & M & \to & 0 \\
 & & \downarrow & & \downarrow \pi & & \downarrow f & & \\
0 & \to & K'' & \stackrel{\alpha''}{\to} & P'' & \stackrel{\beta''}{\to} & M'' & \to & 0 \\
 & & & & & & \downarrow & & \\
 & & \downarrow & & \downarrow & & 0 & &
\end{array}$$

where $\mu : P' \to P' \oplus P''$ is the canonical injective map and $\pi : P' \oplus P'' \to P''$ is the projection.

Proof. Since P'' is projective, there is a homomorphism

$$h : P'' \to M$$

so that

$$\beta'' = fh.$$

Define

$$\beta : P' \oplus P'' \to M$$

by

$$\beta(x', x'') = f'\beta' x' + hx''.$$

This makes the top right square commutative. Moreover,

$$f\beta(x', x'') = ff'\beta' x' + \beta'' x'' = 0 + \beta''\pi(x', x''),$$

so the bottom right square is commutative. Let $K = \ker \beta$. We then obtain the upper row by means of the nine lemma. □

Lemma 4.1.25. *(Turning the Corner Lemma) Given the diagram*

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & K' & \to & A'_n & \to & A'_{n-1} & \to & \cdots \\
 & & \downarrow g & & \downarrow & & \downarrow & & \\
0 & \to & K & \to & A_n & \to & A_{n-1} & \to & \cdots \\
 & & \downarrow h & & \downarrow \beta & & \downarrow \gamma & & \\
0 & \to & K'' & \stackrel{i}{\to} & A''_n & \stackrel{f}{\to} & A''_{n-1} & \to & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

one obtains an exact sequence

$$0 \to K' \stackrel{g}{\to} K \stackrel{ih}{\to} A''_n \stackrel{f}{\to} A''_{n-1} \to \cdots$$

Proof. Since h is an epimorphism

$$\ker f = iK'' = ihK.$$

Since i is a monomorphism we get

$$\ker ih = \ker h = gK'.$$

Hence the result follows. □

Proposition 4.1.26. *Assume $0 \to M' \to M \to M''$ is an exact. If $\mathcal{P}'$ and $\mathcal{P}''$ are projective resolutions of M' and M'' respectively, then there exists a projective resolution $\mathcal{P}$ of M with $P_n = P'_n \oplus P''_n$. Furthermore if K'_n and K''_n are the respective n-th syzygies then we have the following commutative diagram for each n, obtained by cutting $\mathcal{P}'$, $\mathcal{P}$ and $\mathcal{P}''$ at f'_n, f_n and f''_n respectively:*

$$\begin{array}{ccccccccccccc}
 & & 0 & & 0 & & 0 & & & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & & & \downarrow & & \downarrow & & \\
0 & \to & K'_n & \to & P'_n & \to & P'_{n-1} & \to & \cdots & \to & P'_0 & \to & M' & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & & & \downarrow & & \downarrow & & \\
0 & \to & K_n & \to & P_n & \to & P_{n-1} & \to & \cdots & \to & P_0 & \to & M & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & & & \downarrow & & \downarrow & & \\
0 & \to & K''_n & \to & P''_n & \to & P''_{n-1} & \to & \cdots & \to & P''_0 & \to & M'' & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & & & & 0 & & 0 & &
\end{array}$$

Proof. We prove this by induction on n. Suppose for $1 \leq i \leq n-1$ we have $P_i = P'_i \oplus P''_i$ together with the diagram

$$\begin{array}{ccccccccccccc}
 & & 0 & & 0 & & 0 & & & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & & & \downarrow & & \downarrow & & \\
0 & \to & K'_{n-1} & \to & P'_{n-1} & \overset{f'_{n-1}}{\to} & P'_{n-2} & \to & \cdots & \to & P'_0 & \to & M' & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & & & \downarrow & & \downarrow & & \\
0 & \to & K_{n-1} & \to & P_{n-1} & \to & P_{n-2} & \to & \cdots & \to & P_0 & \to & M & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & & & \downarrow & & \downarrow & & \\
0 & \to & K''_{n-1} & \to & P''_{n-1} & \overset{f''_{n-1}}{\to} & P''_{n-2} & \to & \cdots & \to & P''_0 & \to & M'' & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & & & & 0 & & 0 & &
\end{array}$$

Note that

$$K'_{n-1} = \ker f'_{n-1} = f'_n P'_n$$

and

$$K''_{n-1} = \ker f''_{n-1} = f''_n P''_n.$$

Cutting the resolutions $\mathcal{P}'$, $\mathcal{P}''$ at f'_n, f''_n yields the diagram

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
\to & P'_{n+1} & \to & P'_n & \to & f'_nP'_n = K'_{n-1} & \to & 0 & \\
 & & & & & & \downarrow & & \\
 & & & & & & K_{n-1} & \to & 0 \\
 & & & & & & \downarrow & & \\
\to & P''_{n+1} & \to & P''_n & \to & f''_nP''_n = K''_{n-1} & \to & 0 & \\
 & & & & & & \downarrow & & \\
 & & & & & & 0 & &
\end{array}$$

where the column is the $n-1$ - syzygy column from above. By the horseshoe lemma we complete the diagram as follows

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & K'_n & \to & P'_n & \to & f'_nP'_n & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & K_n & \to & P_n & \to & K_{n-1} & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & K''_n & \to & P''_n & \to & f''_nP''_n & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

where $P_n = P'_n \oplus P''_n$. The result now follows by pasting this last diagram to the first one mentioned in the proof. □

Corollary 4.1.27. *Assume $0 \to M' \to M \to M'' \to 0$ is an exact sequence. If M', M'' have projective (resp. f.g. projective, resp. free, resp. f.g. free) resolutions of length $\leq n$, then so does M. In particular*

$$pd(M) \leq \max\{pd(M'), pd(M'')\}.$$

If $pd(M') > pd(M'')$ then $pd(M) = pd(M')$.

Proof. The first two assertions follow at once from Proposition 4.1.26.

For the last assertion we assume $pd(M') > pd(M'')$ and we examine the exact sequence of the n-th syzygies

$$0 \to K'_n \to K_n \to K''_n \to 0$$

for $\mathrm{pd}(M'') = n$. This sequence splits since K''_n is projective. So K'_n is projectively equivalent to K_n. Hence by Proposition 4.1.19, $\mathrm{pd}(M) = \mathrm{pd}(M')$. □

Corollary 4.1.28. *Assume* $0 \to M' \to M \to M'' \to 0$ *is an exact sequence. Suppose* $\mathcal{P}'$, $\mathcal{P}''$ *are projective resolutions of* M', M'' *and let* $\mathcal{P}$ *be built as in Proposition 4.1.26. Let* K'_m, K_m, K''_m *denote the respective* m*-th syzygies. Then for any* m *there is an exact sequence*

$$0 \to K'_{m-1} \to K_{m-1} \to P''_{m-1} \to P''_{m-2} \to \cdots P''_0 \to M'' \to 0.$$

So K'_{m-1} *is the* m*-th syzygy of a projective resolution of* M''*, if* K_{m-1} *is projective.*

So

$$pd(M'') \leq \max\{pd(M'), pd(M)\} + 1.$$

Furthermore,

$$pd(M'') = pd(M) \text{ if } pd(M') < pd(M)$$

and

$$pd(M'') = pd(M') + 1 \text{ if } pd(M') > pd(M).$$

Proof. The first assertion is obtained by the Cutting the Corner Lemma.

Taking $m = \max\{\mathrm{pd}(M'), \mathrm{pd}(M)\}$ we see that K'_{m-1} and K_{m-1} are projective. So $\mathrm{pd}(M'') \leq m + 1 = \max\{\mathrm{pd}(M'), \mathrm{pd}(M)\} + 1$.

If $\mathrm{pd}(M') < \mathrm{pd}(M) = n$ then M' has a projective resolution $\mathcal{P}'$ with $P'_n = \{0\}$. Hence $K'_{n-1} = \{0\}$. So we could choose $\mathcal{P}'$ so that $K'_{n-1} = 0$. Now since $\mathrm{pd}(M) = n$ we know that M has a projective resolution $\mathcal{P}$ with $P_{n+1} = \{0\}$ and thus $K_{n-1} \cong P_n$ is projective. Taking $m = n$ we get an exact sequence

$$0 \to K'_{n-1} = \{0\} \to K_{n-1} \to P''_{n-1} \to P''_{n-2} \to \cdots P''_0 \to M'' \to 0.$$

So K_{n-1} is the $n-1$-th syzygy of a projective resolution of M'' and it is projective. Therefore $\mathrm{pd}(M'') \leq n$. Now by Corollary 4.1.27 we also know that $\mathrm{pd}(M) \leq \max\{\mathrm{pd}(M'), \mathrm{pd}(M'')\}$. Thus, because also $\mathrm{pd}(M') < \mathrm{pd}(M)$ we get $\mathrm{pd}(M) \leq \mathrm{pd}(M'')$ Therefore we get $\mathrm{pd}(M) = \mathrm{pd}(M'') = n$.

Assume now that $\mathrm{pd}(M') > \mathrm{pd}(M)$. If $\mathrm{pd}(M') = 1$, then $\mathrm{pd}(M) = 0$, that is, M is projective. Because of the exact sequence $0 \to M' \to M \to M'' \to 0$ we get that M' is the 0-th syzygy of the projective resolution of M'' starting with the morphism $M \to M'' \to 0$. Since M' is not projective, it follows that $\mathrm{pd}(M'') \geq 2$. On the other hand we know already that $pd(M'') \leq \max\{pd(M'), pd(M)\} + 1 = 2$. Thus $\mathrm{pd}(M'') = 2 = \mathrm{pd}(M') + 1$, as desired. So it is now sufficient to deal with the case $\mathrm{pd}(M') = m \geq 2$. Then, $\mathrm{pd}(M) \leq m - 1$ and thus K_{m-2} is projective, but K'_{m-2} is not. So the $m-1$-th syzygy of

$$0 \to K'_{m-2} \to K_{m-2} \to P''_{m-2} \to \cdots P''_0 \to M'' \to 0$$

is not projective. Therefore $\mathrm{pd}(M'') \geq m + 1 = \mathrm{pd}(M') + 1$. On the other hand we already know $pd(M'') \leq \max\{pd(M'), pd(M)\} + 1 = \mathrm{pd}(M') + 1$. Thus we get $\mathrm{pd}(M'') = \mathrm{pd}(M') + 1$. □

Consider the following example. Let $R = k[y]/(y^2)$, with k a field of characteristic 2. Then we have the nonsplit exact sequence

$$0 \to yR \to R \to R/yR \to 0.$$

Since $yR \cong R/yR$ it follows that $\mathrm{pd}(yR)$ is infinite. Indeed, since $\mathrm{pd}(R) = 0$ and $\mathrm{pd}(yR) \neq 0$, we get from Corollary 4.1.28 that $\mathrm{pd}(R/yR) = \mathrm{pd}(yR)+1$. As $\mathrm{pd}(yR) = \mathrm{pd}(R/yR)$ we obtain that $\mathrm{pd}(yR) = \infty$.

Definition 4.1.29. *The left global dimension of a ring R is the number*

$$gl.dim(R) = \sup\{pd(M) \mid M \text{ a left } R-\text{module}\}.$$

A ring R is semisimple artinian if and only if every module is projective, or equivalently $\mathrm{gl.dim}(R) = 0$. Rings of global dimension at most one are called (left) hereditary.

Lemma 4.1.30. *A ring R is left hereditary if and only if every left ideal of R is left projective.*

Proof. Obviously, if $\mathrm{gl.dim}(R) \leq 1$ then for every left ideal L of R a projective resolution built on the epimorhism

$$R \to R/L \to 0$$

will have a projective first syzygy. Clearly the latter is L. So L is projective.

Conversely, assume that every left ideal of R is left projective.

We now first show that every submodule of a free left R-module F is isomorphic to a direct sum of left ideals. Indeed, let $\{x_i \mid i \in I\}$ be a free basis of F and take a well-ordering on I. For any $i \in I$, let

$$F_i = \oplus_{j<i} Rx_j,$$

and define

$$\pi_i : Rx_i + F_i \to R : rx_i + \sum_{j<i} r_j x_j \mapsto r.$$

Suppose M is a proper submodule of F. Write

$$M_i = M \cap F_i,$$

for $i \in I$. Let

$$f_i = (\pi_i)_{|M_i},$$

the restriction to M_i of π_i. Then

$$\ker f_{i+1} = M_i.$$

So we get the short exact sequence

$$0 \to M_i \to M_{i+1} \to L_i \to 0,$$

with $L_i = f_{i+1}M_{i+1}$. Because of the assumption, L_i is projective, and thus

$$M_{i+1} \cong L_i \oplus M_i.$$

Continuing by induction we get

$$M_\alpha \cong \oplus_{\beta<\alpha} M_\beta$$

for any ordinal α. Taking α to be the ordinal of I we get that M indeed is isomorphic with a direct sum of left ideals of R.

Of course a projective module is submodule of a free module. From the previous claim it therefore follows that a submodule of a projective module is a direct sum of projective modules, and hence is itself projective. Hence the first syzygy of any module is itself projective. Therefore $\mathrm{pd}(M) \leq 1$ for any left R-module M. So it follows that $\mathrm{gl.dim}(R) \leq 1$, that is, R is left hereditary. □

If all left ideals of a domain R are principal, then all left ideals of R are free and thus projective. So R is left hereditary. Examples of such rings are polynomial algebras $k[X]$ over a field k. So, in particular, $\mathrm{gl.dim}k[X] = \mathrm{gl.dim}(k) + 1$. We show that this relation holds more generally for a skew polynomial ring. In order to prove this we need to define some new module structures.

Suppose M is a left R-module and σ is an automorphism of R. We define

$$M[X, \sigma]$$

to be the additive group

$$R[X] \otimes_R M$$

(so as a set this consists of the elements $\sum X^i m_i$ with $m_i \in M$) with $R[X, \sigma]$ module structure defined as follows:

$$(rX^j) \sum X^i m_i = \sum X^{i+j} (\sigma^{-(i+j)} r) m_i.$$

Since $R[X, \sigma]$ is free over itself we obtain that $F[X, \sigma]$ is a free left $R[X, \sigma]$-module for any free R-module F. Consequently, any projective (respectively free) R-resolution

$$0 \to P_n \to \cdots \to P_0 \to M \to 0$$

of M yields a projective (respectively free) $R[X, \sigma]$-resolution

$$0 \to P_n[X, \sigma] \to \cdots \to P_0[X, \sigma] \to M[X, \sigma] \to 0$$

of $M[X, \sigma]$. It follows that

$$\mathrm{pd}_{R[X,\sigma]} M[X, \sigma] \leq \mathrm{pd}_R M.$$

Actually one can show that equality holds.

On the other hand, any $R[X,\sigma]$-module M is also a R-module (in a natural way); hence we can form $M[X,\sigma]$ as above. To distinguish the latter module structure from the given one, we denote

$$X \cdot m$$

for the new product ($m \in M$).

Let σM denote the set of formal elements $\{\sigma m \mid m \in M\}$ with the following R-module structure:

$$\sigma m_1 + \sigma m_2 = \sigma(m_1 + m_2)$$

and

$$r\sigma m = \sigma(\sigma^{-1}(r)m,$$

for $m, m_1, m_2 \in M$ and $r \in R$ (and $\sigma^{-1}(r)m$ is the product in M.

Lemma 4.1.31. *(Hochschild's trick) For any $R[X,\sigma]$-module M there is an exact sequence*

$$0 \to (\sigma M)[X,\sigma] \to M[X,\sigma] \xrightarrow{f} M \to 0$$

where $f(X^i \cdots m) = X^i m$.

Proof. Define

$$g : (\sigma M)[X,\sigma] \to M[X,\sigma]$$

by

$$g(\sum X^i \cdot \sigma m_i) = \sum (X^i \cdot Xm_i - X^{i+1} \cdot m_i).$$

Clearly

$$g(\sigma M[X,\sigma]) \subseteq \ker f.$$

Furthermore,

$$(rX^j) \cdot X^i \cdot \sigma m_i = X^{i+j} \cdot \sigma^{-(i+j)} r\sigma m_i = X^{i+j} \cdot \sigma((\sigma^{-(i+j+1)}r)m_i).$$

So

$$\begin{aligned} g\left(rX^j \sum_i X^i \cdot \sigma m_i\right) &= \sum_i X^{i+j} \cdot X(\sigma^{-(i+j+1)}r)m_i - X^{i+j+1} \cdot (\sigma^{-(i+j+1)}r)m_i) \\ &= \sum_i r(X^{i+j} \cdot Xm_i - X^{i+j+1} \cdot m_i) \\ &= rX^j g(\sum_i X^i \cdot \sigma m_i) \end{aligned}$$

Hence g is an $R[X,\sigma]$ module morphism.

Now

$$g(\sum X^i \cdot \sigma m_i) = 1 \cdot Xm_0 + \sum_{i\geq 1} X^i \cdot (Xm_i - m_{i-1}).$$

Therefore

$$\sum X^i \cdot \sigma m_i \in \ker g \text{ if and only if } Xm_0 = 0 \text{ and } Xm_i = m_{i-1} \ (i \geq 1).$$

But for large i we have $m_i = 0$ and thus it follows that all $m_i = 0$ for all $i \geq 0$. So g is a monomorphism.

Finally suppose $x = \sum_{i=0}^{n} X^i \cdot m_i' \in \ker f$. Put $m_n' = 0$, $m_{n-1} = -m_n'$ and given m_i put $m_{i-1} = Xm_i = m_i'$. Then

$$g(\sum_{i\geq 0} X^i \cdot \sigma m_i) = x.$$

This proves the exactness of the sequence. □

Proposition 4.1.32. *Let σ be an automorphism of the ring R then*

$$gl.dim(R[X,\sigma]) \leq gl.dim(R) + 1.$$

Proof. Let n =gl.dim(R). For any $R[X,\sigma]$-module M we have

$$\mathrm{pd}_{R[X,\sigma]}(M[X,\sigma]) \leq \mathrm{pd}_R(M) \leq n.$$

and

$$\mathrm{pd}_{R[X,\sigma]}(\sigma M)[X,\sigma] \leq \mathrm{pd}_R(\sigma M) \leq n.$$

Thus by Hochschild's trick and Corollary 4.1.28

$$\mathrm{pd}_{R[X,\sigma]} M \leq n + 1.$$

□

With a bit more work one can actually show that

$$\mathrm{gl.dim}(R[X,\sigma]) = \mathrm{gl.dim}(R) + 1.$$

for any ring R and automorphism σ on R. Now, using localization techniques one can show that

$$\mathrm{gl.dim}(R[X, X^{-1}\sigma]) \leq \mathrm{gl.dim}(R[X,\sigma]).$$

As a consequence

Proposition 4.1.33. *Let G be a group with a subnormal series each of whose factors is infinite cyclic. Then, for any field F,*

$$gl.dim(F[G]) \leq h(G).$$

One can improve this theorem as follows.

Theorem 4.1.34. *(Serre) Let F be a field. Suppose a group G has a subgroup H of finite index such that $gl.dim(F[H])$ is finite. If G does not have elements of order $char(F)$, then*

$$gl.dim(F[G]) < \infty.$$

In particular, G is a polycyclic-by-finite group without elements of order $char(F)$, then

$$gl.dim(F[G]) < \infty.$$

The importance of the introduced notions is also indicated in the following result.

Theorem 4.1.35. *Let R be a ring. If R satisfies the following conditions*

1. *R is left noetherian and semiprime,*
2. *all finitely generated left R-modules have finite projective dimension,*
3. *all finitely generated projective left R-modules are stably free*

then R is a domain.

We already know that a group algebra of a torsion-free polycyclic-by-finite group G is noetherian. Later we will see that it is also semiprime. Due to Serre's Theorem we also know that $K[G]$ has finite global dimension. Furthermore J.Moody proved that the third condition also holds for $K[G]$. Hence we have the following.

Theorem 4.1.36. *(Brown, Cliff, Farkas and Snider) Let K be a field and G a torsion-free polycyclic-by-finite group. Then $K[G]$ is a domain.*

Chapter 5

Prime and semiprime rings

5.1 Group algebras

The problem of determining when a group ring is prime turns out to be much simpler than the zero divisor problem.

One of the techniques of studying infinite groups is in terms of nice subgroups of finite index. We are interested in relating the structure of $K[G]$ with that of $K[H]$, where H is a subgroup of finite index in G.

First we note the following facts for subgroups H, H_i of a group G:

1. If $[G : H_i] = n$, then $[H : H_i \cap H] \leq n$.
2. If $[G : H_i] = n_i$, for $1 \leq i \leq t$, then $[G : (H_1 \cap \cdots \cap H_t)] \leq n_1 \cdots n_t$. This because any coset $(\cap H_i)g = \cap H_i g$ is determined by the cosets $H_1 g, \cdots, H_t g$.

Proposition 5.1.1. *Let G be a group. Any subgroup H of finite index n contains a normal subgroup H_1 of finite index. Actually we can take $H_1 = \cap\{g^{-1}Hg \mid g \in G\}$ and thus $[G : H_1] \leq n!$.*

Proof. Rowen page 297. □

Now let H be a subgroup of finite index in a group G. We say that a subset $T = \{g_1, \cdots, g_n\}$ is a left transversal of H in G if T contains precisely one element of each left coset Hg of G (with $g \in G$). It is easily seen that for any field K the group ring $K[G]$ is a free left $K[H]$-module with basis T. We then obtain a mapping

$$\psi : K[G] \to M_n(K[H])$$

defined by

$$\psi(g)(g_i) = h_i g_{\sigma(i)},$$

where $h_i \in H$ and $1 \leq \sigma(i) \leq n$ are such that $g_i g = h_i g_{\sigma(i)}$. The mapping

$$\sigma : \{1, \cdots, n\} \to \{1, \cdots, n\}$$

is injective. Indeed, if $\sigma(i) = \sigma(j)$ then $h_i^{-1}g_ig = h_j^{-1}g_jg$. Thus $h_i^{-1}g_i \in Hg_i \cap Hg_j$, and therefore $i = j$. It follows that σ is a permutation and

$$\psi(g) = \sum_{i=1}^{n} h_i e_{\sigma(i),i}.$$

In case H is abelian we can take determinants and obtain

$$\det\psi(g) = (\mathrm{sgn}\sigma)h_1 \cdots h_n.$$

Forgetting the sign we obtain a group homomorphism

$$\tilde{\psi} : G \to H : g \mapsto h_1 \cdots h_n.$$

Note that $G' \subseteq \ker \tilde{\psi}$.

If $H = Z(G)$, the centre of G and $g \in G' \cap H$, then it is easily seen that $h_i = g$ for each i. Thus $1 = \tilde{\psi}(g) = g^n$. So we have shown the following property.

Proposition 5.1.2. *If G is a group with $[G : Z(G)] = n$, then $G' \cap Z(G)$ has exponent a divisor of n.*

Proposition 5.1.3. *Let $G = \langle g_1, \cdots, g_m\rangle$ be a finitely generated group. If H is a subgroup of index n, then H is finitely generated by nm elements.*

Proof. Let $T = \{1 = t_1, \cdots, t_n\}$ be a transversal for H in G. Then

$$(Ht_i)g_j = Ht_{\sigma(i)}$$

for a suitable permutation σ. Hence

$$t_ig_j = h_{ij}t_{\sigma(i)}$$

for suitable $h_{ij} \in H$. Let

$$H_0 = \langle h_{ij} \mid 1 \le i \le n,\ 1 \le j \le m\rangle \text{ and } G_0 = \cup_{i=1}^{n} H_0t_i.$$

We claim that $H_0 = H$. To show this it is sufficient to show that $G_0 = G$. Now

$$G_0g_j = \cup H_0t_ig_j = \cup H_0h_{ij}t_{\sigma(i)} = \cup H_0t_{\sigma(i)} = G_0.$$

Hence $G_0 = G_0G \supseteq G$. □

Theorem 5.1.4. *Let G be a group. If $[G : Z(G)] = n$ then $|G'| \le n^{n^3+1}$.*

Proof. Let $\{t_1, \cdots t_n\}$ be a transversal for $Z(G)$ in G. A commutator is then an element of the form

$$[z_1t_i, z_2t_j] = [t_i, t_j],$$

where $z_1, z_2 \in Z(G)$. Hence there are at most n^2 distinct commutators; and these generate G'. Let $m = n^3$. The abelian group $G' \cap Z(G)$ has index at most n in G'. Thus, by a previous proposition, $G' \cap Z(G)$ is generated by at most m elements. So $G' \cap Z(G)$ is a direct product of m cyclic groups, and by a previous proposition each of the generators has order at most n. Thus $|G' \cap Z(G)| \leq n^m$ and therefore $|G'| \leq n^{m+1}$. □

Let G be a group and

$$\begin{aligned} \Delta(G) &= \{g \in G \mid g \text{ has finitely many conjugates}\} \\ &= \{g \in G \mid C_G(g) \text{ has finite index in } G\} \end{aligned}$$

It is easily verified that $\Delta(G)$ is a characteristic subgroup of G and $\Delta(\Delta(G)) = \Delta(G)$. This group is called the *finite conjugate centre* of G. Any group G with $G = \Delta(G)$ is called an *f.c. group.*

If we denote by $\hat{A} = \sum_{a \in A} a$, then it is well known that the elements $\hat{A}$, with A a finite conjugacy class in G, form a K-basis for $Z(K[G])$ (with K a field).

Corollary 5.1.5. *Let G be a group. Suppose $H = \langle h_1, \cdots, h_t \rangle$ is a subgroup of $\Delta(G)$. The following properties hold:*

1. $[H : Z(H)] \leq [G : C_G(H)] \leq \prod [G : C_G(h_i)]$,
2. *H' is a finite group,*
3. *if H_{tor} is the set of the elements of finite order in H, then H_{tor} is a finite normal subgroup of H, and H/H_{tor} is torsion-free abelian.*

Proof. (1) This follows from an early remark in this section and from the following facts: $Z(H) = H \cap C_G(H)$ and $C_G(H) = \cap_{i=1}^{t} C_G(h_i)$.

(2) Apply (1) to Theorem 5.1.4 (since $C_G(h_i)$ has finite index).

(3) Since H' is finite we get that $H_{tor}/H' \cong (H/H')_{tor}$, which is finite and normal in the finitely generated abelian group H/H'. Thus H_{tor} is finite and normal in H. Moreover, $H/H_{tor} \cong (H/H')/(H/H')_{tor}$ is torsion-free abelian. □

For a group G we denote by $\Delta(G)^+$ the torsion elements in $\Delta(G)$.

Corollary 5.1.6. *Let G be a group. Then*

1. *$\Delta(G)$ and $\Delta(G)^+$ are characteristic subgroups of G.*
2. *$\Delta(G)/\Delta(G)^+$ is torsion-free abelian.*
3. *$\Delta(G)^+$ is generated by the finite normal subgroups of G.*

Lemma 5.1.7. *Let G be a group. If G is a finite union of cosets of subgroups $H_1, \cdots, H_m$ of G, then some H_i has finite index in G.*

Proof. We prove this by induction on m. If $m = 1$ the result is obvious. So we may assume $m > 1$ and $[G : H_m]$ is infinite. Write

$$G = \cup_{i=1}^{m} \cup_{j=1}^{t_i} H_i g_{ij}.$$

Some coset $H_m g$ does not appear among the $H_m g_{mj}$. Since the cosets are disjoint we have

$$H_m g \subseteq \cup_{i=1}^{m-1} \cup_{j=1}^{t_i} H_i g_{ij}.$$

But each

$$H_m g_{mj} = H_m g g^{-1} g_{mj} \subseteq \cup_{i=1}^{m-1} \cup_{j=1}^{t_i} H_i g_{ij} g^{-1} g_{mj}.$$

So G is a finite union of cosets of $H_1, \cdots, H_{m-1}$. The result therefore follows by induction. □

Definition 5.1.8. *Let H be a subgroup of a group G and K a field. Define*

$$\pi_H : K[G] \to K[H] : \sum_{g \in G} k_g g \mapsto \sum_{g \in H} k_g g.$$

This map is a left and right $K[H]$-module homomorphism.

Theorem 5.1.9. *Let K be a field, G a group and $\pi = \pi_{\Delta(G)}$. Let $\alpha, \beta, \gamma, \delta \in KG$ and suppose that for all $x \in G$ we have $\alpha x \beta = \gamma x \delta$. Then*

1. *$\pi(\alpha)\beta = \pi(\gamma)\delta$, and*
2. *$\pi(\alpha)\pi(\beta) = \pi(\gamma)\pi(\delta)$.*

Proof. To prove (1), suppose on the contrary that $\pi(\alpha)\beta \neq \pi(\gamma)\delta$. Then pick an element $v \in \operatorname{supp}(\pi(\alpha)\beta - \pi(\gamma)\delta)$.

Let $\operatorname{supp}\, \pi(\alpha) \cup \operatorname{supp} \pi(\gamma) = \{u_1, u_2, \ldots, u_r\}$ and let $W = \cap_i C_G(u_i)$. Since each $u_i \in \Delta(G)$ it follows that $(G : C_G(u_i)) < \infty$. Hence (as mentioned in the introduction of this chapter) it follows that $[G : W] < \infty$.

Write $\alpha = \pi(\alpha) + \alpha'$, $\gamma = \pi(\gamma) + \gamma'$, $\pi(\alpha), \pi(\gamma) \in K(\phi)$ and $\operatorname{supp} \alpha' \cap \phi = \emptyset$, $\operatorname{supp} \gamma' \cap \Delta(G) = \emptyset$. Also

$$\begin{aligned} \alpha' &= \textstyle\sum a_i y_i, \quad \gamma' = \sum c_i y_i \\ \beta &= \textstyle\sum b_i z_i, \quad \delta = \sum d_i z_i \end{aligned}$$

with $a_i, b_i, c_i, d_i \in K$, $y_i, z_i \in G, y_i \notin \Delta(G)$. If y_i is conjugate to $v z_j^{-1}$ in G, fix $h_{ij} \in G$ with $h_{ij}^{-1} y_i h_{ij} = v z_j^{-1}$.

Let $x \in W$. Then, from the hypothesis it follows that

$$\begin{aligned} 0 &= x^{-1}\alpha x \beta - x^{-1}\gamma x \delta \\ &= x^{-1}\big(\pi(\alpha) + \alpha'\big)x\beta - x^{-1}\big(\pi(\gamma) + \gamma'\big)x\delta \\ &= \big(x^{-1}\pi(\alpha)x\beta - x^{-1}\pi(\gamma)x\delta\big) + x^{-1}\alpha' x\beta - x^{-1}\gamma' x\delta \\ &= \big(\pi(\alpha)\beta - \pi(\gamma)\delta\big) + (x^{-1}\alpha' x\beta - x^{-1}\gamma' x\delta). \end{aligned}$$

Since v appears in the support of the first term it must also show up in the second. Thus there exist y_i, z_i with $v = x^{-1}y_i x z_j$ and therefore, $x^{-1}y_i x = vz_j^{-1} = h_{ij}^{-1}y_i h_{ij}$. Thus $xh_{ij}^{-1} \in C_G(y_i)$ and $x \in C_G(y_i)h_{ij}$. So we have shown that

$$W \subseteq \bigcup_{i,j} C_G(y_i)h_{ij}.$$

Since $[G : W] < \infty$ we can write $G = \cup W w_k$ for finitely many $w_k \in G$. Hence

$$G = \bigcup_{i,j,k} C_G(y_i)h_{ij}w_k,$$

a finite union of cosets. Hence Lemma 5.1.7 implies that $\big[G : C_g(y_i)\big] < \infty$ for some i. However this yields a contradiction as $y_i \notin \Delta(G)$. This finishes the proof of (1).

Next we prove (2), that is, $\pi(\alpha)\pi(\beta) = \pi(\gamma)\pi(\delta)$. Write $\beta = \pi(\beta) + \beta'$, $\delta = \pi(\delta) + \delta'$ with $\mathrm{supp}\beta' \cap \Delta(G) = \emptyset$ and $\mathrm{supp}\,\delta' \cap \Delta(G) = \emptyset$. Because of part (1)

$$\begin{aligned} 0 &= \pi(\alpha)\beta - \pi(\gamma)\delta \\ &= \pi(\alpha)\big(\pi(\beta) + \beta'\big) - \pi(\gamma)\big(\pi(\delta) + \delta'\big) \\ &= \big(\pi(\alpha)\pi(\beta) - \pi(\gamma)\pi(\delta)\big) + \big(\pi(\alpha)\beta' - \pi(\gamma)\delta'\big). \end{aligned}$$

The support of the first term is contained in $\Delta(G)$ but that of the second term is disjoint from $\Delta(G)$. Hence $\pi(\alpha)\pi(\beta) - \pi(\gamma)\pi(\delta) = 0$. This proves part (2). □

As an immediate consequence we obtain the following result.

Corollary 5.1.10. *Let G be a group and K a field, and assume I_1, I_2 are ideals of $K[G]$. If $I_1 I_2 = \{0\}$ then $\pi_{\Delta(G)}(I_1)\pi_{\Delta(G)}(I_2) = \{0\}$.*

Lemma 5.1.11. *Assume $r_{11}, \cdots, r_{t1}, r_{12}, \cdots, r_{t2} \in K[G]$. If*

$$\sum_{i=1}^{t} r_{i1} g r_{i2} = 0 \text{ for all } g \in G,$$

then

$$\sum_{i=1}^{t} r_{i1}\pi_{\Delta(G)}(r_{i2}) = 0$$

and

$$\sum_{i=1}^{t} \pi_{\Delta(G)}(r_{i1})\pi_{\Delta(G)}(r_{i2}) = 0.$$

Let N be a finite subgroup of a group G. Define

$$\hat{N} = \sum_{n \in N} n.$$

It is easily seen that

$$(\hat{N})^2 = |N|\hat{N}$$

and thus

$$\hat{N}(\hat{N} - |N|1) = 0.$$

Furthermore, $\hat{N}$ is central in $K[G]$ if and only of N is a normal subgroup of G.

Theorem 5.1.12. *Let K be a field and G a group. The following conditions are equivalent:*

1. *$K[G]$ is prime,*
2. *$Z(K[G])$ is an integral domain,*
3. *G has no nontrivial finite normal subgroups,*
4. *$\Delta(G)$ is torsion-free abelian,*
5. *$K[\Delta(G)]$ is an integral domain.*

Proof. (1) implies (2). Suppose $r_1, r_2 \in Z(K[G])$ with $r_1 r_2 = 0$. Then $I = r_1 K[G]$ and $J = r_2 K[G]$ are two-sided ideals of $K[G]$ with $IJ = \{0\}$. Because, by assumption, $K[G]$ is prime, it follows that $I = \{0\}$ or $J = \{0\}$. Therefore $r_1 = 0$ or $r_2 = 0$. hence $Z(K[G])$ is a domain.

(2) implies (3). Let N be a finite normal subgroup of G. Then $\hat{N}$ is central in $K[G]$ and $\hat{N}(\hat{N} - |N|1) = 0$. Because $\hat{N} \neq 0$ and $Z(K[G])$ is a domain, we obtain that $\hat{N} = |N|1$. Hence $N = \{1\}$.

(3) implies (4) The assumptions and Corollary 5.1.6 imply that $\Delta^+(G) = \{1\}$ and $\Delta(G)$ is torsion-free abelian.

(4) implies (5) The assumptions and Lemma 4.1.9 imply at once that $K[\Delta(G)]$ is a domain.

(5) implies (1). Let I and J be two ideals of $K[G]$ with $IJ = \{0\}$. Then by Corollary 5.1.10 we have $\pi_{\Delta(G)}(I)\pi_{\Delta(G)}(J) = \{0\}$. Since, by assumption $K[\Delta(G)]$ is a domain, it follows that either $\pi_{\Delta(G)}(I) = \{0\}$ or $\pi_{\Delta(G)}(J) = \{0\}$. Since I and J are ideals it then also follows that either $I = \{0\}$ or $J = \{0\}$. □

One also proves the following theorem.

Theorem 5.1.13. *Let K be a field and G a group.*

1. *If $char(K) = 0$ then $K[G]$ is semiprime.*

2. *If $char(K) = p > 0$ then $K[G]$ is semiprime if and only if $\Delta(G)^p = \{1\}$ (here $\Delta(G)^p$ is the subgroup of $\Delta(G)^+$ generated by all elements of order a power of p. Or equivalently, G has no finite normal subgroup whose order is divisible by p.*

Proof. Because of Theorem 2.4.5 we know that $K[G]$ does not have non-zero nil left ideals if $\mathrm{char}(K) = 0$. Hence $K[G]$ is semiprime in this case.

So suppose now that $\mathrm{char}(K) = p > 0$. If G has a finite normal subgroup N whose order is divisible by p then $\widehat{N} = \sum_{x \in N} x$ is a central element of square zero. Thus $\widehat{N}K[G] = I$ is an ideal of square zero and thus $K[G]$ is not semiprime.

Conversely, suppose $K[G]$ is not semiprime, that is, suppose there exists a non-zero ideal I of $K[G]$ so that $I^2 = \{0\}$. Then Corollary 5.1.10 implies that $\pi_{\Delta(G)}(I) \neq \{0\}$ and $\pi_{\Delta(G)}(I)^2 = \{0\}$. Theorem 2.4.5 then implies that $\Delta(G)$ has a p-element, say g. Clearly we then have that $g \in \Delta(G)^+$ and because of Corollary 5.1.6 g belongs to a a normal finite subgroup N of G. □

5.2 Semigroup algebras

Only quite recently has a characterization been obtained of semiprime semigroup algebras $K[S]$ with S a subgroup of a group G. In general the following problem remains open.

Problem 6: When is a (contracted) semigroup algebra a (semi)prime ring?

Chapter 6

Maximal Orders

Let R be a commutative ring and S an R-algebra.

One says that $s \in S$ is *integral over* R if s is the root of a monic polynomial in one variable with coefficients in R. That is, s is integral over R if $s^n + r_{n-1}s^{n-1} + \cdots + r_1 s + r_0 1_S = 0$ for some $r_0, r_1, \ldots, r_{n-1} \in R$. If every element of S is integral over R then we say that S is *integral over* R. If every element of S which is integral over R belongs to $R1_S$ then we say that R is *integrally closed* in S. If P is a prime ideal of R and $a \in S$ is integral over R then $\frac{a}{x}$ is integral over R_p for every $x \in R \setminus P$. Hence, if S is integral over R then S_P is integral over R_P.

Proposition 6.0.1. *Let R be a commutative ring and let S be an R-algebra. The following conditions are equivalent for an element $s \in S$.*

1. *s is integral over R.*
2. *$R[s]$ is finitely generated as R-module.*
3. *$R[s]$ is contained in a subring T of S which is finitely generated as R-module.*
4. *There is a faithful $R[s]$-submodule M that is finitely generated as an R-module.*

Proposition 6.0.2. *Let R be a commutative ring and let S be an R-algebra. The following properties hold.*

1. *If $s_1, \ldots, s_n \in S$ are integral over R and $s_i s_j = s_j s_i$ for every i, j then $R[s_1, \ldots, s_n]$ is finitely generated over R. In particular every element of $R[s_1, \ldots, s_n]$ is integral over R.*
2. *If T is a subring of $Z(S)$ containing $R1_S$ and T is integral over R, then an element $s \in S$ is integral over T if and only if it is integral over R. In particular, if S is integral over T and T is integral over R then S is integral over R.*

If the R-algebra S is commutative then, by Proposition 6.0.2, the set of elements of S which are integral over R form a ring called the *integral closure of R in S*. The integral closure of R in S is the unique maximal subring of S which is integral over R and integrally closed in S.

For domains one uses the terminology "integrally closed" and "integral closure" in the following absolute meaning. A domain R is said to be *integrally closed* if it is integrally closed in its field of fractions F. The *integral closure* of R is its integral closure in F.

Example 6.0.3. If R is a unique factorization domain then R is integrally closed.

Proof. Let $\alpha = \frac{r}{s}$ with r and s coprime elements of R. We will prove that if α is integral over R then $s \in U(R)$. This implies that $\alpha \in R$ as desired. Suppose that $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$, with $a_i \in R$ for every i. Then $r^n + a_{n-1}r^{n-1}s + a_{n-2}r^{n-2}s^2 + \cdots + a_1rs^{n-1} + a_0s^n = 0$. If s is not a unit in R then s has an irreducible divisor in R, say t. Thus t divides r^n, and hence t divides r in R. This contradicts the assumption that r and s are coprime in R and hence the claim is proved. □

Proposition 6.0.4. *Let R be a domain with field of fractions F and let A be an F-algebra.*

1. *If $a \in A$ is algebraic over F then there is $r \in R \setminus \{0\}$ such that ra is integral over R.*

2. *If A is finite dimensional over F then A contains a basis over F formed by elements which are integral over R.*

Proof. (1) Assume that $a^n + b_{n-1}a^{n-1} + \cdots + b_1a + b_0 = 0$, with each $b_i \in F$. Let $0 \neq r \in R$ such that $rb_i \in R$ for every i. Then ra is a root of $X^n + rb_{n-1}X^{n-1} + r^2b_{n-2}X^{n-2} + \cdots + r^{n-1}b_1X + r^nb_0 \in R[X]$. Hence ra is integral over R.

(2) is an immediate consequence of (1). □

Lemma 6.0.5 (Gauss Lemma)**.** *Let R be an integrally closed domain with field of fractions F. If $f, g \in F[X]$ are monic and $fg \in R[X]$ then $f, g \in R[X]$.*

Proposition 6.0.6. *Let R be an integrally closed domain with field of fractions F. Let A be an F-algebra and let $a \in A$. Then, a is integral over R if and only if a is algebraic over F and $Min_F(a) \in R[X]$.*

Proof. (1) Assume that a is algebraic over F and let $f = Min_F(a)$. If $f \in R[X]$ then a is integral over R. Conversely, assume that a is integral over R and let g be a monic element in $R[X]$ with $g(a) = 0$. Then a is algebraic over F and $f = Min_F(a)$ divides g in $F[X]$. Therefore $f \in R[X]$, by the Gauss Lemma (Lemma 6.0.5). □

Of course, every ring S is a $\mathbb{Z}$-algebra in the obvious way. One simply says "integral" to mean "integral over $\mathbb{Z}$". In case S is commutative, the integral closure of $\mathbb{Z}$ in S is called the *ring of integers of* S.

Example 6.0.7. *Let d be a square-free integer and let R be the ring of integers of $\mathbb{Q}(\sqrt{d})$. Then*

$$R = \begin{cases} \mathbb{Z}[\sqrt{d}], & \text{if } d \not\equiv 1 \mod 4; \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}], & \text{otherwise.} \end{cases}$$

If R is a subring of the center of S then we consider S as an R-algebra in the obvious way. If I is an ideal of S then we can consider $R/R \cap I$ as a subring of S/I via the injective map $x + (R \cap I) \mapsto x + I$. It is clear that if $s \in S$ is integral over R then $s + I$ is integral over $R/R \cap I$. In particular, if S is integral over R then S/I is integral over $R/R \cap I$. If Q is a prime ideal of S then $R \cap Q$ is a prime ideal of R. The following result shows that if S is an integral over R then there is a strong relation between chains of prime ideals of R and S.

Theorem 6.0.8. *Let S be a ring and R a subring of the center of S such that S is integral over R. Let Q_1 be a prime ideal of S and $P_1 = R \cap Q_1$.*

1. *If Q_2 is a prime ideal of S properly containing Q_1 then $P_1 \neq Q_2 \cap R$.*
2. *Assume that either S is commutative or S is finitely generated as R-module. Suppose P_2 is a prime ideal of R. If $P_1 \subseteq P_2$ then there is a prime ideal Q_2 of S containing Q_1 such that $Q_2 \cap R = P_2$.*

Proof. The statements of (1) and (2) are unchanged if R and S are replaced by R/P_1 and S/Q_1 respectively. Thus one may assume that $Q_1 = 0$ and hence $P_1 = 0$. Hence, R is a domain and in (1) Q_2 is a non-zero prime ideal Q of S and in (2) P_2 is a non-zero prime ideal P of R.

(1) Let Q be a non-zero prime ideal of S and let $P = Q \cap R$. We have to prove that $P \neq 0$. We know that Q_P is a non-zero prime ideal of S_P. Replacing R by R_P and S by S_P, one may assume that R is local and P is the unique maximal ideal of R. Indeed, if we assume the result holds for R a local domain, then it follows that $Q_P \cap R_P \neq 0$. Therefore, $\frac{q}{x} = \frac{r}{y} \neq 0$ for some $q \in Q$, $r \in R$ and $x, y \in R \setminus P$. As $\frac{y}{1}$ is invertible in S_P we have $0 \neq \frac{yq}{x} = r$, so that $0 \neq yq = xr \in Q \cap R$, as desired.

So assume that R is a local domain and P is the unique maximal ideal of R. By means of contradiction, assume $P = 0$. Then R is a field. If $0 \neq s \in Q$ and $s^n + r_{n-1}s^{n-1} + \cdots + r_1 s + r_0 = 0$, with $r_i \in R$ and n minimal, then $0 \neq r_0 = -s(s^{n-1} + r_{n-1}s^{n-1} + \cdots + r_1)$ and therefore s is an invertible element of Q. This yields a contradiction with the fact that $Q \neq S$. Thus $P \neq 0$, as desired.

(2) Let P be a non-zero prime ideal of R. We have to prove that there is an ideal Q of S such that $R \cap Q = P$. Localizing at P one may assume that R is local with unique maximal ideal P. Indeed, if we assume the result holds in this case then S_P has a prime ideal Q' such that $Q' \cap R_P = P_P$. Now $Q' = Q_P$ for some prime ideal Q of S such $Q \cap (R \setminus P) = \emptyset$. Then $P_P = Q_P \cap R_P = (Q \cap R)_P$ and therefore $P = P_P \cap R = (Q \cap R)_P \cap R = Q \cap R$. So we prove the result assuming that P is the only maximal ideal of R. We claim that $PS \neq S$. Otherwise $1 = \sum_{i=1}^{k} x_i s_i$ with $x_i \in P$ and $s_i \in S$. If S is commutative then let $T = R[s_1, \ldots, s_k]$ and otherwise let $T = S$. By assumption, in both cases T is finitely generated as R-module. Thus $T = Rt_1 + \cdots + Rt_n$ for some $t_1, \ldots, t_n \in T$. Moreover $t_i = \sum_{j=1}^{n} y_{ij} t_j$ for $y_{ij} \in P$. Then $\sum_{j=1}^{n} (\delta_{ij} - y_{ij}) t_j = 0$ for every i. Thus if A is the $n \times n$ matrix having $\delta_{ij} - y_{ij}$ at the (i, j)-th entry and t is the $n \times 1$ vector with t_i at the i-th entry then $Am = 0$. Then $\det(A)t = \mathrm{Adj}(A)Am =$ and hence $\det(A)T = 0$. As $1 \in T$, we have $0 = \det(A) \equiv 1 \mod P$, so that $1 \in P$, a contradiction. This proves the claim. Therefore, PS is a proper ideal of S and hence it is contained in a maximal ideal Q of S. So, $R \cap Q$ is prime ideal of R containing P and hence $P = R \cap Q$. □

By Theorem 6.0.8, for every ascending finite chain $Q_1 \subset Q_2 \subset \cdots \subset Q_k$ of prime ideals of S, $P_1 = Q_1 \cap R \subset Q_2 \cap R \subset \cdots \subset Q_k \cap R$ is an ascending chain of prime ideals of R. Vice versa, if $P_1 \subset P_2 \subset \cdots \subset P_k$ is an ascending chain of prime ideals of R then there is an ascending chain $Q_1 \subset Q_2 \subset \cdots \subset Q_k$ of ideals of S with $P_i = Q_i \cap R$ for every i. Statement (2) of Theorem 6.0.8 is known as *Going Up Theorem*. There is a dual Going Down Theorem.

The ring of integers R of a number field shares many properties with the ring $\mathbb{Z}$ of integral numbers. However, in general R is not a unique factorization domain and thus not a principal ideal domain (abbreviated as PID). This implies that the ideal and module theory of R is more complicated than that of principal ideal domains. However, as we will see in this section, for every maximal ideal P of R, the local ring R_P is a PID. Using this and localization techniques one can obtain a nice description of the ideal and module theory of R.

A discrete valuation ring is a commutative local principal ideal domain which is not a field. A Dedekind domain is a commutative noetherian domain R such that R_P is discrete valuation ring for every non-zero prime ideal P of R. For example, every PID is a Dedekind domain. We will see that the ring of integers of a number field also is a Dedekind domain. The following theorem describes the ideal theory of Dedekind domains.

Theorem 6.0.9. *Let R be a Dedekind domain. If I is a non-zero and proper ideal of R then $I = P_1^{e_1} \ldots P_k^{e_k}$ for some maximal ideals $P_1, \ldots, P_k$ of R and some positive numbers $e_1, \ldots, e_n$. The maximal ideals $P_1, \ldots, P_k$ and the*

numbers e_i are uniquely determined by the following conditions: $P_1, \ldots, P_k$ are the maximal ideals of R containing I and $I_{P_i} = (P_{iP_i})^{e_i}$.

Let R be a Dedekind domain and I a non-zero and proper ideal of R. The factorization of I is the expression $I = P_1^{e_1} \cdots P_k^{e_k}$, with $P_1, \ldots, P_k$ the different maximal ideals containing I of R and $e_1, \ldots, e_k$ positive integers. We will use the following notation:

$$e_P(I) = \max\{n \geq 0 : I \subseteq P^n\},$$

for P a maximal ideal of R. Then $e_P(I) = 0$ for almost all $P \in Max(R)$,

$$I = \prod_{P \in Max(R)} P^{e_P(I)}$$

and the factorization of I is obtained by dropping in the previous expression the factors with $e_P(I) = 0$.

The proof of 6.0.9 is based on the properties of localization and the following two additional lemmas.

Lemma 6.0.10. *The following properties hold for a commutative noetherian ring R such that every prime ideal of R is maximal.*

1. *Every ideal of R contains the product of finitely many maximal ideals of R.*
2. *R has finitely many maximal ideals.*
3. *If $P_1, \ldots, P_n$ are the distinct maximal ideals of R then $0 = P_1^{a_1} \cdots P_n^{a_n}$ for some positive integers $a_1, \ldots, a_n$.*

Proof. (1) We argue by contradiction. So assume that the statement is false. Because R is noetherian, there then exists an ideal I of R which is maximal amongst the ideals that do not contain a product of maximal ideals. In particular, I is not maximal and thus, by the assumption, I is not prime. Hence there exist $x, y \in R \setminus I$ so that $xy \in I$. Therefore both $I + Rx$ and $I + Ry$ are ideals of R properly containing I. Thus, $P_1 \cdots P_k \subseteq I + Rx$ and $Q_1 \cdots Q_l \subseteq I + Ry$ for some maximal ideals $P_1, \ldots, P_k, Q_1, \ldots, Q_l$ of R. Consequently, $P_1 \cdots P_k Q_1 \cdots Q_l \subseteq (I + Rx)(I + Ry) \subseteq I$, a contradiction.

(2) and (3) As a particular case of (1), $0 = P_1^{a_1} \cdots P_k^{a_k}$ for $P_1, \ldots, P_k$ distinct maximal ideals of R and $a_1, \ldots, a_k > 0$. If P is an arbitrary maximal ideal of R then from $P_1^{a_1} \cdots P_k^{a_k} \subseteq P$ we deduce that $P_i \subseteq P$ for some i. As P_i is maximal, $P_i = P$. □

Lemma 6.0.11. *Let R be a commutative domain such that R_Q is a PID for every maximal ideal Q of R. Let P be a non-zero prime ideal of R and m a positive integer. Then P is maximal in R, $R/P^m \cong R_P/(P^m)_P$ (as rings), every ideal of R/P^m is a power of P/P^m and $\dim_{R/P}(P^{m-1}/P^m) = 1$.*

Proof. We first show that P is a maximal ideal. So, suppose Q is a prime ideal of R with $P \subset Q$. Then, P_Q and Q_Q are distinct non-zero prime ideals of R_Q. As R_Q is a PID, both P_Q and Q_Q are maximal and this contradicts with the fact that R_Q is local.

The kernel of the natural map $f : R \to R_P/(P^m)_P$ is P^m. Since R_P is a local PID, every ideal of $R_P/(P^m)_P$ is a power of $P_P/(P^m)_P$. Hence, to prove the second and third part of the statement it is enough to show that f is surjective. To do so, let $r/s \in R_P$, where $r \in R$ and $s \in R \setminus P$. Then $Rs+P = R$, because P is maximal in R. This implies that $Rs+P^m = R$ and thus $1 = xs + q$, for some $x \in R$ and $q \in P^m$. Then $f(rx) = rx + (P^m)_P = r(1/s - q/s) + (P^m)_P = r/s + (P^m)_P$. So, indeed f is surjective.

Because of the isomorphism $R/P^m \cong R_P/(P^m R)_P$, to prove the last part, we may replace R by R_P. Hence, we may assume that R is a local PID. So, $P = pR$ for some $p \in R$ and the map $x \mapsto xp^{m-1}$ gives an isomorphism $R/P \to P^{m-1}/P^m$. Consequently, $\dim_{R/P}(P^{m-1}/P^m) = 1$. □

Proof of Theorem 6.0.9. Let I be a non-zero and proper ideal in a Dedekind domain R. Because of Lemma 6.0.11, every prime ideal of the ring R/I is maximal. Hence, we may apply Lemma 6.0.10 to the Noetherian ring R/I and we deduce that I contains $J = P_1^{b_1} \dots P_k^{b_k}$, where $P_1, \dots, P_k$ are the unique maximal ideals of R containing I and each b_i is a positive integer. The Chinese Remainder Theorem then yields that $R/J \cong R/P_1^{b_1} \times \cdots \times R/P_k^{b_k}$. By Lemma 6.0.11, for $1 \leq i \leq k$, the natural projection of I/J in $R/P_i^{b_i}$ is of the form $P_i^{a_i}/P_i^{b_i}$, for some positive integer a_i. As all the projections of I/J and $P_1^{a_1} \dots P_k^{a_k}/J$ coincide, we get that $I = P_1^{a_1} \dots P_k^{a_k}$. The uniqueness of the a_i's follows from the fact that each a_i is uniquely determined by the equality $I_{P_i} = (P_i P^i)^{a_i}$, as R_{P_i} is a principal ideal domain which is not a field. This finishes the proof of Theorem 6.0.9.

We give two alternative characterizations of Dedekind domains.

Theorem 6.0.12. *The following statements are equivalent for a domain R.*

1. *R is Dedekind domain.*
2. *R_P is a principal ideal domain for every non-zero prime ideal P of R and every non-zero element of R is contained in only finitely many ideals of R.*
3. *R is noetherian, integrally closed and each non-zero prime ideal of R is maximal.*

Proof. Let R be a domain that is not a field and let F be its field of fractions.

(1) implies (2) is a consequence of the definition of Dedekind domain and Theorem 6.0.9.

(2) implies (3). Assume that R satisfies (2). By Lemma 6.0.11, every non-zero prime ideal of R is maximal. Let $\alpha \in F$ be integral over R. Then

α is integral over R_P, for every maximal ideal P of R. Because of Example 6.0.3, each R_P is integrally closed and thus $\alpha \in R_P$. This proves that $\alpha \in \cap_{P \in Max(R)} R_P$. Thus $\alpha \in R$. This proves that R is integrally closed.

It remains to show that R is noetherian. Let I be a non-zero ideal of R. If P is a maximal ideal of R then R_P is a principal ideal domain and therefore $I_P = x_P R_P$, for some $x_P = r_P/s_P$ with $r_P \in I$ and $s_P \in R \setminus P$. Then $I_P = r_P R_P$. Let $0 \neq a \in I$. By assumption a is contained in finitely many maximal ideals, say $P_1, \ldots, P_n$. Let $J = Ra + Rr_{P_1} + \cdots + Rr_{P_n}$, an ideal contained in I. If P is a maximal ideal of R then either $P = P_i$ for some i or a is invertible in R_P. In the former case $J_P = I_P$, because $r_P \in J$. In the latter case, $J_P = R_P$ and hence $I_P = R_P$. One deduces that $I = J$. So, indeed, I is finitely generated and hence R is noetherian.

(3) implies (1). Assume that R satisfies the conditions of (3). If P is a maximal ideal of R then R_P satisfies the conditions of (3). Thus, replacing R by R_P, we may assume without loss of generality that R has a unique non-zero prime ideal P and we have to show that every ideal of R is principal. Fix a non-zero element a in P and, for every $x \in R$, let $J_x = \{y \in R : xy \in Ra\}$. Clearly, each J_x is an ideal of R. As R is noetherian, the set of ideals of the form J_x, with $x \in R \setminus Ra$, contains a maximal element J_b, with $b \in R \setminus Ra$. We claim that $J_b = P$. As $0 \neq a \in J_b$, $1 \notin J_b$ and P is the unique non-zero prime ideal of R, it is enough to show that J_b is prime in R. We prove this by contradiction. So assume there are $x, y \in R$ such that $xyb \in Ra$, $xb \notin Ra$ and $yb \notin Ra$. Hence, J_{xb} contains J_b properly and $xb \in R \setminus Ra$. This contradicts with the choice of b. Thus $J_b = P$.

Consider $x = a/b \in F$. Since $b \notin Ra$, $x^{-1} \notin R$. Hence, because by assumption because R is integrally closed, x^{-1} is not integral over R.

We claim that $P = Rx$, or equivalently $Px^{-1} = R$. For this, first note that $Pb = J_b b \subseteq Ra$. Hence, Px^{-1} is an ideal of R. If it is a proper ideal of R then $Px^{-1} \subseteq P$ and therefore P is a $R[x^{-1}]$-submodule of F which is finitely generated over R. Proposition 6.0.1 therefore implies that x^{-1} is integral over R, a contradiction. This proves the claim.

Let now I be a non-zero ideal of R. We claim that $Ix^{-n} \neq Ix^{-(n+1)}$ for every n. Otherwise, Ix^{-n} is a finitely generated faithful $R[x^{-1}]$-submodule of F. Then x^{-1} is integral over R. This yields a contradiction and so the claim is proved. Thus $I \subset Ix^{-1} \subset Ix^{-2} \subset \ldots$ is a strictly ascending chain of R-submodules of F. As R is noetherian, at least one of the terms of the chain is not contained in R. Let n be the largest non-negative integer so that $Ix^{-n} \subseteq R$. Because $P = Rx$ we obtain that $Ix^{-n} \not\subseteq P$. Hence, $Ix^{-n} = R$, or equivalently I is principally generated by x^n, as desired. □

The following lemma is sometimes called the Approximation Lemma.

Lemma 6.0.13. *Let R be a Dedekind domain with field of fractions F. Let $P_1, \ldots, P_k$ be different non-zero prime ideals of R, $x_1, \ldots, x_k \in F$ and*

$n_1, \ldots, n_k \in \mathbb{Z}$. Then F has an element x such that

$$e_{P_i}(x - x_i) \geq n_i \text{ and } e_Q(x) \geq 0$$

for every $i = 1, \ldots, k$ and every maximal ideal Q of R different from $P_1, \ldots, P_k$.

Proof. Let r be a non-zero element of R such that $rx_1, \ldots, rx_k \in R$. Let e be the maximum exponent in the factorization of rR and let $Q_1, \ldots, Q_t$ be the maximal ideals of R containing r and different from $P_1, \ldots, P_k$. By the Chinese Remainder Theorem there is $y \in R$ such that $y - rx_i \in P_i^{e+n_i}$ and $y \in Q_j^e$ for every $i = 1, \ldots, k$ and $j = 1, \ldots, t$. Take $x = r^{-1}y$. Then $v_{P_i}(x - x_i) = v_{P_i}(y - rx_i) - v_{P_i}(r) \geq e + n_i - v_{P_i}(r) \geq n_i$, $v_{Q_j}(x) = v_{Q_j}(y) - v_{Q_i}(r) \geq e - v_{Q_j}(r) \geq 0$ and if Q is a maximal ideal different from $P_1, \ldots, P_k, Q_1, \ldots, Q_t$ then $v_Q(x) = v_Q(y) \geq 0$. □

Theorem 6.0.14. *Let R be a Dedekind domain with field of quotients F and let E/F be a finite field extension. Then the integral closure S of R in E is a Dedekind domain which contains a basis of E over F. Moreover, if E/F is separable then S is finitely generated as R-module.*

Proof. Let K denote the separable closure of F in E and T the integral closure of R in K. Then K/F is separable and E/K is purely inseparable. Moreover, by the transitivity of integrality (statement (2) of Proposition 6.0.2), S is the integral closure of T in E. This shows that it is enough to prove the theorem under the assumption that E/F is either separable or purely inseparable.

Assume first that E/F is separable. We check that S satisfies condition (3) of Theorem 6.0.12. By the transitivity of integrality, S is integrally closed. By Theorem 6.0.8, every non-zero prime ideal of S is maximal. Thus it remains to prove that S is noetherian. We will show that S is finitely generated as R-module. Since R is noetherian, this implies that S is noetherian as R module, and hence S is a noetherian ring. From Proposition 6.0.4.(2), S contains a basis $x_1, \ldots, x_n$ of E over F. Let $y_1, \ldots, y_n$ be the dual basis of $x_1, \ldots, x_n$ with respect to the bilinear trace form. If $s \in S$ and $s = \sum_{i=1}^n r_i y_i$, with $r_i \in F$, then $r_i = Tr_{E/F}(sx_i) \in R$, by Proposition 6.0.6. This proves that $S \subseteq Ry_1 \oplus \cdots \oplus Ry_n$. As R is noetherian, we obtain that S is finitely generated as R-module. This finishes the proof for this case.

Now assume that E/F is purely inseparable and let p be the characteristic of F and $q = [E : F]$. Then q is a power of p and $x^q \in F$ for every $x \in E$. If $x \in S$ then $x^q \in F \cap S = R$, because R is integrally closed. Conversely, if $x^q \in R$, then x is integral over R and hence $x \in S$. This proves that $S = \{x \in E : x^q \in R\}$. If P is a maximal ideal of R, let $P' = \{x \in E : x^q \in P\}$. Then P' is a maximal ideal of S and $P' \cap R = P$, because P is prime.

We claim that the maps $Q \mapsto R \cap Q$ and $P \mapsto P'$ give mutually inverse maps between $Max(S)$ and $Max(R)$. Moreover, if $Q \in Max(S)$ and

$P \in Max(R)$ correspond under these maps, then $S_P \cong S_Q$. To prove this, suppose Q is a maximal ideal of S. Then, by Theorem 6.0.8, $Q \cap R$ is a maximal ideal of R. If $x \in Q$ then $x^q \in R \cap Q$. Conversely, if $x^q \in R \cap Q$ then $x \in S$ and hence $x \in Q$, because Q is a prime ideal of S. This shows that $(R \cap Q)' = Q$. This, together with the previous paragraph, proves the first part of the claim. Furthermore, if $P = Q \cap R$ then $x \in Q$ if and only if $x^q \in P$. Using this it is easy to prove that the natural map $S_P \to S_Q$ is an injective homomorphism. Moreover, if $s \in S$ and $x \in S \setminus Q$ then $\frac{s}{x} = \frac{sx^{q-1}}{x^q} \in S_P$. Thus this map is an isomorphism. This finishes the proof of the claim.

We will show that S satisfies condition (2) of Theorem 6.0.12. First, because of the above claim, every non-zero ideal of S is contained in only finitely many maximal ideals of S. It also implies that S_P is a local ring for every maximal ideal P of R and we need to show that S_P is a discrete valuation ring. So, let P be a maximal ideal of R. It remains to show that S_P is a PID. It is readily verified that S_P is the integral closure of R_P in E. Hence, we may replace R by R_P, and assume from the beginning that R is a discrete valuation ring with maximal ideal $P = R \cap Q$, where Q is the unique maximal ideal of S. Choose $a \in R$ so that $P = Ra$. Let M be the ideal of R generated by all elements b^q with $b \in Q$. Since R is a PID with unique maximal ideal, its ideals are totally ordered. Therefore $M = Rb^q = Ra^k$ for some $b \in Q$ and some positive integer k.

We now show that if $0 \neq s \in S$ then $s = wb^t$ for some $w \in U(S)$ and some non-negative integer t. This is clear if $s \in U(S)$. Otherwise $s \in Q$. Then $s^q \in M$ and thus $s^q = ua^d$ for some $u \in U(R)$ and some non-negative integer d. Write $d = kt + r$, with $k, r \in \mathbb{Z}$ and $0 \leq r < k$. Then, for some $v \in U(R)$, we get that $(sb^{-t})^q = s^q b^{-tq} = uva^{d-tk} = uva^r$, for some $v \in U(R)$. Hence, $(sb^{-t})^q \in R \setminus M$ and thus $w = sb^{-t} \in S \setminus Q$. So $w \in U(S)$ and $s = wb^t$, as desired.

Let now I be a non-zero ideal of S. Take $m \geq 0$ the least non-negative integer so that $b^m \in I$. The existence of m is a consequence of the above paragraph. Clearly $Sb^m \subseteq I$. If $0 \neq s \in I$ then, by the above, $s = wb^t$ for some $u \in U(S)$ and $t \geq 0$. The minimality of m guarantees that $t \geq m$. So $s \in Sb^m$ and thus $I = Sb^m$. Hence, S is a PID. □

If E/F is a finite extension of F that is not separable then the integral closure of R in E is not necessarily finitely generated over E. Therefore the proof of Theorem 6.0.14 for the separable case does not work in general.

Corollary 6.0.15. *The ring of integers of a number field is a Dedekind domain and it is finitely generated over* $\mathbb{Z}$.

A commutative integral domain R with field of fractions K is, by definition, a completely integrally closed if for any $x, c \in K$ with $c \neq 0$ and $cR[x] \subseteq R$ implies $x \in R$. Clearly a completely integrally closed domain

is integrally closed. If R is noetherian then both notions are the same. It is easily seen that being completely integrally closed is that same as if $R \subseteq R' \subseteq K$ with R' a subring so that $rR' \subseteq R$ then $R' = R$. One also says that R is a maximal order. Equivalently, a commutative domain R is a maximal order if and only if for any nonzero ideal I of R the set $(I : I) = \{k \in K \mid kI \subseteq I\} = R$.

A noetherian unique factorization domain R is a commutative domain that is a maximal order and so that every minimal nonzero prime ideal (i.e. a prime of height one) is principal.

Gilmer and Chouinard characterized the commutative semigroup algebras that are domains and noetherian maximal orders.

Theorem 6.0.16. *Let S be an abelian cancellative monoid with torsion free group of quotients and let K be a field. Then, $K[S]$ is a noetherian maximal order if and only if S is a maximal order in its group of quotient and S is finitely generated, or equivalently, S is finitely generated and $S = U(S) \cap S_1$ with $S_1 = F^+ \cap S_1 S_1^{-1}$, where F^+ is the positive cone of a free abelian group containing S_1.*

In this case, all height one primes of $K[S]$ are principal if and only if all minimal primes of S are principal.

Obviously, the above definition of maximal order can also be considered in the non-commutative situtation within the classical ring of quotients of a prime ring R.

K. Brown proved the following result. An element α of a group algebra KG is said to be G-normal if $K[G]\alpha = \alpha K[G] = \alpha^g K[G]$ for any $g \in G$. A group G is said to be dihedral free if $[G : N_G(H)] = \infty$ for any subgroup H of G that is isomorphic with the infinite dihedral group $D_\infty = \langle a, b \mid b^2 = 1,\ b^{-1}ab = a^{-1} \rangle$.

Theorem 6.0.17. *Let G be a polycyclic-by-finite group and let K be a field. Then, $K[G]$ is a prime Noetherian maximal order if and only if $\Delta(G)$ is torsion-free and G is dihedral free (for example if G is torsion-free).*

Furthermore, in this case, a height one prime ideal P of $K[G]$ contains a nonzero normal element if and only if $P = K[G]\alpha = \alpha K[G]$ for some G-normal element $\alpha \in K[\Delta(G)]$.

Brown also proved the following result.

Theorem 6.0.18. *Let G be a polycyclic-by-finite group and let K be a field. If $\Delta(G)$ is torsion free (i.e. $K[G]$ is prime) then the following conditions are equivalent.*

1. *Every nonzero ideal of $K[G]$ contains an invertible ideal.*
2. *Every nonzero ideal of $K[G]$ contains a nonzero central element (for example when $K[G]$ is a PI-algebra).*

3. Every nonzero ideal contains a nonzero normal element.

One also now knows when a semigroup algebra $K[S]$ is a noetherian PI domain that is a maximal order.

Chapter 7

Units of Group Rings

In this chapter we study units of the integral group ring $\mathbb{Z}G$ of a (finite) group G. One of the reasons to study this object is to investigate the famous isomorphism problem. This asks whether, for any finite groups G and H

$$\text{if } \mathbb{Z}G \cong \mathbb{Z}H \text{ then } G \cong H.$$

This problem was posed by Higman in 1940. In 1950 Perlis and Walker proved that for abelian finite groups the answer is positive. Actually they showed that if A and B are finite abelian groups so that $\mathbb{Q}A \cong \mathbb{Q}B$ then $A \cong B$. So a finite abelian group is determined by its rational group algebra (and hence also by its integral group ring). In 1987 a real break through was made by Roggenkamp and Scott who proved that the isomorphism problem has a positive answer for nilpotent finite groups. Also for all finite simple groups is the answer positive. So it came as a big surprise that in 2001 Hertweck published a counter example to the isomorphism problem. More precisely he showed that there are two non-isomorphic groups G and H of order $2^{21}97^{28}$ so that $\mathbb{Z}G \cong \mathbb{Z}H$.

7.1 Constructions of units in $\mathbb{Z}G$

Let G be a finite group. In order to study the unit group $\mathcal{U}(\mathbb{Z}G)$ one would of course first like some natural constructions of units. Only few such constructions are known. We give the most important of these.

The trivial units.

Each element $\pm g \in \mathbb{Z}G$ with $g \in G$ is a unit. Its inverse is $- \pm g^{-1}$). These units are called the trivial units of $\mathbb{Z}G$. Thus $\pm G \subseteq \mathcal{U}(\mathbb{Z}G)$..

Note that these units are of finite order (we say that they are torsion units). Of course any conjugate ugu^{-1}, with $g \in G$ and $u \in \mathcal{U}(\mathbb{Z}G)$, also is a torsion unit. Of course for the latter units one needs to know already a unit u. A theorem says that if γ is a torsion unit of $\mathcal{U}(\mathbb{Z}G)$, thus $\gamma^n = 1$ for some n, then n is a divisor of $|G|$.

Bicylic units

If R is a ring and $r \in R$ is such that $r^2 = 0$ then

$$(1 + r)(1 - r) = 1.$$

Hence both $1 + r$ and $1 - r$ are units in R. More generally, if $r^n = 0$ then

$$(1 - r)(1 + r + r^2 + \cdots + r^{n-1}) = 1$$

and

$$(1 + r)(1 - r + r^2 - \cdots + (-1)^n r^{n-1}) = 1.$$

Thus if r is a nilpotent element then both $1 + r$ and $1 - r$ are units. These are called unipotent units.

To apply this to the integral group ring $\mathbb{Z}G$ of a finite group one needs thus constructions of nilpotent elements. Well let $g \in G$ be an element of order n. So $g^n = 1$ and $g^{n-1} \neq 1$. Then

$$(1 - g)(1 + g + g^2 + \cdots + g^{n-1}) = 0$$

and thus, for any $h \in G$

$$\begin{aligned} 0 &= \left((1 - g)h(1 + g + g^2 + \cdots + g^{n-1})\right)^2 \\ &= \left((1 + g + g^2 + \cdots + g^{n-1})h(1 - g)\right)^2. \end{aligned}$$

For simplicity reasons we write

$$\hat{g} = 1 + g + \cdots + g^{n-1}.$$

Thus both

$$u_{g,h} = 1 + (1 - g)h\hat{g} \text{ and } u'_{g,h} = 1 + \hat{g}h(1 - g)$$

are units. They are called bicyclic units.

Of course we would like to know when such a bicylic is a new unit, i.e., when is it not a trivial unit. First of all note that

$$u_{g,h}^n = 1 + n(1 - g)h\hat{g}.$$

Hence if $(1 - g)h\hat{g} \neq 0$ then $u_{g,h}$ is a unit of infinite order, and thus it is not trivial.

Hence $u_{g,h}$ is a non-trivial unit if and only $(1 - g)h\hat{g} \neq 0$. The latter is equivalent with the cyclic group $\langle g \rangle$ is not normalized by h (i.e. $h\langle g \rangle h^{-1} \not\subseteq \langle g \rangle$). Indeed, for if $h\langle g \rangle h^{-1} = \langle g \rangle$ then $h^{-1}\hat{g}h = \hat{g}$, and thus $h\hat{g} = \hat{g}h$ and $u_{g,h} = 1$. Conversely, suppose $u_{g,h}$ is trivial. Then $(1 - g)h\hat{g} = 0$ and thus $h\hat{g} = gh\hat{g}$. Consequently, $h^{-1}gh\hat{g} = \hat{g}$. This means $h^{-1}gh(1 + g + \cdots + g^{n-1}) = 1 + g + \cdots + g^{n-1}$. So, as $h^{-1}gh$ is in the support of the left hand

side, it also must be in the support of the right hand side. Hence $h^{-1}gh = g^j$ for some j. So $h^{-1}\langle g\rangle h \subseteq \langle g\rangle$, as desired.

It follows that all bicylic units are trivial units if and only if every cyclic subgroup, and thus every subgroup of G, is normal in G. Non-abelian groups of this type are called Hamiltonian groups. Such groups have been characterized. They are the groups of the form

$$Q_8 \times E \times A,$$

where Q_8 is the quaternion group of order 8, E is a finite elementary abelian 2-group (that is, every non-trivial element of E has order 2) and A is an abelian group of odd order.

Bass cyclic units

Recall that the mapping $\varphi : \mathbb{N}_0 \setminus \{1\} \longrightarrow \mathbb{N}_0$ defined by

$$\varphi(n) = |\{k \mid 0 < k < n, gcd(k, n) = 1\}|$$

is called the Euler φ function.

If p is a prime number then $\varphi(p) = p - 1$.

Let now C_n be a cyclic group of order n. A generator of C_n is not uniquely determined, but we know that there $\varphi(n)$ such generators.

Also recall that $|\mathcal{U}(\mathbb{Z}_n)| = \varphi(n)$ and thus if $a \in \mathcal{U}(\mathbb{Z}_n)$ then $a^{\varphi(n)} = 1$.

Let G be a finite group and let $g \in G$ with $o(g) = n$. Let $1 < k < n$ be so that $gcd(k, n) = 1$. Then, k becomes an invertible element in $\mathbb{Z}_n$. Since the latter group has $\varphi(n)$ elements we obtain that $k^{\varphi(n)} \equiv 1 \bmod n$. Write $ni = 1 - k^{\varphi(n)}$. Then put

$$b(g, k) = (1 + g + \cdots + g^{k-1})^{\varphi(n)} + \frac{1 - k^{\varphi(n)}}{n}\hat{g}.$$

Note that

$$b(g, k) = \left(\sum_{j=0}^{k-1} g^j\right)^{\varphi(n)} + i\hat{g} \in \mathbb{Z}G.$$

Such elements are called Bass cyclic units of $\mathbb{Z}G$. The fact that this is indeed a unit can be shown directly by verifying that

$$b(g, k)^{-1} = (1 + g^k + \cdots + g^{k(i-1)})^{\varphi(n)} + \frac{1 - k^{\varphi(n)}}{n}\hat{g}.$$

To avoid these calculations one can use some nice structural techniques. First of all we need to know the description of a rational group algebra $\mathbb{Q}\langle g\rangle$ of the cyclic group $\langle g\rangle$. Second we introduce the notions of a $\mathbb{Z}$-order, a generalization of integral group rings. An thirdly we need to give some elementary properties of the unit group of $\mathbb{Z}$-orders. We will do this in the following section.

7.2 Rational group algebras of finite cyclic groups

Recall that an element $\xi \in \mathbb{C}$ is said to be root of unity if $\xi^n = 1$ for some $n \geq 1$. A root of unity is a primitive m-th root of unity if m is the multiplicative order of ξ. Of course, $\xi_m = e^{2\pi i/m}$ a primitive m-th root of unity, m a nonzero natural number, and

$$\{\xi^j \mid gcd(j, m) = 1, 0 < j < m\}$$

is the set of all primitive m-th roots of unity in $\mathbb{C}$ (these are precisely the generators of the group $\langle \xi_m \rangle$). Thus there are $\varphi(m)$ primitive mth roots of unity.

Recall that the m-th cyclotomic polynomial ($m \geq 1$) over $\mathbb{C}$ is

$$\phi_m(x) = \prod_{0<k<m, gcd(k,m)=1} (x - \xi_m^k).$$

Obviously, it has degree $\varphi(m)$. Important facts proved in an earlier course are

1. $\phi_m(x) \in \mathbb{Z}[x]$,
2. $\phi_m(x)$ is irreducible over $\mathbb{Q}$,
3. $x^n - 1 = \prod_{d|n, 1 \leq d \leq n} \phi_d(x)$,
4. $\sum_{d|n, 1 \leq d \leq n} \varphi(d) = n$,
5. the cyclotomic field $\mathbb{Q}[\xi_n] = \mathbb{Q}(\xi_n)$ is the splitting field of $x^n - 1$ in $\mathbb{C}$.
6. $\dim_{\mathbb{Q}} \mathbb{Q}[\xi_n] = [\mathbb{Q}[\xi_n] : \mathbb{Q}] = \varphi(n)$.

Now we turn the attention to the Wedderburn Decomposition of the rational group algebra of a finite cyclic group C_n of order n.

Lemma 7.2.1. *If $C_n = \langle x \mid x^n = 1 \rangle$. then $\mathbb{Q}C_n \cong \mathbb{Q}[X]/(X^n - 1)$*

Proof. The group algebra $\mathbb{Q}C_n$ has $\mathbb{Q}$-basis $1, x, \ldots, x^{n-1}$. Since the polynomial algebra $\mathbb{Q}[X]$ is free on X there exists a $\mathbb{Q}$-algebra morphism

$$s : \mathbb{Q}[X] \longrightarrow \mathbb{Q}C_n$$

defined by $s(X) = x$.

Let

$$P(X) = \sum_{i=0}^{m} q_i X^i \in \ker s.$$

Write

$$\begin{aligned} P(X) &= q_0 1 + \cdots + q_{n-1}X^{n-1} + q_n X^n + \cdots + q_m X^m \\ &= g_0(X) + \sum_{i\geq 1} g_i(X)X^{in}, \end{aligned}$$

where $g_0(X) = q_0 1 + \cdots + q_{n-1}X^{n-1}$ and $deg(g_i(X)) \leq n-1$. Thus, as $x^n = 1$,

$$\begin{aligned} s(P(X)) &= s\left(\sum_{i\geq 0} g_i(X)X^{in}\right) \\ &= \sum_{i\geq 0} g_i(x) \\ &= 0 \end{aligned}$$

This is the same as $\sum_{i\geq 0} g_i(X) = 0$. Thus

$$\begin{aligned} P(X) &= \sum_{i\geq 0} g_i(X)X^{in} - \sum_{i\geq 0} g_i(X) \\ &= \sum_{i\geq 0} g_i(X)(X^{in} - 1) \\ &= \sum_{i\geq 0} g_i(X)(X^n - 1)Q_i(X), \end{aligned}$$

for some $Q_i(X) \in \mathbb{Q}[X]$. Hence $P(X) \in ((X^n - 1))$.

Conversely, since $x^n = 1$, it is clear that an element of $((X^n - 1))$ is in $\ker s$.

Since s is obviously an epimorphism, the statement is clear. □

Theorem 7.2.2. *The Wedderburn Decomposition of the rational group algebra of a finite cyclic group C_n is given by*

$$\mathbb{Q}C_n \cong \bigoplus_{m|n, 0<m\leq n} \mathbb{Q}(\xi_m),$$

where each ξ_m is a primitive m-th root of unity in $\mathbb{C}$.

Proof. The homomorphism induced by $X \mapsto \xi_m$ is an epimorphism p of $\mathbb{Q}[X]$ to $\mathbb{Q}[\xi_m]$. Let $P(X)$ be a polynomial in $\ker p$, then $p(P(X)) = 0$. Now $p(P(X)) = P(\xi_m)$. Since $\phi_m(X)$ is irreducible over $\mathbb{Q}$ and has ξ_m as a root, we have that $\phi_m(X)$ is a divisor of $P(X)$ and thus $P(X) \in (\phi_m(X))$. So $\ker p \subseteq (\phi_m(X))$. Conversely, if $f(X) \in (\phi_m(X))$ then $P(f(X)) = f(\xi_m) = 0$. Thus $f \in \ker p$. So we have shown that $\ker p = (\phi_m(X))$.

The first isomorphism theorem then yields that

$$\mathbb{Q}(\xi_m) \cong \mathbb{Q}[X]/(\phi_m(X)).$$

Because of the previous Lemma we have

$$\mathbb{Q}C_n \cong \mathbb{Q}[X]/(X^n - 1) \cong \mathbb{Q}[X]/(\prod_{m|n, 0<m\leq n} \phi_m(X)).$$

Note that $\mathbb{Q}[X]$ is a PID. So, applying the Chinese Remainder Theorem to the irreducible polynomials $\phi_m(X)$ we get that

$$\begin{aligned} \mathbb{Q}C_n &\cong \bigoplus_{m|n, 0<m\leq n} \mathbb{Q}[x]/(\phi_m(x)) \\ &\cong \bigoplus_{m|n, 0<m\leq n} \mathbb{Q}(\xi_m). \end{aligned}$$

□

Note that in the proof the explicit isomorphism

$$\mathbb{Q}C_n \longrightarrow \mathbb{Q}[X]/(X^n - 1) \longrightarrow \bigoplus_{m|n} \mathbb{Q}[\xi_m] : x \mapsto (\xi_1, \ldots, \xi_m, \ldots, \xi_n),$$

where x is a generator of C_n.

Corollary 7.2.3. *$\mathbb{Z}C_n$ can be embedded in a direct product of rings over cyclotomic integers (i.e. rings of the form $\mathbb{Z}[\xi_m]$, with ξ_m a primitive m-th root of unity).*

With quite a bit more work one can describe the Wedderburn decomposition of the rational group algebra of a finite abelian group A. This is a result due to Perlis and Walker 1950. For a positive integer a and a field F we denote by aF the direct product of a copies of the field F.

Theorem 7.2.4. *Let A be a finite abelian group of order n. Then*

$$\mathbb{Q}A = \oplus_{d|n} a_d \mathbb{Q}(\xi_d),$$

where ξ_d denotes a primitive root of unity of order d and a_d is the number of cyclic subgroups of A of order d.

Example 7.2.5. *It follows that*

$$\mathbb{Q}C_2 \cong \mathbb{Q} \oplus \mathbb{Q},$$

an isomorphism as $\mathbb{Q}$-algebras. Now $\mathbb{Z}C_2 \subseteq \mathbb{Q}C_2$, but $\mathbb{Z}C_2$ is not ring isomorphic to $\mathbb{Z} \oplus \mathbb{Z}$. This because $\mathbb{Z} \oplus \mathbb{Z}$ contains a non-trivial idempotent (e.g. (0,1)), while $\mathbb{Z}C_2$ does not. Indeed, if $C_2 = \langle x \rangle$ and $a + bx = (a + bx)^2$ with $a, b \in \mathbb{Z}$ then $a^2 + b^2 = a$ and $2ab = b$ and thus $b = 0$ and , $a = 0$ or $a = 1$; thus $a + bx = 0$ or $a + bx = 1$.

Example 7.2.6. $\mathbb{Q}C_3 \cong \mathbb{Q} \oplus \mathbb{Q}(\xi_3)$, *an isomorphism as* $\mathbb{Q}$*-algebras.*

Proof. The divisors of three are one and three itself, so

$$\mathbb{Q}C_3 \cong \mathbb{Q}(\xi_1) \oplus \mathbb{Q}(\xi_3).$$

Now ξ_1 is 1 and thus $\mathbb{Q}(\xi_1) = \mathbb{Q}$. □

Thus $\mathbb{Q}C_3$ contains only two non-trivial primitive idempotents. Write $C_3 = \langle x \mid x^3 = 1 \rangle$. It is easy to see that $e_1 = \frac{1+x+x^2}{3}$ and $e_2 = 1 - e_1$ are non-trivial orthogonal idempotents. Hence these are all the non-trivial idempotents of $\mathbb{Q}C_3$.

It is now worth mentioning that the construction of Bass cyclic unit is an imitation and adaption of a much earlier known construction of units in the ring of cyclotomic integers. To recall this, let n be a positive integer and ξ_n a primitive nth root of unity. If i is a natural number greater than one and relatively prime to n then

$$u_i = \frac{(\xi_n^i - 1)}{(\xi_n - 1)} = 1 + \xi_n + \cdots + \xi_n^{i-1} \in \mathbb{Z}[\xi_n].$$

Moreover u_i is a unit with inverse in $\mathbb{Z}[\xi_n]$, because

$$\frac{(\xi_n - 1)}{(\xi_n^i - 1)} = \frac{(\xi_n^{ik} - 1)}{(\xi_n^i - 1)} = 1 + \xi_n^i + \cdots + \xi_n^{i(k-1)} \in \mathbb{Z}[\xi_n]$$

where k is such that $ik \equiv 1 \bmod n$. These units are called cyclotomic units or Ramachandra units.

7.3 Orders

In this section we give some back ground on ($\mathbb{Z}$-)orders. But before we introduce these rings let us first recall the basic example.

Recall that an algebraic number field k is a finite field extension of $\mathbb{Q}$. It is necessarily of the form $\mathbb{Q}(a)$, for some $a \in \mathbb{C}$. An algebraic integer in k is an element that is a root of a monic polynomial with integral coefficients. The algebraic integers in an algebraic number field k form a subring which is denoted by $\mathcal{O}_k$, It is the best-known example of an order.

Note that if ξ_m is an m-th root of unity in $\mathbb{C}$, then $\mathbb{Z}[\xi_m]$ is contained in the ring of integers in $\mathbb{Q}(\xi_m)$. Note that $\mathbb{Z}[\xi_m]$ is a finitely generated $\mathbb{Z}$-modules (i.e. a finitely generated abelian group) and $\mathbb{Q}\,\mathbb{Z}[\xi_m] = \mathbb{Q}(\xi_m)$.

The unit group of such a ring has been characterized.

Theorem 7.3.1 (Dirichlet Unit Theorem)**.**

$$\mathcal{U}(\mathcal{O}_k) \cong F \times C,$$

where F is a torsion-free abelian group of rank $r_1 + r_2 - 1$, with $[k : \mathbb{Q}] = r_1 + 2r_2$ and k has r_1 real and $2r_2$ complex embeddings, and C is a finite group of roots of unity in k.

The generators of F are called fundamental units. In general, one does not know generic constructions for these units.

Definition 7.3.2. *Let A be a $\mathbb{Q}$- algebra with unity. A subring R with unity is called a $\mathbb{Z}$-order (or, simply, an order) if R is a finitely generated $\mathbb{Z}$-submodule that contains a $\mathbb{Q}$-basis of A, or equivalently $\mathbb{Q}R = A$.*

We give some examples.

1. The ring $\mathcal{O}_k$ of algebraic integers of an algebraic number field k is an order in k and $M_n(\mathcal{O}_k)$ is an order in $M_n(k)$.

2. If a is an algebraic integer, then the subring $\mathbb{Z}[a]$ of $\mathbb{Q}(a)$ generated by a is an order in $\mathbb{Q}(a)$.

3. The integral group ring $\mathbb{Z}G$ of a finite group G is an order in the rational group algebra $\mathbb{Q}G$. More generally, $\mathcal{O}_kG$ is an order in kG.

Lemma 7.3.3. *Let R_1 and R_2 be orders in a $\mathbb{Q}$-algebra A. Then the following statements hold.*

1. *$R_1 \cap R_2$ is an order in A.*

2. *If $R_2 \subseteq R_1$, then the index $[\mathcal{U}(R_1) : \mathcal{U}(R_2)]$ is finite.*

3. *Suppose R_3 is a subring of A (with unity) which is finitely generated as a $\mathbb{Z}$-module. If $R_1 \subseteq R_3$, then R_3 is an order in A.*

4. *If $R_2 \subseteq R_1$ then*
$$\mathcal{U}(R_2) = R_2 \cap \mathcal{U}(R_1).$$
Thus, if $R_2 \subseteq R_1$ and $u \in R_2$ is invertible in R_1, then $u^{-1} \in R_2$, that is, u is invertible in R_2.

Proof.

1. First note that $R_1 \cap R_2$ is a submodule of the finitely generated $\mathbb{Z}$-module R_1 and hence it is finitely generated. Since $\mathbb{Q} \cdot R_1 = A$, for every element $a \in A$ there exists $0 \neq z_1 \in \mathbb{Z}$ so that $az_1 \in R_1$. Similarly there exists $0 \neq z_2 \in \mathbb{Z}$ so that $az_2 \in R_2$. Then $az_1z_2 \in R_1 \cap R_2$. It follows that $\mathbb{Q} \cdot (R_1 \cap R_2) = A$.

2. Since R_1 is a finitely generated $\mathbb{Z}$-submodule of A and because $\mathbb{Q}\cdot R_2 = A$, there exists a positive integer l such that $lR_1 \subseteq R_2$. Furthermore, considering R_1 and lR_1 as additive groups, the additive index $[R_1 : lR_1]$ is finite. We now show that the (multiplicative) index $[\mathcal{U}(R_1) : \mathcal{U}(R_2)]$ is bounded by the additive index $[R_1 : lR_1]$. Suppose that $x, y \in \mathcal{U}(R_1)$ are such that $x+lR_1 = y+lR_1$. Let 1 denote the common unity of A and R_2. Then $x^{-1}y \in 1 + lR_1 \subseteq R_2$. Thus $x^{-1}y \in R_2$. Similarly, $y^{-1}x \in R_2$ and therefore $x^{-1}y \in \mathcal{U}(R_2)$. Thus $y \in x\mathcal{U}(R_2)$ and therefore $x\mathcal{U}(R_2) = y\mathcal{U}(R_2)$.

3. Since $R_1 \subseteq R_3$, for every element $a \in A$ there exists $0 \neq z \in \mathbb{Z}$ so that $az \in R_1$. Hence $az \in R_3$. So $\mathbb{Q} \cdot R_3 = A$.

4. Clearly $\mathcal{U}(R_2) \subseteq R_2$ and $\mathcal{U}(R_2) \subseteq \mathcal{U}(R_1)$, because $R_2 \subseteq R_1$. So $\mathcal{U}(R_2) \subseteq R_2 \cap \mathcal{U}(R_1)$. On the other hand, if $u \in R_2 \cap \mathcal{U}(R_1)$ then $R_1u = R_1$. Hence, considering all algebras as additive groups, we see that,
$$[R_1 : uR_2] = [uR_1 : uR_2].$$
Since u is invertible in R_1, it follows that
$$[R_1 : uR_2] \leq [R_1 : R_2].$$
Since $uR_2 \subseteq R_2$, the opposite inequality obviously holds. Hence $[R_1 : uR_2] = [R_1 : R_2]$. Thus $uR_2 = R_2$ and therefore $u^{-1} \in R_2$. So $R_2 \cap \mathcal{U}(R_1) \subseteq \mathcal{U}(R_2)$ and this establishes $\mathcal{U}(R_2) = R_2 \cap \mathcal{U}(R_1)$ as required.

□

Corollary 7.3.4. *Let R be a subring of $\mathbb{Q}G$ and suppose R is a finitely generated $\mathbb{Z}$-module. If $\mathbb{Z}G \subseteq R$ then $[\mathcal{U}(R) : \mathcal{U}(\mathbb{Z}G)] < \infty$.*

Proof. As $\mathbb{Z}G$ is an order in $\mathbb{Q}G$ and $\mathbb{Z}G \subseteq R \subseteq \mathbb{Q}G$ we get from Lemma 7.3.3 that R is also an order in $\mathbb{Q}G$. Furthermore, $[\mathcal{U}(R) : \mathcal{U}(\mathbb{Z}G)] < \infty$. □

We know that the rational group algebra $\mathbb{Q}C_n$ is a direct sum of cyclotomic fields, namely
$$\mathbb{Q}C_n \cong \bigoplus_{d|n} \mathbb{Q}(\xi_d),$$
where ξ_d is a primitive dth root of unity. We also saw in Corollary 7.2.3 that
$$\mathbb{Z}C_n \subseteq \bigoplus_{d|n} \mathbb{Z}[\xi_d] = \mathbb{M},$$
an order of $\mathbb{Q}C_n$. Hence the unit group of $\mathbb{Z}C_n$ and $\mathbb{M}$ differ by a subgroup of finite index. Since $\mathcal{M} = \prod_{d|n} \mathcal{U}(\mathbb{Z}[\xi_d])$ the Dirichlet unit theorem gives

us, up to finite index, the description of the unit group of $\mathbb{Z}C_n$. In particular it follows that the unit group of $\mathbb{Z}C_n$ is finitely generated.

In case G is a non-commutative finite group then it is much harder to deal with its unit group. Recall that from the Wedderburn-Artin theorem we know that $\mathbb{Q}G = \oplus_i M_{n_i}(D_i)$, a direct sum of matrices over division rings D_i. Hence it is plausible that also $\oplus_i M_{n_i}(O_i)$ is an order in $\mathbb{Q}G$, where each O_i is an order in D_i. For example,

$$\mathbb{Z}S_3 \subseteq \mathbb{Z} \oplus \mathbb{Z} \oplus M_2(\mathbb{Z}) = \mathbb{M},$$

and

$$\mathbb{Z}D_8 \subseteq \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus M_2(\mathbb{Z}) = \mathbb{M}.$$

Hence by Lemma 7.3.3, the unit group is up to finite index the same as that of $\prod_i \mathrm{GL}_{n_i}(O_i)$, where we denote by $\mathrm{GL}_{n_i}(O_i)$ the invertible $n_i \times n_i$-matrices over O_i. Now the latter groups are called linear groups over the orders O_i and their structure is much more complicated. For example these groups are rather "large" as they contain non-commutative free groups. Indeed recall that in an earlier course we have proved that the group

$$\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \rangle$$

is a free group.

However, a famous theorem says that the unit group $\mathcal{U}(\mathbb{Z}G)$, for any finite group G, is finitely generated, even finitely presented. To compute specific generators, even for concrete examples, is a very hard problem. Only quite recently does one know for many finite groups G such a set of generators. These are often the bicylic units together with the Bass cyclic units.

As a general but very difficult problem one can now state:

Problem 7: Describe the structure of the unit group $\mathcal{U}(\mathbb{Z}G)$ of the integral group ring $\mathbb{Z}G$ of a finite group G.

Or even more general

Problem 8: Describe the structure of the unit group $\mathcal{U}(R)$ of a $\mathbb{Z}$-order R.

We now prove again that Bass cyclic units are indeed units. For this let $C_n = \langle g \rangle$. We have established in Corollary 7.2.3 that $\phi : \mathbb{Z}C_n \longrightarrow \bigoplus_{d|n} \mathbb{Z}[\xi_d]$ is a monomorphism. Recall that

$$g \mapsto (\xi_1, \ldots, \xi_d, \ldots, \xi_n).$$

Thus $\phi(\mathbb{Z}C_n)$ is an order in $\bigoplus_{d|n} \mathbb{Z}[\xi_d] = \mathbb{M}$. Thus by Lemma 7.3.3 (note that $\phi(\mathbb{Z}C_n)$ and $\mathbb{M}$ are $\mathbb{Z}$-orders in $\bigoplus_{d|n} \mathbb{Q}(\xi_d)$) we have that a Bass cyclic unit is invertible in $\mathbb{Z}C_n$ if its image under ϕ is invertible in $\bigoplus_{d|n} \mathbb{Z}[\xi_d]$. For

each $d \mid n$ let u_d be the image of $b(g,k)$ under the projection of $\phi(b(g,k))$ onto $\mathbb{Z}[\xi_d]$. Hence note that

$$u_d = \left(\sum_{j=0}^{k-1} \xi_d^j\right)^{\varphi(n)} + \frac{1-k^{\varphi(n)}}{n} \sum_{j=0}^{n-1} \xi_d^j.$$

If $d = 1$ and thus $\xi_d = 1$, then

$$\begin{aligned} u_d &= (\textstyle\sum_{j=0}^{k-1} 1^j)^{\varphi(n)} + \frac{1-k^{\varphi(n)}}{n} \sum_{j=0}^{n-1} 1^j \\ &= k^{\varphi(n)} + \frac{1-k^{\varphi(n)}}{n} n \\ &= 1. \end{aligned}$$

If $d \neq 1$ and thus $\xi_d \neq 1$, then $\sum_{j=0}^{d-1} \xi_d^j = \frac{1-\xi_d^d}{1-\xi_d} = \frac{1-1}{1-\xi_d} = 0$. Hence

$$\begin{aligned} u_d &= (\textstyle\sum_{j=0}^{k-1} \xi_d^j)^{\varphi(n)} + \frac{1-k^{\varphi(n)}}{n} (\frac{n}{d} \sum_{j=0}^{d-1} \xi_d^j) \\ &= (\textstyle\sum_{j=0}^{k-1} \xi_d^j)^{\varphi(n)} + \frac{1-k^{\varphi(n)}}{n} \cdot 0 \\ &= (\frac{1-\xi_d^k}{1-\xi_d})^{\varphi(n)} \end{aligned}$$

Hence $\phi(b(g,k))$ is a unit in $\mathbb{M}$ (a tupple is a unit if all its components are units) and thus $b(g,k)$ is a unit in $\mathbb{Z}C_n$.

7.4 Free subgroups in $\mathcal{U}(\mathbb{Z}G)$

It has been known for many years that the unit group $\mathcal{U}(\mathbb{Z}G)$ seldom belongs to a well-established class of groups, such as for example solvable or nilpotent groups. This is caused by the existence of non-abelian free subgroups in $\mathcal{U}(\mathbb{Z}G)$, for most finite groups G. The aim of this Section is to give a proof of this result.

Definition 7.4.1. *An involution of an algebra A is a linear map*

$$a \mapsto \overline{a}$$

of A which satisfies

$$\begin{aligned} \overline{ab} &= \overline{b}\,\overline{a} \\ \overline{\overline{a}} &= a. \end{aligned}$$

The complex group algebra $\mathbb{C}G$ has an involution. For $\gamma = \sum \gamma_g g \in \mathbb{C}G$, set $\gamma^* = \sum \overline{\gamma_g} g^{-1}$, where $\overline{\ }$ denotes the complex conjugation. Then,

- $(\gamma + \mu)^* = \gamma^* + \mu^*$
- $(\gamma\mu)^* = \mu^*\gamma^*$
- $(\gamma^*)^* = \gamma$.

Thus $*$ is an involution. When $\gamma \in \mathbb{Z}G$, clearly $\gamma^* = \sum \gamma_g g^{-1}$.

Theorem 7.4.2. *For $\gamma \in \mathbb{Z}G, \gamma\gamma^* = 1$ if and only if $\gamma = \pm g, g \in G$.*

Proof. Clearly, if $\gamma = \pm g$, then $\gamma^* = \pm g^{-1}$ and $\gamma\gamma^* = 1$.

Conversely, suppose $\gamma = \sum \gamma_g g, \gamma^* = \sum \overline{\gamma_g} g^{-1}$, with $\gamma\gamma^* = 1$. Then

$$1 = \gamma\gamma^* = \sum_{g \in G} \gamma_g^2 1 + \cdots .$$

It follows that $\sum \gamma_g^2 = 1$ and thus $\gamma_{g_0} = \pm 1$ for a unique g_0 and $\gamma_g = 0$ for all $g \neq g_0$. Hence $\gamma = \pm g_0$, as claimed. □

The following important Theorem will be proved later on.

Theorem 7.4.3. *(Marciniak and Sehgal) Let G be any group. If $u_{g,h}$ is a non-trivial bicyclic unit of $\mathbb{Z}G$, then the pair $\{u_{g,h}, u_{g,h}^*\}$ generates a non-abelian free subgroup of $\mathcal{U}(\mathbb{Z}G)$.*

Corollary 7.4.4. *(Hartley and Pickel) Let G be a non-abelian finite group. Then $\mathcal{U}(\mathbb{Z}G)$ contains a non-abelian free group if and only if G is not an Hamiltonian 2-group.*

We will now prove a more general version of Theorem 7.4.3. The proof is due to Salwa and is based on ideas of Marciniak and Sehgal.

By $|a|$ we mean the absolute value of $a \in \mathbb{C}$. $\mathcal{J}(R)$ denotes the Jacobson radical of a ring R.

Definition 7.4.5. *We say that an algebra A over $\mathbb{C}$ admits a trace function if there exists a $\mathbb{C}$-linear map $Tr : A \longrightarrow \mathbb{C}$ such that, $Tr(ab) = Tr(ba)$ for all $a, b \in A$, $Tr(e) \in \mathbb{R}^+$ for all idempotents $e \in A \setminus \{0\}$ and $Tr(n) = 0$ for every nilpotent element $n \in A$.*

Consider a ring R with unity. Let $\langle x, y \rangle$ denote the subgroup of the ring R generated by two units $x, y \in R$. From now on F_2 stands for the free (non-abelian) group on two generators.

Theorem 7.4.6. *Let R be a torsion-free ring with unity (i.e. R is torsion-free as an additive group). Assume that $a, b \in R$ with $a^2 = b^2 = 0$ and ab is not nilpotent. Then there exists $m \in \mathbb{N}$ such that*

$$\langle 1 + ma, 1 + mb \rangle \cong F_2.$$

If moreover $\mathbb{C} \otimes_{\mathbb{Z}} R$ admits a trace function Tr, then

$$\langle 1 + a, 1 + b \rangle \cong F_2$$

provided that $|Tr(ab)| \geq 2Tr(1)$.

Proof. Let $\mathbb{Z}\langle a, b\rangle$ be the subring of R generated by a and b. Put $A = \mathbb{C} \otimes_{\mathbb{Z}} \mathbb{Z}\langle a, b\rangle$.

If there are no relations in A other than those coming from $a^2 = b^2 = 0$, then we can define a homomorphism $\phi : A \longrightarrow M_2(\mathbb{C})$ by the rule $\phi(a) = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}, \phi(b) = \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix}$. Because $\langle 1+\phi(a), 1+\phi(b)\rangle \cong F_2$ by a Theorem of Sanow, we have also $\langle 1 + a, 1 + b\rangle \cong F_2$.

So assume that there exists a non-trivial relation between elements of the set S of non-zero words in a, b. Elements of S are of the form $x(ab)^n y$ where $n \geq 0, x \in \{1, b\}$ and $y \in \{1, a\}$. S can be ordered by lexicographic order assuming that $a > b$. So there is a relation of the form $w = \sum_i a_i w_i$ where $a_i \in \mathbb{C}, w, w_i \in S$ and $w > w_i$ for all i. Note that any word $z \in S$ of length greater than the length of w has to contain w as a subword. Hence substituting $\sum_i a_i w_i$ in place of w we can express z as a linear combination of words which are smaller than w. Repeating this argument we obtain that $A = Vect_{\mathbb{C}}\{z \in S : \text{length of } z < \text{length of } w\}$. In particular $\dim_{\mathbb{C}} A < \infty$. Let

$$A/\mathcal{J}(A) \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_k}(\mathbb{C}).$$

First we will prove that $n_i \leq 2$ for each i. Clearly there exists an homomorphism $\phi_i : A \longrightarrow M_{n_i}(\mathbb{C})$ which is onto. We will often consider the elements $\phi_i(a)$ of $M_{n_i}(\mathbb{C})$ as linear transformations. Hence we can speak of their respective kernel and image.

Since $\phi_i(a)^2 = 0$, we obtain $\ker \phi_i(a) \supseteq \mathrm{Im}\phi_i(a)$. It follows by the Dimension Theorem of Linear Transformations that $n_i \geq 2 \cdot \dim \mathrm{Im}\phi_i(a)$ and therefore $rank(\phi_i(a)) \leq [n_i/2]$.

Define $X = Vect\{(\phi_i(a)\phi_i(b))^t : t = 0, 1, \dots\}$. Since $rank(\phi_i(a) \circ \phi_i(b)) \leq [n_i/2]$, we get $\dim X \leq [n_i/2] + 1$ by the Cayley-Hamilton theorem. It is easy to see that $M_{n_i}(\mathbb{C}) = X + \phi_i(b)X + X\phi_i(a) + \phi_i(b)X\phi_i(a)$. This implies $n_i^2 \leq 4([n_i/2] + 1)$. Hence $n_i \leq 2$, as desired.

Suppose that $n_i = 1$ for all i. This means that $A/\mathcal{J}(A)$ is commutative. Hence $ab - ba \in \mathcal{J}(A)$. Since $\mathcal{J}(A)$ is nilpotent, say of index m, this implies $[(ab - ba)a(ab - ba)b]^m = 0$. Hence $(-ababab)^m = 0$, a contradiction, as ab is assumed not to be nilpotent. Hence there exists i such that $n_i = 2$ and an onto homomorphism $\phi : A \longrightarrow M_2(\mathbb{C})$. Clearly $M_2(\mathbb{C}) = \mathbb{C}\langle\phi(a), \phi(b)\rangle$. Now $\phi(a)^2 = 0$ and $\phi(a) \neq 0$. So $rank(\phi(a)) = 1$. Similarly $rank(\phi(b)) = 1$.

If $\phi(a)\phi(b) = 0$ then $\mathrm{Im}\phi(b)$ is $\phi(a)$- and $\phi(b)$-invariant. Thus $\mathrm{Im}\phi(b)$ is invariant under $M_2(\mathbb{C})$, a contradiction. Hence $\phi(a)\phi(b) \neq 0$ and similarly $\phi(b)\phi(a) \neq 0$. Since $rank(\phi(a)\phi(b)) \leq rank(\phi(a)) = 1$ and $\phi(a)\phi(b) \neq 0$, we get $rank(\phi(a)\phi(b)) = 1$. This implies

$$\mathrm{Im}(\phi(a)\phi(b)) = \mathrm{Im}\phi(a), \tag{7.1}$$

$$\ker(\phi(a)\phi(b)) = \ker\phi(b).$$

Assume that $\phi(a)\phi(b)$ is nilpotent. Then $\mathrm{Im}(\phi(a)\phi(b)) = \ker(\phi(a)\phi(b))$ and thus implies $\mathrm{Im}\phi(a) = \ker\phi(b)$ and we get $\phi(b)\phi(a) = 0$, a contradiction.

Hence $\phi(a)\phi(b)$ is not nilpotent and we can find a basis $\{v_1, v_2\}$ of $\mathbb{C}^2$ such that $\phi(a)\phi(b) = \begin{pmatrix} \lambda & 0 \\ 0 & 0 \end{pmatrix}$, $\lambda \in \mathbb{C} \setminus \{0\}$. From (7.1) it follows that $\phi(a) = \begin{pmatrix} p & q \\ 0 & 0 \end{pmatrix}$ and $\phi(b) = \begin{pmatrix} r & 0 \\ s & 0 \end{pmatrix}$ for some $p, q, r, s \in \mathbb{C}$. Because $\phi(a)$ and $\phi(b)$ are nilpotent we have $p = r = 0$. Now we can find $m \in \mathbb{N}$ such that $|mq|, |ms| \geq 2$. In this case $\langle 1 + m\phi(a), 1 + m\phi(b)\rangle \cong F_2$, (Theorem of Sanow), whence $\langle 1 + ma, 1 + mb\rangle \cong F_2$. This completes the proof of the first assertion of the theorem.

Now assume that A admits a trace function Tr and $|Tr(ab)| > 2Tr(1)$. By the first part of the proof we can assume that $\dim_{\mathbb{C}} A < \infty$. Hence $\mathcal{J}(A)$ is nilpotent. Define $tr : A/\mathcal{J}(A) \longrightarrow \mathbb{C}$ by the rule

$$tr(a + \mathcal{J}(A)) = Tr(a)$$

for $a \in A$. Then tr is well-defined, because if $a \in A$ is nilpotent, then $Tr(a) = 0$. It follows also that $tr(c) = 0$ for all nilpotent elements $c \in A/\mathcal{J}(A)$. Of course tr is $\mathbb{C}$-linear and

$$tr(\overline{a}\overline{b}) = tr(\overline{b}\overline{a})$$

for $\overline{a}, \overline{b} \in A/\mathcal{J}(A)$. Moreover if $A/\mathcal{J}(A)$ has a non-zero idempotent $\overline{e}$ then by a Theorem of ring theory there exists a non-zero idempotent $e \in A$ such that $\overline{e} = e + \mathcal{J}(A)$. This implies $tr(\overline{e}) = Tr(e) \in \mathbb{R}^+$. It follows that tr is a trace function. By the proof of the first part of the theorem we know that

$$A/\mathcal{J}(A) \cong \underbrace{\mathbb{C} \times \cdots \times \mathbb{C}}_{k} \times \underbrace{M_2(\mathbb{C}) \times \cdots \times M_2(\mathbb{C})}_{l}.$$

Let ϕ_i denote the composition of the quotient map $A \longrightarrow A/\mathcal{J}(A)$ with the projection on the i-th factor of $A/\mathcal{J}(A)$. Then $\phi_i(a) = 0$ for $i \leq k$ because $a^2 = 0$, and $\phi_i(a) = \begin{pmatrix} 0 & q_i \\ 0 & 0 \end{pmatrix}$ for $i > k$. Similarly $\phi_i(b) = 0$ for $i \leq k$ and $\phi_i(b) = \begin{pmatrix} 0 & 0 \\ s_i & 0 \end{pmatrix}$ for $i > k$. The trace function tr has the form $tr = \sum_i \lambda_i tr_i, \lambda_i \in \mathbb{R}^+$, where tr_i denotes the usual trace function. In fact, it is easy to verify that a trace function on matrices has to be a scalar multiple of the usual trace function. The condition $|Tr(ab)| \geq 2Tr(1)$ implies $|\sum_{i>k} \lambda_i q_i s_i| \geq 2(\sum_{i\leq k} \lambda_i + \sum_{i>k} 2\lambda_i)$.

If $|q_i s_i| < 4$ for all $i > k$, then

$$4\sum_{i>k} \lambda_i \leq 2\sum_{i\leq k} \lambda_i + 4\sum_{i>k} \lambda_i < |\sum_{i>k} \lambda_i q_i s_i| \leq \sum_{i>k} \lambda_i |q_i s_i| < 4\sum_{i>k} \lambda_i,$$

a contradiction.

Hence there exists an $i_0 > k$ such that $|q_{i_0}s_{i_0}| \geq 4$. Clearly $\phi_{i_0}(1+a) = \begin{pmatrix} 1 & q_i \\ 0 & 1 \end{pmatrix}$, $\phi_{i_0}(1+b) = \begin{pmatrix} 1 & 0 \\ s_{i_0} & 1 \end{pmatrix}$, or changing the basis $\phi_{i_0}(1+a) = \begin{pmatrix} 1 & q_{i_0}s_{i_0} \\ 0 & 1 \end{pmatrix}, \phi_{i_0}(1+b) = \begin{pmatrix} 1 & 0 \\ \sqrt{q_{i_0}s_{i_0}} & 1 \end{pmatrix}$ where $|\sqrt{q_{i_0}s_{i_0}}| \geq 2$. Therefore (Theorem of Sanow) $\langle 1+a, 1+b\rangle \cong F_2$. □

We will prove Theorem 7.4.3.

Proof. A non-trivial bicyclic unit $u_{g,h} = 1 + (1-g)h\hat{g}$ is of the form $1+a$, where $a^2 = 0$ and $a \neq 0$. Also $u_{g,h}^* = 1 + b$ with $b^2 = 0$ and $b = \hat{g}h^{-1}(1 - g^{-1}) = a^*$. We will again use geometry to investigate the statement. The group ring $\mathbb{Z}G$ itself carries a natural geometric structure. To see this let us embed $\mathbb{Z}G$ into the complex vector space $\mathbb{C}G$ for which G serves as a basis. We induce geometry on this space by demanding that this basis is unitary. This goal can be achieved by introducing in $\mathbb{C}G$ a Hermitian inner product by the formula

$$\Big(\sum a_g g, \sum b_g g\Big) := \sum \overline{a_g} b_g.$$

It leads to a norm $\|a\| = \sqrt{(a,a)}$ on $\mathbb{C}G$ which can be used to measure the sizes of group ring elements.

In some instances the size of an element $a \in \mathbb{Z}G$ inter plays nicely with its algebraic properties. Indeed, we have that if $a \in \mathbb{Z}G, a \neq 0$ and $a^2 = 0$, then $\|a\| \geq 2$. To show this let $a = \sum a_g g$ with $a_g \in \mathbb{Z}$. Suppose that $4 > \|a\|^2 = \sum a_g^2$. Thus at most three integers a_g are different from zero and those satisfy $a_g = \pm 1$. As the augmentation of any nilpotent element is zero, we have an additional equation $\sum a_g = 0$. It follows that $a = g - h$ for some $g, h \in G$. But then $0 = g^2 - gh - hg + h^2$, which implies that $g = h$ and hence $a = 0$, a contradiction. In other words, nilpotent elements in $\mathbb{Z}G$ cannot be "too short".

Now the star operator is strongly related to our inner product. Indeed,

$$(a,b) = \sum \overline{a_g} b_g = tr(a^* b),$$

where tr denotes the coefficient at 1. Now put $c = a^* a$. Then

$$\|c\| \geq |c_1| = tr(a^* a) = \|a\|^2 \geq 4.$$

Hence $tr(a^*a) \neq 0$ and thus we can deduce from the properties of the trace function tr that a^*a is not nilpotent. Since $\mathbb{C} \otimes_{\mathbb{Z}} \mathbb{Z}G \cong \mathbb{C}G$ admits the trace function tr the previous theorem implies that $\langle 1 + (1-g)h\hat{g}, 1 + \hat{g}h^{-1}(1 - g^{-1})\rangle \cong F_2$. This implies $F_2 \subseteq \mathcal{U}(\mathbb{Z}G)$. □

It happens very seldom that the unit group $\mathcal{U}(\mathbb{Z}G)$ has a free subgroup of finite index.

Theorem 7.4.7. *(Jespers) The only finite non-abelian groups G such that $\mathcal{U}(\mathbb{Z}G)$ has a free subgroup of finite index are S_3, D_8,*

$$\mathcal{T} = \langle a, b \mid a^6 = 1, b^2 = a^3, ba = a^2 b \rangle, \text{ the dicyclic group of order 12,}$$

and

$$\mathcal{P} = \langle a, b \mid a^4 = 1 = b^4, ba = a^{-1} b \rangle, \text{ a group of order 16.}$$

In fact, these free subgroups of finite index will be (free) normal complements of the groups G in $\mathcal{U}(\mathbb{Z}G)$.

Bibliography

[1] L. Rowen, Ring Theory, Vol I and II, Academic Press, New York, 1988.
ISBN: 0-12-599841-4(vol.1), 0-12-599842-2(vol.2).

[2] N. Jacobson, Basic Algebra I and II, W.H. Freeman and Company, San Francisco, 1980.
ISBN: 0-7167-1480-9(vol.1), 0-7167-1079-X(vol.2).

[3] J.C. McConnell, J.C. Robson, Noncommutative Noetherian Rings, John Wiley and Sons, New York, 1987.
ISBN: 0-471-91550-5.

[4] Jan Okniński, Semigroup algebras, Marcel Dekker.

[5] D.S. Passman, The algebraic structure of group rings, Wiley-Interscience, New York, 1977.

[6] A. H. Clifford and G.B. Preston, The algebraic structure of semigroups, Vol.I, American Math. Soc., 1961.

[7] S.K. Sehgal, Topics in Group Rings, Marcel Dekker, 1978.

[8] S.K. Sehgal, Units in integral group rings, Longman, 1993.

Index