Chapter 6
Miscellanea

In this Chapter we present assorted examples involving the group ring construction.

6.1 Power-closed Groups

Modular dimension subgroup play a fundamental role in understanding the power structure of p-groups (see e.g., [Sco91], [Wil03]).

Let G be a p-group. Then G is said to be *k-power closed*, $k \geq 1$, if every product $x_1^{p^k} \ldots x_n^{p^k}$ $x_i \in G$, $n \geq 1$, can be written as y^p for some $y \in G$.

Theorem 6.1 (Wilson [Wil03]). *If G is a p-group of nilpotency class less than p^k, then G is k-power closed.*

This result is proved by carrying out an extensive study of the modular dimension subgroups $D_{n,\mathbb{F}_p}(G)$. Note that, for every $x \in G$ and $k \geq 1$, $x^{p^k} \in D_{p^k,\mathbb{F}_p}(G)$; therefore, Theorem 6.1 follows from the following:

Theorem 6.2 (Wilson [Wil03]). *Let G be a finite p-group such that $\gamma_{p^k}(G) \subseteq D_{p^{k+1},\mathbb{F}_p}(G)$ for some k. Then $D_{p^{k+\ell-1},\mathbb{F}_p}(G) \subseteq \{x^{p^\ell} \mid x \in G\}$ for positive integers ℓ.*

An immediate consequence of Theorem 6.2 is the following:

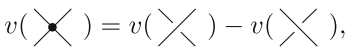
Corollary 6.3 (Wilson [Wil03]). *Let G be a finite p-group of nilpotency class c. Let k be the minimal integer such that $c < p^{k+1}$. Then $D_{p^{k+\ell},\mathbb{F}_p}(G) \subseteq \{x^{p^\ell} \mid x \in G\}$ for positive integers l.*

6.2 Braid Groups

The lower central series of pure braid groups (see §1.2, p. 15) plays an important role in the theory of braid invariants. A *singular pure braid* is a

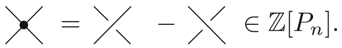
R. Mikhailov, I.B.S. Passi, *Lower Central and Dimension Series of Groups*,
Lecture Notes in Mathematics 1952,

pure braid with a finite number of transversal intersections. Any invariant of braids which takes values in some ring R can be viewed as a collection of maps $P_n \to R$, $n \geq 2$. Let $v : P_n \to R$ be an invariant of pure braids. Then we can extend v to be defined on singular braids, by the following rule (so-called *Vassiliev skein relation*):



where the above diagrams represent braids which differ by one intersection inside a ball and completely identical outside the ball. Clearly, this rule makes it possible to extend the invariant v to be defined on singular pure braids. An invariant v of pure braids is said to be an *invariant of type* k if its extension vanishes on all singular braids with more than k double points. We say that two braids B_1 and B_2 are *k-equivalent* if $v(B_1) = v(B_2)$ for any invariant v of type less than k.

One can formally view a singular pure braid with n strands as an element of the integral group ring $\mathbb{Z}[P_n]$ by setting



(6.1)

Then the extension of the invariant v defines a $\mathbb{Z}$-linear map

$$\bar{v} : \mathbb{Z}[P_n] \to R.$$

Clearly, any singular braid with exactly one double point defines an element of the augmentation ideal $\Delta(P_n)$ of $\mathbb{Z}[P_n]$, since it is a "difference" of two pure braids. It is easy to see that any singular braid with exactly two double points can be drawn as a composition of two singular braids with exactly one double point each. In general, any singular braid with k double points can be written as a composition of k singular braids with one double point each. With composition of braids corresponding to the multiplication in the group ring $\mathbb{Z}[P_n]$, any singular braid with n strands and more than k double points represents an element from the kth power of the augmentation ideal of $\mathbb{Z}[P_n]$. On the other hand, any pure braid can be deformed to the trivial one by the sequence of crossed moves:

This implies that the augmentation ideal of $\mathbb{Z}[P_n]$ is the $\mathbb{Z}$-linear closure of elements of the form (6.1), i.e., of singular braids with n strands. Similarly, we conclude that the kth power of the augmentation ideal of $\mathbb{Z}[P_n]$ is the $\mathbb{Z}$-linear closure of singular braids with n strands and not less than k double points.

Let p_1 and p_2 be pure braids with n strands. For $k \geq 1$, the above argument shows that there is an invariant v of type k which differs on p_1 and p_2 if and only if $p_1 - p_2$ determines a nontrivial element in the quotient $\mathbb{Z}[P_n]/\Delta^k(P_n)$;

this is equivalent to saying that $1 - p_1p_2^{-1} \notin \Delta^k(P_n)$, i.e., $p_1p_2^{-1} \notin D_k(P_n)$, the kth dimension subgroup of P_n. It is easy to see, in view of (Chapter 1, 1.6), that the lower central series and the dimension series are identical for the pure braid groups. Hence, we have the following

Proposition 6.4 *Two pure braids p_1, p_2 with n strands are k-equivalent if and only if $p_1p_2^{-1} \in \gamma_k(P_n)$.*

A similar equivalence occurs in the case of classical knots. Every knot is the closure of some braid. However, different braids can determine isotopical knots. In analogy with singular braids, one can define the singular knots and type k invariants as knot isotopy invariants which vanish for singular knots with more than k double points. As for braids, we say that two knots K_1 and K_2 are *k-equivalent* if $v(K_1) = v(K_2)$ for any invariant v of type less than k.

Theorem 6.5 (Stanford [Sta98]). *Let K_1 and K_2 be knots. Then K_1 and K_2 are k-equivalent if and only if there exists a braid $b \in B_n$ and a pure braid $p \in P_n$ for some n, such that K_1 is the closure of b, but K_2 is the closure of bp.*

Remark. It may be noted that the residual nilpotence of the pure braid groups implies that non-equal (non-isotopical) braids always differ by some invariant of finite type. However, the same result for knots does not follow immediately and the conjecture about completeness of invariants of finite type for knots is still open.

6.3 3-dimensional Surgery

The applications of the dimension subgroup theory to the 3-dimensional surgery was discovered by G. Massuyeau [Mas07]. Here we recall the construction from [Mas07].

Let S be a surface. The mapping class group $\mathcal{M}(S)$ of S is the group of all isotopy classes of orientation-preserving homeomorphisms of S to itself. There is a natural action of $\mathcal{M}(S)$ on the first homology group of S, hence there is a natural homomorphism

$$\Psi : \mathcal{M}(S) \to \mathrm{Aut}(H_1(S)).$$

The kernel of Ψ is called *Torelli group* of S and denoted by $\mathcal{I}(S)$. The homeomorphisms of S to itself acting trivially on homology are called *Torelli automorphisms.*

Let M be a compact oriented 3-dimensional manifold and $H \subset M$ a handlebody. Consider a Torelli automorphism $h : \partial(M) \to \partial(M)$. Then one can construct a new 3-dimensional manifold M_h in the following way:

$$M_h = (M \setminus \mathrm{int}(H)) \cup_h H.$$

The transformation

$$M \rightsquigarrow M_h$$

is called a *Torelli surgery.* One can naturally generalize this definition for the case

$$M \rightsquigarrow M_I$$

where I is a set of pairwise disjoint handlebodies in M with selected Torelli automorphisms.

Following M. Goussarov and K. Habiro, given $k \geq 1$, call two compact oriented 3-manifolds M and N, Y_k*-equivalent* if there exists a Torelli automorphism h, which belongs to the k-th term of lower central series of the Torelli group $\partial(H)$, such that

$$M \rightsquigarrow M_h = N.$$

Let A be an abelian group and f a topological invariant of compact oriented 3-manifolds with values in A. We call f an invariant of degree at most d if, for any manifold M and every set Γ of pairwise disjoint handlebodies $H_i,\ i \in \Gamma$ with selected Torelli automorphisms $h_i : \partial(H_i) \to \partial(H_i),\ i \in \Gamma$, the following identity holds:

$$\sum_{\Gamma' \subset \Gamma} (-1)^{|\Gamma'|} \cdot f(M_{\Gamma'}) = 0 \in A.$$

Two Y_{k+1}-equivalent manifolds are not distinguished by invariants of degree at most k [Mas07]. The converse statement is proved for integral homology 3-spheres by M. Goussarov and K. Habiro [Hab00], [Gou99]; however, in general, the converse statement is not true [Mas07]. The special interest of the equivalence of the above equivalence relations is in the case of homology cylinders. Given an oriented surface Σ, the homology cylinder over Σ is a cobordism M between Σ and $-\Sigma$, which can be obtained from $\Sigma \times [1, -1]$ by a Torelli surgery. Homology cylinders form a natural monoid $\mathrm{Cyl}(\Sigma)$, where the product is the composition of cobordisms. It is shown in [Hab00] and [Gou99] that the quotient of the monoid $\mathrm{Cyl}(\Sigma)$ by the Y_{k+1}-equivalence relation is a group.

In [Hab00] and [Gou99] the following filtration of the monoid $\mathrm{Cyl}(\Sigma)$ is introduced:

$$\mathrm{Cyl}(\Sigma) = \mathrm{Cyl}_1(\Sigma) \supseteq \mathrm{Cyl}_2(\Sigma) \supseteq \mathrm{Cyl}_3(\Sigma) \supseteq \dots,$$

where

$$\mathrm{Cyl}_k(\Sigma) = \{M \in \mathrm{Cyl}(\Sigma) \mid M \text{ is } Y_k - \text{equivalent to } \Sigma \times [1, -1]\}.$$

For $1 \leq k \leq l$, the quotients $\mathrm{Cyl}_k(\Sigma)/Y_l$ are finitely generated subgroups of $\mathrm{Cyl}(\Sigma)/Y_l$ and for $1 \leq k_1 + k_2 \leq l$, one has

$$[\mathrm{Cyl}_{k_1}(\Sigma)/Y_l, \mathrm{Cyl}_{k_2}(\Sigma)/Y_l] \subseteq \mathrm{Cyl}_{k_1+k_2}(\Sigma)/Y_l$$

(see [Hab00], [Gou99]). The following result provides a connection between the above equivalence relations and the dimension subgroup theory.

Theorem 6.6 (Massuyeau [Mas07]). *Let $1 \leq d \leq k$. The following statements are equivalent:*

(1) *The homology cylinders over a surface Σ are Y_{d+1}-equivalent if and only if the $\mathbb{Z}$-valued invariants of degree $\leq d$ do not separate them.*
(2) $D_{d+1}(\mathrm{Cyl}(\Sigma)/Y_{k+1}) = \mathrm{Cyl}_{d+1}(\Sigma)/Y_{k+1}$.

Note that the problem of description of dimension subgroups $D_{d+1}(\mathrm{Cyl}(\Sigma)/Y_{k+1})$ seems to be highly non-trivial. It is shown in [Mas03] that the group $\mathrm{Cyl}(\Sigma)/Y_2$ contains elements of order 2.

6.4 Vanishing Sums of Roots of Unity

We mention next an interesting application, due to T. Y. Lam and K. H. Leung [Lam00], to a problem in number theory.

Given a natural number m, the problem asks for the computation of the set $W(m)$ of all the possible integers n for which there exist mth roots of unity $\alpha_1, \ldots, \alpha_n$ in the field $\mathbb{C}$ of complex numbers such that $\alpha_1 + \cdots + \alpha_n = 0$.

Let $G = \langle z \rangle$ be a cyclic group of order m. Let $m = p_1^{a_1} \ldots p_r^{a_r}$ be the prime factorization of m with $p_1 < \ldots < p_r$ and $\zeta = \zeta_m$ a primitive mth root of unity. Let $\mathbb{N}[G]$ be the subgroup of $\mathbb{Z}[G]$ consisting of elements $\alpha \in \mathbb{Z}[G]$ with coefficients in $\mathbb{N}$, the set of non-negative integers. Consider the ring homomorphisms

$$\varphi : \mathbb{Z}[G] \to \mathbb{Z}[\zeta], \quad \epsilon : \mathbb{Z}[G] \to \mathbb{Z} \tag{6.2}$$

defined by $z \mapsto \zeta$ and $z \mapsto 1$ respectively.

Since, for every prime p and a primitive pth root ζ of unity,

$$1 + \zeta + \cdots + \zeta^{p-1} = 0,$$

it is easy to see that

$$\mathbb{N}p_1 + \cdots + \mathbb{N}p_r \subseteq W(m). \tag{6.3}$$

That equality holds in (6.3) follows from the following

Theorem 6.7 (Lam - Leung [Lam00]). *For every $\alpha \in \mathbb{N}[G] \cap \ker \varphi$, $\epsilon(\alpha) \in \sum_{i=1}^{r} \mathbb{N}p_i$.*

Call a nonzero element $x \in \mathbb{N}[G] \cap \ker \varphi$ to be *minimal* if it cannot be decomposed as a sum of two nonzero elements in $\mathbb{N}[G] \cap \ker \varphi$. For any group

H, let

$$\sigma(H) := \sum_{h \in H} h \in \mathbb{N}[H].$$

Let P_i be the unique subgroup of G of order p_i. The elements $g.\sigma(P_i)$ with $g \in G$ and $i - 1, \dots, r$, are clearly all minimal elements in $\mathbb{N}[G] \cap \ker(\varphi)$; call these elements *symmetric minimal elements.* The crux of the argument in the proof of Theorem 6.7 is the following

Theorem 6.8 (Lam - Leung [Lam00]). *For any minimal $x \in \mathbb{N}[G] \cap \ker(\varphi)$, either*

(*A*) *x is symmetric, or*

(*B*) *$r \geq 3$ and $\epsilon(x) \geq \epsilon_0(x) \geq p_1(p_2 - 1) + p_3 - p_2 > p_3$, where $\epsilon_0(x)$ denotes the cardinality of the support of x.*

To deduce Theorem 6.7 from Theorem 6.8, note that it clearly suffices to consider minimal elements in $\mathbb{N}[G] \cap \ker(\varphi)$. By Theorem 6.8, such an element is either symmetric or $r \geq 3$ and $\epsilon(x) \geq p_1(p_2 - 1) + p_3 - p_2$. Thus either $\epsilon(x) = p_i$ for some i, or

$$\epsilon(x) > p_1(p_2 - 1) > (p_1 - 1)(p_2 - 1),$$

and consequently $\epsilon(x) \in \mathbb{N}p_1 + \mathbb{N}p_2$. $\square$

We thus have

Theorem 6.9 (Lam - Leung [Lam00]). *For any natural number m,*

$$W(m) = \mathbb{N}p_1 + \cdots + \mathbb{N}p_r,$$

where $p_1, \dots, p_r$ are all the distinct prime divisors of m.

The above result in turn has an application to representation theory of finite groups.

Theorem 6.10 (Lam - Leung [Lam00]). *Let χ be the character of a representation of a finite group G over a field F of characteristic 0. Let $g \in G$ be an element of order $m = p_1^{a_1} \dots p_r^{a_r}$ (where $p_1 < p_2 < \dots p_r$) such that $\chi(g) \in \mathbb{Z}$, and let $t := \chi(1) + |\chi(g)|$. If $\chi(g) \leq 0$, then $t \in \sum \mathbb{N}p_i$. If $\chi(g) > 0$ and t is odd, then $t \geq \ell$, where ℓ $(= p_1$ or $p_2)$ is the smallest odd prime dividing m.*

6.5 Fundamental Groups of Projective Curves

Let k be an algebraically closed field of characteristic $p > 0$. For a projective curve D over k, let $\pi_A(D)$ denote the set of isomorphism classes of finite groups occurring as Galois groups of un-ramified Galois covers of D. A group

G occurs as a quotient of the fundamental group $\pi_1(D)$ if and only if it lies in $\pi_A(D)$. For an integer $g \geq 0$, let $\pi_A(g)$ denote the set of finite groups G for which there exists a curve D of genus g such that G lies in $\pi_A(D)$. Let $d(G)$ denote the minimal number of generators of the group G, and let $t(G)$ denote the number of generators of the augmentation ideal $\mathfrak{g}_k$, of the group algebra $k[G]$, as a $k[G]$ module.

Theorem 6.11 (Stevenson [Ste98]). *Let $g \geq 2$ be a positive integer and let G be a finite group with normal Sylow p-subgroup P, such that $d(G/P) \leq g$. Then G lies in $\pi_A(g)$ if and only if $t(G) \leq g$.*