A

Tools from Commutative Algebra

In this Appendix, we present those results from Commutative Algebra that were used in Chaps. 2 and 3. For more details on the subject, the reader is referred to the specialized books [3] and [52] or the encyclopedic treatise [8].

A.1 Localization and Local Rings

I. LOCALIZATION. Let R be a commutative ring and $S \subseteq R$ a multiplicatively closed subset containing 1. The localization $R[S^{-1}]$ of R at S is the ring obtained from R by formally inverting the elements of S. More precisely, $R[S^{-1}]$ consists of the equivalence classes of pairs of the form (r, s), where $r \in R$ and $s \in S$, under the equivalence relation defined by the rule

$$(r, s) \sim (r', s') \text{ if and only if there exists } s_0 \in S \text{ such that } s_0 s r' = s_0 s' r$$

for $r, r' \in R$ and $s, s' \in S$. We denote the equivalence class of a pair (r, s), where $r \in R$ and $s \in S$, by r/s. Addition and multiplication in $R[S^{-1}]$ are defined by the rules

$$r/s + r'/s' = (s'r + sr')/ss' \quad \text{and} \quad (r/s) \cdot (r'/s') = (rr')/(ss')$$

for $r, r' \in R$ and $s, s' \in S$. It is straightforward to verify that these operations are well-defined and endow $R[S^{-1}]$ with the structure of a commutative ring.

Remark A.1 Let S be a multiplicatively closed subset of a commutative ring R containing 1. Then, the group of units $U(R[S^{-1}])$ of the localization $R[S^{-1}]$ consists of those formal fractions $x = r/s \in R[S^{-1}]$, where $r \in R$ and $s \in S$ are such that there exists $t \in R$ with $rt \in S$. Indeed, it is clear that an element x of that form is invertible with inverse $st/rt \in R[S^{-1}]$. Conversely, if $x = r/s \in U(R[S^{-1}])$ and $x^{-1} = r'/s' \in R[S^{-1}]$, for some $r' \in R$ and $s' \in S$, then $rr'/ss' = 1/1 \in R[S^{-1}]$ and hence there exists $s'' \in S$ with $rr's'' = ss's'' \in R$. Then, the element $t = r's'' \in R$ is such that $rt = rr's'' = ss's'' \in S$, as needed. In particular, assume that the multiplicatively closed subset S has the following property: If $r \in R$ is such that there exists $t \in R$ with $rt \in S$, then $r \in S$.[1] In that case, the group of units of the ring $R[S^{-1}]$ consists of the fractions r/s with $r, s \in S$.

We now consider the map

$$\lambda = \lambda_{R,S} : R \longrightarrow R[S^{-1}] ,$$

which is given by $r \mapsto r/1$, $r \in R$. It is clear that λ is a ring homomorphism; as such, it endows the localization $R[S^{-1}]$ with the structure of a commutative R-algebra. The following Proposition characterizes $R[S^{-1}]$ as the universal commutative R-algebra in which the elements of S (more precisely, their canonical images) are invertible.

Proposition A.2 *Let R be a commutative ring, $S \subseteq R$ a multiplicatively closed subset containing 1, $R[S^{-1}]$ the corresponding localization and λ the ring homomorphism defined above. Then, for any commutative ring A and any ring homomorphism $\varphi : R \longrightarrow A$ with the property that $\varphi(S) \subseteq U(A)$, there exists a unique ring homomorphism $\Phi : R[S^{-1}] \longrightarrow A$ with $\Phi \circ \lambda = \varphi$.*

Proof. Given a pair (A, φ), we may define Φ by letting $\Phi(r/s) = \varphi(r)\varphi(s)^{-1}$ for all $r/s \in R[S^{-1}]$. It is easily seen that Φ is a well-defined ring homomorphism and $\Phi \circ \lambda = \varphi$. The uniqueness of Φ satisfying that condition follows since $r/s = \lambda(r)\lambda(s)^{-1} \in R[S^{-1}]$ for all $r \in R$, $s \in S$. □

Corollary A.3 *(i) Let R be a commutative ring and $T \subseteq S \subseteq R$ two multiplicatively closed subsets containing 1. If S' is the multiplicatively closed subset of $R' = R[T^{-1}]$ consisting of the elements of the form s/t, where $s \in S$ and $t \in T$, then there is a unique homomorphism of R-algebras*

$$R'[S'^{-1}] \longrightarrow R[S^{-1}] .$$

Moreover, this homomorphism is bijective and identifies $(r/t)/(s/t')$ with rt'/st for any $r \in R$, $s \in S$ and $t, t' \in T$.

(ii) Let R be a commutative ring and $s, t \in R$ two elements with $u = st$. If S, T and U are the multiplicatively closed subsets of R generated by s, t and u respectively[2] and T' is the image of T in $R' = R[S^{-1}]$, then there is a unique R-algebra homomorphism

$$R'[T'^{-1}] \longrightarrow R[U^{-1}] .$$

Moreover, this homomorphism is bijective and identifies $(r/s^n)/(t^m/1)$ with $rs^m t^n/u^{n+m}$ for any $r \in R$ and $n, m \geq 0$.

---

[1] This property can be rephrased by saying that the complement $I = R \setminus S$ is such that $IR \subseteq I$.

[2] By this, we mean that S consists of the powers s^n, $n \geq 0$, of s and similarly for T and U.

Proof. Assertion (i) follows since $R'[S'^{-1}]$ is the universal commutative R-algebra in which the image of S consists of invertible elements. Similarly, the claim in (ii) is a consequence of the observation that the universal commutative R-algebra in which the images of s and t are invertible is precisely the universal commutative R-algebra in which the image of their product u is invertible. □

Our next goal is to prove the flatness of localization. To that end, we let S be a multiplicatively closed subset of a commutative ring R containing 1 and fix an R-module M. We then consider the $R[S^{-1}]$-module $M[S^{-1}]$, which is defined as follows: As a set, $M[S^{-1}]$ consists of the equivalence classes of pairs of the form (m, s), where $m \in M$ and $s \in S$, under the equivalence relation defined by the rule

$$(m, s) \sim (m', s') \text{ if and only if there exists } s_0 \in S \text{ such that } s_0 s m' = s_0 s' m$$

for $m, m' \in M$ and $s, s' \in S$. We denote the equivalence class of a pair (m, s), where $m \in M$ and $s \in S$, by m/s. Addition and the $R[S^{-1}]$-action on $M[S^{-1}]$ are defined by the rules

$$m/s + m'/s' = (s'm + sm')/ss' \quad \text{and} \quad (r/s) \cdot (m'/s') = (rm')/(ss')$$

for $m, m' \in M$, $r \in R$ and $s, s' \in S$. It is straightforward to verify that these operations are well-defined and endow $M[S^{-1}]$ with the structure of an $R[S^{-1}]$-module.

Pursuing further the analogy with the construction of the ring $R[S^{-1}]$, we consider the map

$$\lambda = \lambda_{M,S} : M \longrightarrow M[S^{-1}] ,$$

which is given by $m \mapsto m/1$, $m \in M$. Then, λ is R-linear and has the universal property described in the following result.

Proposition A.4 *Let R be a commutative ring, $S \subseteq R$ a multiplicatively closed subset containing 1, M an R-module, $M[S^{-1}]$ the $R[S^{-1}]$-module defined above and $\lambda : M \longrightarrow M[S^{-1}]$ the corresponding R-linear map. Then, for any $R[S^{-1}]$-module N and any R-linear map $\varphi : M \longrightarrow N'$ there exists a unique $R[S^{-1}]$-linear map $\Phi : M[S^{-1}] \longrightarrow N$ with $\Phi \circ \lambda = \varphi$. (Here, we denote by N' the R-module obtained from N by restricting the scalars along the natural homomorphism $R \longrightarrow R[S^{-1}]$.)*

Proof. Given a pair (N, φ), we may define Φ by letting $\Phi(m/s) = (1/s) \cdot \varphi(m)$ for all $m/s \in M[S^{-1}]$. Then, Φ is a well-defined $R[S^{-1}]$-linear map such that $\Phi \circ \lambda = \varphi$. The uniqueness of Φ satisfying that condition follows since $m/s = (1/s) \cdot \lambda(m) \in M[S^{-1}]$ for all $m \in M$, $s \in S$. □

Corollary A.5 *Let R be a commutative ring, $S \subseteq R$ a multiplicatively closed subset containing 1 and M an R-module.*

(i) There is an $R[S^{-1}]$-module isomorphism $M \otimes_R R[S^{-1}] \simeq M[S^{-1}]$, which identifies $m \otimes 1/s$ with m/s for all $m \in M$ and $s \in S$.

(ii) If there exists an element $s \in S$ such that $sM = 0$, then the $R[S^{-1}]$-module $M \otimes_R R[S^{-1}]$ vanishes.

(iii) If the R-module M is finitely generated and the $R[S^{-1}]$-module $M \otimes_R R[S^{-1}]$ vanishes, then there exists $s \in S$ such that $sM = 0$.

Proof. (i) This follows from Proposition A.4, in view of the universal property of the $R[S^{-1}]$-module $M \otimes_R R[S^{-1}]$.

(ii) If $s \in S$ and $m \in M$ are such that $sm = 0$, then $m/1 = 0/1 \in M[S^{-1}]$. Therefore, if $sM = 0$ then $M \otimes_R R[S^{-1}] \simeq M[S^{-1}] = 0$.

(iii) Assume that M is generated over R by $m_1, \ldots, m_n$. Since the module $M[S^{-1}] \simeq M \otimes_R R[S^{-1}]$ vanishes, we have $m_i/1 = 0/1 \in M[S^{-1}]$ for all $i = 1, \ldots, n$. But then there exists for each i an element $s_i \in S$, such that $s_i m_i = 0$. If $s = \prod_{i=1}^n s_i \in S$ then s annihilates all generators $m_1, \ldots, m_n$ of M and hence $sM = 0$. □

Corollary A.6 *Let R be a commutative ring and $S \subseteq R$ a multiplicatively closed subset containing 1. Then, the R-module $R[S^{-1}]$ is flat.*

Proof. In view of Corollary A.5(i), we have to verify that the functor $M \mapsto M[S^{-1}]$, M an R-module, is left exact. In other words, we have to verify that for any submodule N of an R-module M the map $N[S^{-1}] \longrightarrow M[S^{-1}]$, which maps $n/s \in N[S^{-1}]$ onto $n/s \in M[S^{-1}]$ is injective. But this is clear from the definition of equality in the modules $M[S^{-1}]$ and $N[S^{-1}]$. □

II. Localization at a prime ideal. An important class of multiplicatively closed subsets of a commutative ring R is that arising from prime ideals. If $\wp \subseteq R$ is a prime ideal (i.e. if $\wp$ is a proper ideal of R such that the quotient ring $R/\wp$ is an integral domain) then the complement $S = R \setminus \wp$ is multiplicatively closed and contains 1. The corresponding localization is denoted by $R_\wp$ and referred to (by an obvious abuse of language) as the localization of R at $\wp$. For example, if R is an integral domain then 0 is a prime ideal and the localization R_0 is the field of fractions of R.

The following result describes a property of localization that was used in a crucial way in §2.1.1, in the proof of the continuity of the geometric rank function associated with a finitely generated projective module.

Proposition A.7 *Let R be a commutative ring, M (resp. P) a finitely generated (resp. finitely generated projective) R-module and $\varphi : M \longrightarrow P$ an R-linear map. Assume that $\wp \subseteq R$ is a prime ideal, such that φ becomes an isomorphism when localized at $\wp$. Then, there exists an element $u \in R \setminus \wp$, such that φ becomes an isomorphism after inverting u (i.e. when localizing at the multiplicatively closed subset $U \subseteq R$ generated by u).*

Proof. The localized map $\varphi \otimes 1 : M \otimes_R R_\wp \longrightarrow P \otimes_R R_\wp$ being bijective, the R-flatness of $R_\wp$ (cf. Corollary A.6) implies that both $\ker \varphi \otimes_R R_\wp$ and $\operatorname{coker} \varphi \otimes_R R_\wp$ vanish. Since the R-module $\operatorname{coker} \varphi$ is finitely generated, Corollary A.5(iii) implies that there exists $s \in R \setminus \wp$ such that $s \cdot \operatorname{coker} \varphi = 0$. Let S be the multiplicatively closed subset of R generated by s; we note that $S \subseteq R \setminus \wp$. If $R' = R[S^{-1}]$, $\varphi' = \varphi \otimes 1$ and $\wp' = \wp R[S^{-1}]$, then the R-flatness of R' and the vanishing of $\operatorname{coker} \varphi \otimes_R R'$ (cf. Corollary A.5(ii)) show that there is a short exact sequence of R'-modules

$$0 \longrightarrow \ker \varphi \otimes_R R' \longrightarrow M \otimes_R R' \xrightarrow{\varphi'} P \otimes_R R' \longrightarrow 0 \, .$$

Since the R'-module $P \otimes_R R'$ is projective, this short exact sequence splits; in particular, the R'-module $\ker \varphi' = \ker \varphi \otimes_R R'$ is finitely generated. We note that

$$\ker \varphi' \otimes_{R'} R'_{\wp'} = \ker \varphi \otimes_R R'_{\wp'} = \ker \varphi \otimes_R R_\wp = 0 \, ,$$

where the second equality follows using Corollary A.3(i). Hence, we may invoke Corollary A.5(iii) once again in order to find an element $t' \in R' \setminus \wp'$ with $t' \cdot \ker \varphi' = 0$. Without loss of generality, we assume that $t' = t/1$ for some $t \in R \setminus \wp$. Let U (resp. T') be the multiplicatively closed subset of R (resp. R') generated by $u = st \in R \setminus \wp$ (resp. by t'). Then,

$$\ker \varphi \otimes_R R[U^{-1}] = \ker \varphi \otimes_R R'[T'^{-1}] = \ker \varphi' \otimes_{R'} R'[T'^{-1}] = 0 \, ,$$

where the first (resp. third) equality follows from Corollary A.3(ii) (resp. Corollary A.5(ii)). Since $u = st$ annihilates $\operatorname{coker} \varphi$, Corollary A.5(ii) implies that $\operatorname{coker} \varphi \otimes_R R[U^{-1}] = 0$. It follows that the map

$$\varphi \otimes 1 : M \otimes_R R[U^{-1}] \longrightarrow P \otimes_R R[U^{-1}]$$

is an isomorphism and this finishes the proof. □

III. Local rings. A commutative ring is called local if it has a unique maximal ideal. For example, any field is local, whereas the ring $\mathbf{Z}$ is not.

Remarks A.8 (i) It is clear that any proper ideal in a commutative ring consists of singular (i.e. non-invertible) elements. In fact, if R is a local ring then its maximal ideal $\mathbf{m}$ is precisely the set of singular elements. Indeed, if $r \in R$ is not invertible then the ideal Rr is proper and hence contained in the (unique) maximal ideal $\mathbf{m}$, i.e. $r \in \mathbf{m}$.

(ii) As a converse to (i), we note that if the set of singular elements of a commutative ring R forms an ideal I, then R is a local ring with maximal ideal $\mathbf{m} = I$. This is clear since any proper ideal J of R consists of singular elements and is therefore contained in I.

(iii) If R is a commutative ring and $\wp \subseteq R$ a prime ideal, then the localization $R_\wp$ is a local ring with maximal ideal

$$\wp R_\wp = \{r/s : r \in \wp, s \notin \wp\} \subseteq R_\wp \, .$$

This is an immediate consequence of (ii) above, as soon as one notices that an element of the localization $R_\wp$ is invertible if and only if it is of the form r/s, with $r, s \notin \wp$ (cf. Remark A.1).

Our next goal is to show that any finitely generated projective module over a local ring is free,[3] a fact used in the very definition of the geometric rank function associated with a finitely generated projective module in §2.1.1. To that end, we need the following lemma.

Lemma A.9 *Let R be a commutative ring, $I \subseteq R$ a proper ideal and M a finitely generated R-module satisfying the equality $IM = M$. Then, there exists an element $r \in I$ such that $(1 + r)M = 0$. In particular, M is trivial (i.e. $M = 0$) if either one of the following two conditions is satisfied:*
(i) (Nakayama) R is a local ring or
(ii) R is an integral domain and the R-module M is torsion-free.

Proof. If $M = \sum_{i=1}^{n} Rm_i$ then $IM = \sum_{i=1}^{n} Im_i$ and hence we can write $m_i = \sum_{j=1}^{n} r_{ij}m_j$, for suitable elements $r_{ij} \in I$. It follows that the matrix

$$A = \begin{bmatrix} 1 - r_{11} & -r_{12} & \cdots & -r_{1n} \\ -r_{21} & 1 - r_{22} & \cdots & -r_{2n} \\ \vdots & \vdots & & \vdots \\ -r_{n1} & -r_{n2} & \cdots & 1 - r_{nn} \end{bmatrix} \in \mathbf{M}_n(R)$$

annihilates the $n \times 1$ column-vector

$$\vec{m} = \begin{bmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{bmatrix}$$

Multiplying the equation $A \cdot \vec{m} = \mathbf{0}$ to the left by the matrix $\operatorname{adj} A$, we deduce that the element $\det A \in R$ annihilates all of the m_i's. Since these elements generate M, we conclude that $(\det A)M = 0$. It is immediate by the form of the matrix A that $\det A = 1 + r$, for a suitable element $r \in I$.

(i) Assume that the ring R is local with maximal ideal $\mathbf{m}$. Since the ideal I is proper, we have $I \subseteq \mathbf{m}$ and hence $1 + r \notin \mathbf{m}$. In view of Remark A.8(i), we conclude that $1 + r$ is invertible in R. The equation $(1 + r)M = 0$ then shows that $M = 0$.

(ii) Assume that R is an integral domain, whereas M is torsion-free and non-zero. Then, the equation $(1 + r)M = 0$ implies that $1 + r = 0$. But then $1 = -r \in I$, contradicting our assumption that I is proper. □

Proposition A.10 *Let R be a local ring and P a finitely generated projective R-module. Then, P is free.*

Proof. Let $\mathbf{m}$ be the maximal ideal of R and $k = R/\mathbf{m}$ the residue field. Then, $P/\mathbf{m}P = P \otimes_R k$ is a finite dimensional k-vector space; hence, it has a basis

[3] In fact, any projective module (not necessarily finitely generated) over a local ring is free; this result is due to I. Kaplansky [37].

$\overline{x_1}, \ldots, \overline{x_n}$ for suitable elements $x_1, \ldots, x_n \in P$. We shall prove that the x_i's form a basis of P by showing that the R-linear map $\varphi : R^n \longrightarrow P$, which maps $(r_1, \ldots, r_n) \in R^n$ onto $r_1 x_1 + \ldots + r_n x_n \in P$ is an isomorphism. The exact sequence of R-modules

$$R^n \xrightarrow{\varphi} P \longrightarrow \operatorname{coker}\varphi \longrightarrow 0$$

induces the exact sequence of k-vector spaces

$$k^n \xrightarrow{\varphi\otimes 1} P \otimes_R k \longrightarrow \operatorname{coker}\varphi \otimes_R k \longrightarrow 0 .$$

Since $\varphi \otimes 1$ is bijective, the k-vector space $\operatorname{coker}\varphi \otimes_R k$ vanishes. Therefore, Nakayama's lemma implies that the finitely generated R-module $\operatorname{coker}\varphi$ is actually zero and hence φ is onto. We note that the short exact sequence of R-modules

$$0 \longrightarrow \ker\varphi \longrightarrow R^n \xrightarrow{\varphi} P \longrightarrow 0$$

splits, since P is projective. It follows that the R-module $\ker\varphi$ is finitely generated, whereas there is an induced (split) short exact sequence

$$0 \longrightarrow \ker\varphi \otimes_R k \longrightarrow k^n \xrightarrow{\varphi\otimes 1} P \otimes_R k \longrightarrow 0 .$$

As before, Nakayama's lemma implies that $\ker\varphi = 0$ and hence φ is 1-1. □

A.2 Integral Dependence

Let us consider a commutative ring R and a commutative R-algebra T. An element $t \in T$ is called integral over R if there is a monic polynomial $f(X) \in R[X]$, such that $f(t) = 0 \in T$. It is clear that elements in the canonical image of R in T are integral over R; if these are the only elements of T that are integral over R, then R is said to be integrally closed in T. On the other extreme, the algebra T is called integral over R (or an integral extension of R) if any element $t \in T$ is integral over R. The following result establishes a few equivalent formulations of the integrality condition.

Proposition A.11 *Let R be a commutative ring and T a commutative R-algebra. Then, the following conditions are equivalent for an element $t \in T$:*

(i) t is integral over R.

(ii) The R-subalgebra $R[t] \subseteq T$ is finitely generated as an R-module.

(iii) There is a finitely generated R-submodule $M \subseteq T$ containing 1, *such that $tM \subseteq M$.*

Proof. (i)→(ii): Assume that t is integral over R. Then, there is an integer $n \geq 1$ and elements $r_0, \ldots, r_{n-1} \in R$, such that

$$t^n + r_{n-1}t^{n-1} + \cdots + r_1 t + r_0 = 0 \in T .$$

It follows that t^n is an R-linear combination of $1, t, \ldots, t^{n-1}$ and hence $R[t] = \sum_{i=0}^{n-1} Rt^i$ is a finitely generated R-module.

(ii)→(iii): This is clear, since we may choose $M = R[t]$.

(iii)→(i): Let $M = \sum_{i=1}^{n} Rm_i \subseteq T$ be an R-submodule of T that contains 1 and is closed under multiplication by t. Then, there are equations of the form $tm_i = \sum_{j=1}^{n} r_{ij} m_j$, $i = 1, \ldots, n$, for suitable elements $r_{ij} \in R$. It follows that the $n \times n$ matrix

$$A = \begin{bmatrix} t - r_{11} & -r_{12} & \cdots & -r_{1n} \\ -r_{21} & t - r_{22} & \cdots & -r_{2n} \\ \vdots & \vdots & & \vdots \\ -r_{n1} & -r_{n2} & \cdots & t - r_{nn} \end{bmatrix} \in \mathbf{M}_n(T)$$

annihilates the $n \times 1$ column-vector

$$\vec{m} = \begin{bmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{bmatrix}$$

Multiplying the equation $A \cdot \vec{m} = \mathbf{0}$ to the left by the matrix $\operatorname{adj} A$, we deduce that the element $\det A \in T$ annihilates all of the m_i's. Since these elements generate the R-module M, it follows that $\det A$ annihilates M; in particular, $\det A = (\det A)1 = 0$. Then, the expansion of $\det A$ provides us with an equation that shows t to be integral over R. □

Corollary A.12 *Let R be a commutative ring, T a commutative R-algebra and U a commutative T-algebra.*

(i) If $t_1, \ldots, t_n \in T$ are integral over R, then the finitely generated R-subalgebra $R[t_1, \ldots, t_n] \subseteq T$ is finitely generated as an R-module.

(ii) If $u \in U$ is integral over T and T is integral over R, then u is integral over R. In particular, if U is integral over T and T integral over R, then U is integral over R.

Proof. (i) We use induction on n, the case $n = 1$ following from Proposition A.11. Since t_n is integral over R, it is also integral over $R[t_1, \ldots, t_{n-1}]$. Therefore, Proposition A.11 implies that $R[t_1, \ldots, t_n] = R[t_1, \ldots, t_{n-1}][t_n]$ is finitely generated as an $R[t_1, \ldots, t_{n-1}]$-module. By the induction hypothesis, $R[t_1, \ldots, t_{n-1}]$ is finitely generated as an R-module and hence $R[t_1, \ldots, t_n]$ is finitely generated as an R-module (cf. Lemma 1.1(i)).

(ii) Since u is integral over T, there is an integer $n \geq 1$ and elements $t_0, \ldots, t_{n-1} \in T$, such that

$$u^n + t_{n-1} u^{n-1} + \cdots + t_1 u + t_0 = 0 \in U \ .$$

This equation shows that u is integral over the ring $R' = R[t_0, \ldots, t_{n-1}]$. It follows from Proposition A.11 that $R'[u]$ is finitely generated as an R'-module. But R' is finitely generated as an R-module, in view of (i) above, and hence $R'[u]$ is finitely generated as an R-module (cf. Lemma 1.1(i)). Using Proposition A.11 once again, we deduce that u is integral over R. □

Corollary A.13 *Let R be a commutative ring, T a commutative R-algebra and $R' = \{t \in T : t$ is integral over $R\}$. Then:*

(i) R' is an R-subalgebra of T and

(ii) R' is integrally closed in T.

The R-algebra R' is called the integral closure of R in T.

Proof. (i) For any $t_1, t_2 \in R'$ the R-algebra $R[t_1, t_2]$ is finitely generated as an R-module, in view of Corollary A.12(i). Since $R[t_1, t_2]$ contains 1 and is closed under multiplication by $t_1 \pm t_2$ and $t_1 t_2$, Proposition A.11 implies that $t_1 \pm t_2, t_1 t_2 \in R'$. It follows that R' is a subring of T. Since $r \cdot 1 \in T$ is obviously integral over R for any $r \in R$, it follows that R' is an R-submodule of T (and hence an R-subalgebra of it).

(ii) This is an immediate consequence of Corollary A.12(ii). □

The next result describes some basic properties of the integral closure of a domain in an extension of its field of fractions.

Lemma A.14 *Let R be an integral domain, K its field of fractions, L an algebraic extension field of K and T the integral closure of R in L.*

(i) For any $x \in L$ there exists $r \in R \setminus \{0\}$, such that $rx \in T$. In particular, L is the field of fractions of T.

(ii) Any field automorphism σ of L over K restricts to an automorphism of T over R.

Proof. (i) Any element $x \in L$ is algebraic over K and hence satisfies an equation of the form

$$r_n x^n + r_{n-1} x^{n-1} + \cdots + r_1 x + r_0 = 0 ,$$

for an integer $n \geq 1$ and suitable elements $r_0, \ldots, r_n \in R$, with $r_n \neq 0$. Multiplying that equation by r_n^{n-1}, we obtain the equation

$$(r_n x)^n + r_{n-1}(r_n x)^{n-1} + \cdots + r_n^{n-2} r_1 (r_n x) + r_n^{n-1} r_0 = 0 .$$

Hence, $r_n x$ is integral over R, i.e. $r_n x \in T$.

(ii) Any element $t \in T$ satisfies an equation of the form

$$t^n + r_{n-1} t^{n-1} + \cdots + r_1 t + r_0 = 0 ,$$

for an integer $n \geq 1$ and suitable elements $r_0, \ldots, r_{n-1} \in R$. If σ is an automorphism of L over K, then the element $\sigma(t) \in L$ satisfies the equation

$$\sigma(t)^n + r_{n-1}\sigma(t)^{n-1} + \cdots + r_1 \sigma(t) + r_0 = 0 .$$

Hence, $\sigma(t)$ is integral over R, i.e. $\sigma(t) \in T$. Considering the automorphism σ^{-1} of L over K, it follows that σ maps T bijectively onto itself. □

Having the ring **Z** of integers in mind, we examine the case where R is a principal ideal domain or, more generally, a unique factorization domain.

Lemma A.15 *A unique factorization domain is integrally closed in its field of fractions.*

Proof. Let R be a unique factorization domain and K its field of fractions. An element $x \in K$ is not contained in R if it can be expressed as a quotient of the form a/b, where the elements $a, b \in R \setminus \{0\}$ are relatively prime and b is not a unit. If such an element x is integral over R, it satisfies an equation of the form

$$x^n + r_{n-1}x^{n-1} + \cdots + r_1 x + r_0 = 0 \in K \ ,$$

for an integer $n \geq 1$ and suitable elements $r_0, \ldots, r_{n-1} \in R$. Multiplying that equation by b^n, we obtain the equality

$$a^n + r_{n-1}ba^{n-1} + \cdots + r_1 b^{n-1}a + r_0 b^n = 0 \in R \ . \qquad \text{(A.1)}$$

Since b is not a unit, it has a prime divisor p. Then, p divides the sum

$$r_{n-1}ba^{n-1} + \cdots + r_1 b^{n-1}a + r_0 b^n = b(r_{n-1}a^{n-1} + \cdots + r_1 b^{n-2}a + r_0 b^{n-1})$$

and hence (A.1) implies that p divides a^n. But the prime p does not divide a, since a and b are relatively prime, and this is a contradiction. □

Corollary A.16 *Let R be a unique factorization domain, K its field of fractions, L a Galois extension field of K and T the integral closure of R in L. Let $x \in T$ and consider its Galois conjugates $x_1(= x), x_2, \ldots, x_k$. Then, the polynomial $f(X) = \prod_{i=1}^{k}(X - x_i)$ has coefficients in R.*

Proof. First of all, we note that the x_i's are contained in T, in view of Lemma A.14(ii); therefore, $f(X)$ is a polynomial in $T[X]$. Being a symmetric polynomial in the x_i's, any coefficient $y \in T$ of $f(X)$ is invariant under the action of the Galois group of L over K and hence $y \in K$. Since $T \cap K = R$, in view of Lemma A.15, we conclude that $y \in R$. □

Corollary A.17 *Let R be a principal ideal domain contained in an integral domain T and assume that T is integral over R. Then, for any prime element $p \in R$ there exists a maximal ideal $\mathbf{m} \subseteq T$, such that $R \cap \mathbf{m} = pR$; in that case, the field $T/\mathbf{m}$ is an extension of R/pR.*

Proof. First of all, we note that elements of R that are invertible in T must be already invertible in R; this follows from Lemma A.15, since T is integral over R, whereas the principal ideal domain R is a unique factorization domain.[4] In particular, a prime element $p \in R$ is not invertible in T and hence the ideal $pT \subseteq T$ is proper. If $\mathbf{m} \subseteq T$ is a maximal ideal containing pT, then the

[4] In fact, one doesn't need the assumption that R is a principal ideal domain; cf. Exercise A.5.1.

contraction $R \cap \mathbf{m}$ is a prime (and hence proper) ideal of R containing pR. But pR is a maximal ideal of R and hence $R \cap \mathbf{m} = pR$. □

We now specialize the above discussion and consider the subring $\mathcal{R}$ of $\overline{\mathbf{Q}}$ consisting of those algebraic numbers that are integral over $\mathbf{Z}$; this is the ring of algebraic integers. The following three properties of $\mathcal{R}$ are immediate consequences of the general results established above.

(AI1) For any algebraic number $x \in \overline{\mathbf{Q}}$ there is a non-zero integer n, such that $nx \in \mathcal{R}$.
(AI2) Let x be an algebraic integer and $x_1(= x), x_2, \ldots, x_k$ its Galois conjugates. Then, all x_i's are algebraic integers, whereas the polynomial $\prod_{i=1}^{k}(X - x_i)$ has coefficients in $\mathbf{Z}$.
(AI3) For any prime number $p \in \mathbf{Z}$ there exists a maximal ideal $\mathcal{M} \subseteq \mathcal{R}$, such that $\mathbf{Z} \cap \mathcal{M} = p\mathbf{Z}$; then, the field $\mathcal{R}/\mathcal{M}$ has characteristic p.

A.3 Noether Normalization

I. Finitely generated algebras over fields. In order to obtain some information on the structure of finitely generated commutative algebras over a field, we begin with a few simple observations on polynomials.

Lemma A.18 *Let R be an integral domain of characteristic 0 and consider m distinct polynomials $f_1(X), \ldots, f_m(X) \in R[X]$. Then, there exists $t_0 \in \mathbf{N}$ such that for all $t \in \mathbf{N}$ with $t > t_0$ the m elements $f_1(t), \ldots, f_m(t) \in R$ are distinct.*

Proof. For any $i \neq j$, the equation $f_i(X) = f_j(X)$ has finitely many roots in R. Since $\mathbf{N} \subseteq \mathbf{Z}$ is contained in R, the set $\Lambda_{ij} = \{t \in \mathbf{N} : f_i(t) = f_j(t)\}$ is finite. Being a finite union of finite sets, the set $\Lambda = \bigcup_{i \neq j} \Lambda_{ij}$ is finite as well. We now let $t_0 = \max \Lambda$ and note that if $t \in \mathbf{N}$ exceeds t_0, then $t \notin \Lambda_{ij}$ (i.e. $f_i(t) \neq f_j(t)$) for all $i \neq j$. □

Corollary A.19 *Let $\left(k_j^{(1)}\right)_j, \ldots, \left(k_j^{(m)}\right)_j \in \mathbf{N}^n$ be m distinct n-tuples of non-negative integers. Then, there are positive integers $t_1, \ldots, t_n$, with $t_n = 1$, such that the m integers $\sum_{j=1}^{n} t_j k_j^{(1)}, \ldots, \sum_{j=1}^{n} t_j k_j^{(m)} \in \mathbf{N}$ are distinct.*

Proof. For all $i = 1, \ldots, m$, we consider the polynomial

$$f_i(X) = \sum_{j=1}^{n} k_j^{(i)} X^{n-j} \in \mathbf{Z}[X] .$$

In view of our assumption, the polynomials $f_1(X), \ldots, f_m(X)$ are distinct. Hence, we may invoke Lemma A.18 in order to find $t \in \mathbf{N}$, $t > 0$, such that the m integers $\sum_{j=1}^{n} k_j^{(1)} t^{n-j}, \ldots, \sum_{j=1}^{n} k_j^{(m)} t^{n-j} \in \mathbf{Z}$ are distinct. The proof is finished by letting $t_j = t^{n-j}$ for all $j = 1, \ldots, n$. □

Let k be a commutative ring, R a commutative k-algebra and $k[X_1, \ldots, X_n]$ the polynomial k-algebra in n variables. Then, for any n-tuple of elements $(r_1, \ldots, r_n) \in R^n$ there is a unique k-algebra homomorphism

$$\mathbf{r} : k[X_1, \ldots, X_n] \longrightarrow R \ ,$$

which maps X_i onto r_i for all $i = 1, \ldots, n$. The image of a polynomial $f(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n]$ under $\mathbf{r}$ is denoted by $f(r_1, \ldots, r_n)$ and referred to as the evaluation of f at the n-tuple $(r_1, \ldots, r_n)$.

In particular, let us consider n other variables $Y_1, \ldots, Y_{n-1}, X$ and the corresponding polynomial algebra $R = k[Y_1, \ldots, Y_{n-1}, X]$. If $t_1, \ldots, t_{n-1}$ are positive integers, then the n-tuple $(Y_1 + X^{t_1}, \ldots, Y_{n-1} + X^{t_{n-1}}, X) \in R^n$ induces a homomorphism of k-algebras

$$k[X_1, \ldots, X_n] \longrightarrow R = k[Y_1, \ldots, Y_{n-1}, X] \ ,$$

which maps X_i onto $Y_i + X^{t_i}$ for all $i = 1, \ldots, n-1$ and X_n onto X. For any polynomial $f(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n]$ the element

$$g(Y_1, \ldots, Y_{n-1}, X) = f(Y_1 + X^{t_1}, \ldots, Y_{n-1} + X^{t_{n-1}}, X) \in R$$

may be viewed as a polynomial in X with coefficients in $k[Y_1, \ldots, Y_{n-1}]$. If the degree of g in X is m, then we can write

$$f(Y_1 + X^{t_1}, \ldots, Y_{n-1} + X^{t_{n-1}}, X) = \sum\nolimits_{i=0}^{m} g_i(Y_1, \ldots, Y_{n-1}) X^i, \qquad \text{(A.2)}$$

where $g_i(Y_1, \ldots, Y_{n-1}) \in k[Y_1, \ldots, Y_{n-1}]$ for all i and $g_m(Y_1, \ldots, Y_{n-1}) \neq 0$.

Corollary A.20 *Let k be a commutative ring, $X_1, \ldots, X_n, Y_1, \ldots, Y_{n-1}, X$ independent indeterminates and $f(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n]$ a non-zero polynomial. Then, there are positive integers $t_1, \ldots, t_{n-1}$, such that the leading coefficient $g_m(Y_1, \ldots, Y_{n-1}) \in k[Y_1, \ldots, Y_{n-1}]$ of X in the expression (A.2) of*

$$g(Y_1, \ldots, Y_{n-1}, X) = f(Y_1 + X^{t_1}, \ldots, Y_{n-1} + X^{t_{n-1}}, X) \in k[Y_1, \ldots, Y_{n-1}, X]$$

is a non-zero element of k.

Proof. Let $aX_1^{k_1} \cdots X_n^{k_n}$ be a monomial of the polynomial $f(X_1, \ldots, X_n)$, where $a \in k$ is non-zero and the k_i's are non-negative integers. For any choice of positive integers $t_1, \ldots, t_{n-1}$, it is clear that the monomial in $Y_1, \ldots, Y_{n-1}, X$ of the summand $a(Y_1 + X^{t_1})^{k_1} \cdots (Y_{n-1} + X^{t_{n-1}})^{k_{n-1}} X^{k_n}$ of $g(Y_1, \ldots, Y_{n-1}, X)$ with the highest degree in X is the product

$$aX^{t_1 k_1} \cdots X^{t_{n-1} k_{n-1}} X^{k_n} = aX^{t_1 k_1 + \cdots + t_{n-1} k_{n-1} + k_n} \ ,$$

whereas all other monomials of $a(Y_1 + X^{t_1})^{k_1} \cdots (Y_{n-1} + X^{t_{n-1}})^{k_{n-1}} X^{k_n}$ have degree in X strictly less than $t_1 k_1 + \cdots + t_{n-1} k_{n-1} + k_n$. In view of Corollary A.19, we may choose the positive numbers $t_1, \ldots, t_{n-1}$, in such a way that the exponents $t_1k_1+\cdots+t_{n-1}k_{n-1}+k_n$ that result from the various monomials of $f(X_1,\ldots,X_n)$ are distinct. Then, the largest of these exponents is the degree m of g in X, whereas the leading term g_mX^m is of the form $a'X^m$ for some non-zero element $a' \in k$. □

We are now ready to state and prove the normalization lemma.

Theorem A.21 *(Noether normalization lemma) Let k be a field and R a finitely generated commutative k-algebra. Then, there exists a k-subalgebra $R_0 \subseteq R$, such that:*

(i) R_0 is a polynomial k-algebra and

(ii) R is an integral extension of R_0.

Proof. Let $R = k[r_1,\ldots,r_n]$ for suitable elements $r_1,\ldots,r_n \in R$. We shall use induction on n.

If $n = 1$, then either r_1 is algebraically independent over k, in which case we may let $R_0 = R$, or else r_1 satisfies a (monic) polynomial equation with coefficients in k, in which case $\dim_k R < \infty$ and we let $R_0 = k$.

Assume that $n > 1$ and the result has been proved for k-algebras generated by $n-1$ elements. If the elements $r_1,\ldots,r_n$ are algebraically independent over k, we may let $R_0 = R$. If not, there exists a non-zero polynomial $f(X_1,\ldots,X_n) \in k[X_1,\ldots,X_n]$, such that $f(r_1,\ldots,r_n) = 0$. In view of Corollary A.20, we can find positive integers $t_1,\ldots,t_{n-1}$ such that the leading coefficient $g_m(Y_1,\ldots,Y_{n-1}) \in k[Y_1,\ldots,Y_{n-1}]$ of X in the expression (A.2) of the polynomial

$$g(Y_1,\ldots,Y_{n-1},X) = f(Y_1+X^{t_1},\ldots,Y_{n-1}+X^{t_{n-1}},X) \in k[Y_1,\ldots,Y_{n-1},X]$$

is a non-zero element $a \in k$. Replacing the polynomial $f(X_1,\ldots,X_n)$ by $a^{-1}f(X_1,\ldots,X_n)$, we may assume that $g_m(Y_1,\ldots,Y_{n-1}) = 1$. Then, g may be viewed as a monic polynomial in X with coefficients in $k[Y_1,\ldots,Y_{n-1}]$. Let $r_1' = r_1 - r_n^{t_1}, \ldots r_{n-1}' = r_{n-1} - r_n^{t_{n-1}}$ and consider the k-subalgebra $R' = k[r_1',\ldots,r_{n-1}'] \subseteq R$. It is clear that $R = k[r_1,\ldots,r_n]$ can be generated by $r_1',\ldots,r_{n-1}',r_n$ and hence $R = k[r_1',\ldots,r_{n-1}',r_n] = R'[r_n]$. Since

$$\begin{aligned} g(r_1',\ldots,r_{n-1}',r_n) &= f(r_1'+r_n^{t_1},\ldots,r_{n-1}'+r_n^{t_{n-1}},r_n) \\ &= f(r_1,\ldots,r_{n-1},r_n) \\ &= 0, \end{aligned}$$

r_n is a root of the monic polynomial $g(r_1',\ldots,r_{n-1}',X) \in R'[X]$. Therefore, $R = R'[r_n]$ is a finitely generated R'-module and hence R is integral over R' (cf. Proposition A.11). In view of the induction hypothesis, there exists a k-subalgebra $R_0 \subseteq R'$, such that R_0 is a polynomial k-algebra and R' is integral over it. Since R is integral over R', we may invoke Corollary A.12(ii) and conclude that R is integral over R_0 as well. □

Often, we apply Noether's normalization lemma in the form of one of the following corollaries.

Corollary A.22 *Let k be a subring of a field K.*

(i) If K is integral over k, then k is a field.

(ii) If k is a field and K is finitely generated as a k-algebra, then K is a finite algebraic extension of k.

Proof. (i) If a is a non-zero element of k, then $a^{-1} \in K$ is integral over k and hence

$$a^{-n} + b_{n-1}a^{-n+1} + \cdots + b_1 a^{-1} + b_0 = 0 \, ,$$

for an integer $n \geq 1$ and suitable elements $b_0, \ldots, b_{n-1} \in k$. Multiplying that equation by a^{n-1}, we conclude that

$$a^{-1} + b_{n-1} + \cdots + b_1 a^{n-2} + b_0 a^{n-1} = 0$$

and hence $a^{-1} \in k$.

(ii) In view of Noether's normalization lemma, we can find a polynomial k-algebra K_0 contained in K, such that K is integral over it. Using the result of part (i), we conclude that K_0 is a field. Being a polynomial algebra over k, K_0 can be a field only if $K_0 = k$. Therefore, K is an integral (i.e. algebraic) extension of k. □

Corollary A.23 *Let k be an algebraically closed field and R a finitely generated commutative k-algebra. Then, the set $Hom_{k-Alg}(R, k)$ is non-empty.*

Proof. Let $\mathbf{m} \subseteq R$ be a maximal ideal. Then, the field $K = R/\mathbf{m}$ is finitely generated as a k-algebra and hence Corollary A.22(ii) implies that K is an algebraic extension of k. Being algebraically closed, k has no proper algebraic extensions; therefore, $K = k$. It follows that the quotient map $R \longrightarrow R/\mathbf{m}$ is a homomorphism of the type we are looking for. □

II. Finitely generated algebras over UFD's. We now turn our attention to finitely generated commutative algebras B over a unique factorization domain A. Our goal is to examine the prime elements of A that are invertible in B.

In general, if A is an integral domain and $a \in A$ a non-zero element, we denote by $A[a^{-1}]$ the A-subalgebra of the field of fractions of A generated by a^{-1}. If M is an A-module then $M[a^{-1}]$ denotes the $A[a^{-1}]$-module $M \otimes_A A[a^{-1}]$.

We begin with a generalization of Noether's normalization lemma.

Lemma A.24 *Let A be an integral domain and B a finitely generated commutative A-algebra, which is torsion-free as an A-module. Then, there is a non-zero element $a \in A$ and an $A[a^{-1}]$-subalgebra $B_0 \subseteq B[a^{-1}]$, such that:*

(i) B_0 is a polynomial $A[a^{-1}]$-algebra and

(ii) $B[a^{-1}]$ is integral over B_0.

Proof. Let $B = A[x_1, \ldots, x_n]$ for suitable elements $x_1, \ldots, x_n \in B$ and consider the field of fractions K of A. Since B is torsion-free as an A-module, it can be regarded as a subring of the finitely generated commutative K-algebra $R = K \otimes_A B = K[x_1, \ldots, x_n]$. In view of Noether's normalization lemma, there is a polynomial K-subalgebra $R_0 = K[Y_1, \ldots, Y_m] \subseteq R$, such that R is integral over it. Replacing, if necessary, Y_i by $s_i Y_i$, for a suitable $s_i \in A \setminus \{0\}$, we may assume that $Y_i \in B$ for all $i = 1, \ldots, m$. Then, for any A-subalgebra $T \subseteq K$ the T-subalgebra $T[Y_1, \ldots, Y_m] \subseteq R_0$ is contained in $T \otimes_A B \subseteq R$.

Since $x_i \in R$ is integral over R_0, there is a monic polynomial $f_i(X) \in R_0[X]$, such that $f_i(x_i) = 0$ for all $i = 1, \ldots, n$. The polynomial $f_i(X)$ involves finitely many elements of $R_0 = K[Y_1, \ldots, Y_m]$, whereas each one of these involves finitely many elements of K. It follows that there is a non-zero element $a_i \in A$, such that $f_i(X)$ is a polynomial in X with coefficients in $A[a_i^{-1}, Y_1, \ldots, Y_m] \subseteq R_0$; hence, x_i is integral over $A[a_i^{-1}, Y_1, \ldots, Y_m]$. Letting $a = \prod_{i=1}^n a_i \in A$, we conclude that all of the x_i's are integral over $B_0 = A[a^{-1}, Y_1, \ldots, Y_m]$. Since the integral closure of B_0 in R is a B_0-subalgebra and hence an $A[a^{-1}]$-subalgebra of R (cf. Corollary A.13(i)), it follows that $A[a^{-1}, x_1, \ldots, x_n]$ is integral over B_0. This finishes the proof, since $A[a^{-1}, x_1, \ldots, x_n] = A[a^{-1}] \otimes_A B = B[a^{-1}]$. □

Proposition A.25 *Let A be a unique factorization domain and B a finitely generated commutative A-algebra, containing A as a subring. Then, up to associates, there are only finitely many prime elements $p \in A$ that are invertible in B.*

Proof. The torsion submodule B_t of the A-module B is easily seen to be an ideal of B. Since A is a subring of B, the unit element $1 \in B$ is not contained in B_t. Therefore, B_t is a proper ideal of B and hence the quotient $\overline{B} = B/B_t$ is a *non-zero* A-algebra. Since a prime element $p \in A$ that is invertible in B is also invertible in $\overline{B}$, we may replace B by its quotient $\overline{B}$ and reduce to the case where the finitely generated commutative A-algebra B is torsion-free as an A-module.

Let K be the field of fractions of A. Being torsion-free as an A-module, B can be regarded as a subring of the finitely generated commutative K-algebra $R = K \otimes_A B$. In view of Lemma A.24, there is a non-zero element $a \in A$ and a polynomial $A[a^{-1}]$-subalgebra $B_0 \subseteq B[a^{-1}]$, such that $B[a^{-1}]$ is integral over it. Let $R_0 = K \otimes_{A[a^{-1}]} B_0 \subseteq R$. Being a localization of A, the subring $A[a^{-1}] \subseteq K$ is also a unique factorization domain (cf. Exercise A.5.2). Invoking Gauss' lemma, we conclude that the same is true for the polynomial $A[a^{-1}]$-algebra B_0. Then, Lemma A.15 shows that B_0 is integrally closed in its field of fractions and, a fortiori, in R_0. We now consider the commutative diagram

$$\begin{array}{ccccccc} K & \longrightarrow & R_0 & \longrightarrow & R & & \\ \uparrow & & \uparrow & & \uparrow & & \\ A[a^{-1}] & \longrightarrow & B_0 & \longrightarrow & B[a^{-1}] & \longleftarrow & B \end{array}$$

where all arrows are inclusions. Since any element of $B[a^{-1}]$ is integral over B_0, which is itself integrally closed in R_0, we conclude that the intersection $B[a^{-1}] \cap R_0$ is equal to B_0. Therefore, it follows that

$$B \cap K \subseteq B[a^{-1}] \cap K = B[a^{-1}] \cap R_0 \cap K = B_0 \cap K = A[a^{-1}] ,$$

where the last equality is a consequence of the fact that B_0 is a polynomial $A[a^{-1}]$-algebra. Hence, if a prime element $p \in A$ is invertible in B then $p^{-1} \in B \cap K \subseteq A[a^{-1}]$. It is easily seen that this can happen only if the prime p divides a. The proof is finished, since, up to associates, there are only finitely many such primes. □

Corollary A.26 *Let A be a unique factorization domain and B a finitely generated commutative A-algebra. Consider an element $x \in B$ and assume that no power x^n, $n \geq 1$, is torsion as an element of the A-module B. Then, up to associates, there are only finitely many prime elements $p \in A$ for which $x \in pB$.*

Proof. Consider the localization $B' = B[S^{-1}]$ of B at the multiplicatively closed subset S consisting of the powers of x. Then, $B' = B[Y]/(xY - 1)$ is a finitely generated commutative A-algebra, which, in view of the assumption made on x, contains A as a subring. Hence, Proposition A.25 implies that, up to associates, the set of prime elements $p \in A$ that are invertible in B' is finite. This finishes the proof, since any prime element $p \in A$ for which $x \in pB$ is necessarily invertible in B'. Indeed, if $x = pb$ for some $b \in B$, then $p^{-1} = b/x \in B'$. □

In particular, letting $A = \mathbf{Z}$, we obtain the following corollary.

Corollary A.27 *Let k be a finitely generated commutative ring of characteristic 0. Then, there are only finitely many prime numbers that are invertible in k. If, in addition, k is an integral domain, then for any $x \in k \setminus \{0\}$ there are only finitely many prime numbers $p \in \mathbf{Z}$ for which $x \in pk$.* □

A.4 The Krull Intersection Theorem

I. The ascending chain condition. We begin by developing a few basic properties of Noetherian rings and modules.

Proposition A.28 *Let R be a commutative ring. Then, the following conditions are equivalent for an R-module M:*

(i) Any submodule $N \subseteq M$ is finitely generated.

(ii) Any ascending chain of submodules of M has a maximum element.

If these conditions hold, then M is said to be a Noetherian module.

Proof. (i)→(ii): Let $(N_i)_i$ be an ascending chain of submodules of M and consider the union $N = \bigcup_i N_i$. By assumption, there are elements $x_1, \dots, x_n$ that generate the R-module N. Since there are only finitely many of them, all of the x_i's are contained in N_{i_0} for some index i_0. Therefore, $N = \sum_{i=1}^n Rx_i \subseteq N_{i_0}$ and hence $N = N_{i_0}$ is the maximum element of the given chain of submodules.

(ii)→(i): If a submodule $N \subseteq M$ is not finitely generated, then we may use an inductive argument in order to construct a sequence of elements $(x_i)_i$ of N, such that the sequence of submodules $(N_i)_i$, where $N_i = \sum_{t=1}^i Rx_t$ for all $i \geq 0$, is strictly increasing. But the existence of such a sequence contradicts condition (ii). □

In particular, a commutative ring R if said to be Noetherian if the regular module R is Noetherian.

Lemma A.29 *Let R be a commutative ring.*

(i) Any submodule and any quotient module of a Noetherian module is Noetherian.

(ii) If $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ is a short exact sequence of R-modules and M', M'' are Noetherian, then M is Noetherian as well.

(iii) If R is a Noetherian ring then any finitely generated R-module is Noetherian.

Proof. (i) If N is a submodule (resp. a quotient module) of a Noetherian module M then any submodule of N, being also a submodule (resp. a quotient module of a submodule) of M, is finitely generated.

(ii) This follows since any submodule of M, being an extension of a submodule of M'' by a submodule of M', is finitely generated.

(iii) By an iterated application of (ii), it follows that any finitely generated free R-module is Noetherian. Since any finitely generated R-module is a quotient of such a free module, the result follows from (i). □

Lemma A.30 *Let R be a commutative ring.*

(i) If R is a principal ideal domain, then R is Noetherian.

(ii) If R is a quotient of a commutative Noetherian ring, then R is Noetherian as well.

Proof. (i) This is immediate, since any ideal of R is principal (and hence finitely generated).

(ii) If R is a quotient of a commutative ring T, then any ideal I of R is a quotient of an ideal J of T. If T is Noetherian, then J is finitely generated as a T-module and hence I is finitely generated as an R-module. □

In order to obtain non-trivial examples of Noetherian rings, we need the following result of Hilbert.

Theorem A.31 *(Hilbert basis theorem) If R is a commutative Noetherian ring, then so is the polynomial ring $R[X]$.*

Proof. Let I be an ideal of $R[X]$ and consider the increasing sequence of ideals $(J_n)_n$ of R, where $J_n \subseteq R$ consists of the leading coefficients of all polynomials in I that have degree $\leq n$. We also consider the ideal $J_\infty = \bigcup_n J_n$. Since R is Noetherian, the ideal J_n is finitely generated for all $n \in \mathbf{N} \cup \{\infty\}$. Hence, for all n there is a finite set of polynomials $F_n \subseteq I$, having degree $\leq n$, whose leading coefficients generate J_n.

We claim that if $n_0 = \max\{\deg g : g \in F_\infty\}$, then I is generated by the (finite) set $F = F_0 \cup F_1 \cup \cdots \cup F_{n_0-1} \cup F_\infty$. Indeed, let us consider a non-zero polynomial $f \in I$ and show that $f \in \sum_{g \in F} R[X]g$, by using induction on $n = \deg f$. Assume that elements of I having degree $< n$ are contained in $\sum_{g \in F} R[X]g$ and suppose that $n < n_0$. Then, the leading coefficient of f is an R-linear combination of the leading coefficients of the polynomials in F_n and hence the polynomial $f - \sum_{g \in F_n} r_g X^{n-\deg g} g \in I$ has degree $< n$, for suitable elements $r_g \in R$, $g \in F_n$. In view of the induction hypothesis, we conclude that $f - \sum_{g \in F_n} r_g X^{n-\deg g} g \in \sum_{g \in F} R[X]g$; since $F_n \subseteq F$, it follows that $f \in \sum_{g \in F} R[X]g$. Now suppose that $n \geq n_0$. Since the leading coefficient of f is an R-linear combination of the leading coefficients of the polynomials in F_∞, the polynomial $f - \sum_{g \in F_\infty} r_g X^{n-\deg g} g \in I$ has degree $< n$, for suitable elements $r_g \in R$, $g \in F_\infty$. In view of the induction hypothesis, we conclude that $f - \sum_{g \in F_\infty} r_g X^{n-\deg g} g \in \sum_{g \in F} R[X]g$; since $F_\infty \subseteq F$, it follows that $f \in \sum_{g \in F} R[X]g$ in this case as well. □

Corollary A.32 *Any finitely generated commutative ring is Noetherian.*

Proof. Being a principal ideal domain, the ring $\mathbf{Z}$ is Noetherian (Lemma A.30(i)). Therefore, an iterated application of the Hilbert basis theorem shows that the polynomial ring $\mathbf{Z}[X_1, \ldots, X_n]$ is Noetherian for all n. Since any finitely generated commutative ring is a quotient of such a polynomial ring, the result follows from Lemma A.30(ii). □

II. THE INTERSECTION OF THE POWERS OF AN IDEAL. We now study the intersection of the powers of an ideal in a commutative Noetherian ring.

Proposition A.33 *Let R be a commutative ring, $I \subseteq R$ an ideal and M a Noetherian R-module.*

(i) Assume that N, L are two submodules of M, such that N is maximal with respect to the property $N \cap L = IL$. Then, for any $r \in I$ there exists $n \in \mathbf{N}$, such that $r^n M \subseteq N$. In particular, if I is finitely generated, then $I^t M \subseteq N$ for $t \gg 0$.

(ii) Assume that the ideal I is finitely generated and consider a submodule L of M, such that $L \subseteq \bigcap_n I^n M$. Then, $IL = L$.

Proof. (i) We fix an element $r \in I$ and consider for any non-negative integer i the submodule $M_i \subseteq M$ consisting of those elements $x \in M$ for which $r^i x \in N$. Since the R-module M is Noetherian, the increasing sequence $(M_i)_i$ of submodules of M must be eventually constant; hence, there exists an integer $n \in \mathbf{N}$ such that $M_n = M_{n+1}$. We claim that

$$(r^n M + N) \cap L = N \cap L \, . \tag{A.3}$$

Of course, the $\supseteq$-inclusion is clear. Conversely, let $z \in (r^n M + N) \cap L$. Then, there are elements $x \in M$ and $y \in N$, such that $z = r^n x + y \in L$. Since $rz \in IL = N \cap L \subseteq N$, we have $r^{n+1}x = rz - ry \in N$ and hence $x \in M_{n+1} = M_n$. Therefore, $r^n x \in N$ and hence $z = r^n x + y \in N$, i.e. $z \in N \cap L$. Having established (A.3), the maximality of N implies that $r^n M + N = N$ and hence $r^n M \subseteq N$.

If the ideal I is generated by elements $r_1, \ldots, r_k$ and $n_1, \ldots, n_k$ are positive integers, then $I^t \subseteq \sum_{i=1}^k r_i^{n_i} R$, where $t = 1 + \sum_{i=1}^k (n_i - 1)$. Indeed, it is easily seen that any summand in the expansion of a typical product

$$\prod_{l=1}^t \sum_{i=1}^k r_i s_i^{(l)} = \left(\sum_{i=1}^k r_i s_i^{(1)}\right) \cdot \left(\sum_{i=1}^k r_i s_i^{(2)}\right) \cdots \left(\sum_{i=1}^k r_i s_i^{(t)}\right) ,$$

where all $s_i^{(l)}$'s are elements of R, is divisible by $r_i^{n_i}$ for at least one i. In particular, it follows that $I^t M \subseteq \sum_{i=1}^k r_i^{n_i} M$. Having chosen the n_i's in such a way that $r_i^{n_i} M \subseteq N$ for all i, it follows that $I^t M \subseteq N$.

(ii) Consider the class consisting of those submodules $N \subseteq M$ that satisfy the condition $N \cap L = IL$. This class is non-empty, since it contains IL. Applying Zorn's lemma, we may choose a submodule $N \subseteq M$ maximal in that class. By part (i), we have $I^t M \subseteq N$ for some $t \gg 0$ and hence $L \subseteq \bigcap_n I^n M \subseteq I^t M \subseteq N$; therefore, $L = N \cap L = IL$. □

Theorem A.34 *(Krull intersection theorem) Let $I \subseteq R$ be a proper ideal of a commutative Noetherian ring R and consider a finitely generated R-module M. Then, the submodule $L = \bigcap_n I^n M$ is trivial (i.e. $L = 0$) if either one of the following two conditions is satisfied:*

(i) R is a local ring or

(ii) R is an integral domain and M a torsion-free R-module.

Proof. Since R is a Noetherian ring, the ideal I is finitely generated, whereas Lemma A.29(iii) shows that the R-module M is Noetherian. Therefore, Proposition A.33(ii) implies that $IL = L$. Since M is Noetherian, L is finitely generated; hence, the proof is finished by invoking Lemma A.9. □

Corollary A.35 *Let k be a finitely generated integral domain and $I \subseteq k$ a proper ideal. Then, $\bigcap_n I^n = 0$.*

Proof. This follows from Theorem A.34, in view of Corollary A.32. □

A.5 Exercises

1. Let T be a commutative ring, which is integral over a subring $R \subseteq T$. Then, show that $U(R) = R \cap U(T)$.

2. Let R be a unique factorization domain and $S \subseteq R$ a multiplicatively closed subset containing 1. Show that the localization $R[S^{-1}]$ is a unique factorization domain as well.
3. Let k be a field and R a finitely generated commutative k-algebra.
   (i) Give an example showing that the set $\mathrm{Hom}_{k-Alg}(R, k)$ may be empty if k is not algebraically closed.
   (ii) If $\overline{k}$ is the algebraic closure of k, show that $\mathrm{Hom}_{k-Alg}\big(R, \overline{k}\big) \neq \emptyset$.
4. Show that the conclusion of Proposition A.25 may be false if either
   (i) the commutative A-algebra B is not finitely generated or
   (ii) the structural homomorphism $A \longrightarrow B$ is not injective.

B

Discrete Ring-Valued Integrals

Let X be a compact space and $C(X)$ the associated algebra of continuous complex-valued functions, endowed with the supremum norm. A regular Borel measure μ on X induces a continuous linear functional $\mathcal{I}_\mu$ on $C(X)$, namely the functional $f \mapsto \int f \, d\mu$, $f \in C(X)$. Moreover, the Riesz representation theorem (cf. [61, Theorem 6.19]) asserts that any continuous linear functional on $C(X)$ arises from a unique regular Borel measure μ in this way.

In this Appendix, we consider a discrete version of the above process and consider measures (more precisely, premeasures) which have values in an abelian group A. Since A will have, in general, no topological structure, we suitably restrict the class of functions that can be integrated. In fact, we consider only the locally constant integer-valued functions on X; these are precisely the continuous functions from X to the discrete space $\mathbf{Z}$. It will turn out that the algebra (in the measure-theoretic sense) of subsets of X on which the measure has to be defined is that consisting of the clopen subsets of X. The special case where $A = R$ is a commutative ring and the measure of any clopen subset of X is an idempotent therein is of particular importance for the applications we have in mind.

B.1 Discrete Group-Valued Integrals

Let us fix a compact topological space X and consider the set $L(X)$ consisting of the clopen subsets $Y \subseteq X$. We note that $L(X)$ is a subalgebra of the Boolean algebra $\mathcal{P}(X)$ of all subsets of X (cf. Examples 1.3(ii),(iii)). Since X is compact, any continuous function f on X with values in $\mathbf{Z}$ takes only finitely many values, say $a_1, \ldots, a_n$. We assume that the a_i's are distinct and note that the inverse image of the singleton $\{a_i\} \subseteq \mathbf{Z}$ under f is a clopen subset X_i of X for all $i = 1, \ldots, n$. Then, $f = \sum_{i=1}^n a_i \chi_{X_i}$; we refer to that equation as the canonical decomposition of f. It is clear that a decomposition $f = \sum_{j=1}^m b_j \chi_{Y_j}$, where $b_j \in \mathbf{Z}$ and $Y_j \in L(X)$ for all $j = 1, \ldots, m$, coincides with the canonical one if the following two conditions are satisfied:

(i) The integers $b_1, \ldots, b_m$ are distinct and

(ii) The clopen subsets $Y_1, \ldots, Y_m$ of X are non-empty, mutually disjoint and cover X.

The set of all locally constant integer-valued functions on X is a commutative ring with operations defined pointwise; we denote this ring by $[X, \mathbf{Z}]$. We note that the map $Y \mapsto \chi_Y$, $Y \in L(X)$, is an isomorphism of Boolean algebras

$$\chi : L(X) \longrightarrow \mathrm{Idem}([X, \mathbf{Z}]) \ . \tag{B.1}$$

Indeed, $\chi_\emptyset$ and χ_X are the constant functions with value 0 and 1 respectively, whereas for any two clopen subsets $Y, Y' \subseteq X$ we have

$$\chi_{Y \cap Y'} = \chi_Y \chi_{Y'} = \chi_Y \wedge \chi_{Y'}$$

and

$$\chi_{Y \cup Y'} = \chi_Y + \chi_{Y'} - \chi_{Y \cap Y'} = \chi_Y + \chi_{Y'} - \chi_Y \chi_{Y'} = \chi_Y \vee \chi_{Y'} \ .$$

We now let $\mathcal{L}$ be a Boolean algebra of subsets of a set Ω and A an abelian group. An A-valued premeasure μ on $\mathcal{L}$ is a function $\mu : \mathcal{L} \longrightarrow A$ satisfying the following two conditions:

(μ1) $\mu(\emptyset) = 0$ and

(μ2) if $Y_1, \ldots, Y_n \in \mathcal{L}$ are disjoint, then $\mu(\bigcup_{i=1}^n Y_i) = \sum_{i=1}^n \mu(Y_i)$.

Given an A-valued premeasure μ on the Boolean algebra $L(X)$ of clopen subsets of X, we may define for any function $f \in [X, \mathbf{Z}]$ with canonical decomposition $f = \sum_{i=1}^n a_i \chi_{X_i}$ the element $\mathcal{I}_\mu(f) = \sum_{i=1}^n a_i \mu(X_i) \in A$.

Definition B.1 *The element $\mathcal{I}_\mu(f) \in A$ defined above is called the discrete A-valued integral of f with respect to the premeasure μ.*

Lemma B.2 *Let X be a compact space, A an abelian group and μ an A-valued premeasure on $L(X)$.*

(i) If $a_1, \ldots, a_n$ are integers, $X_1, \ldots, X_n$ mutually disjoint clopen subsets covering X and $f = \sum_{i=1}^n a_i \chi_{X_i}$, then $\mathcal{I}_\mu(f) = \sum_{i=1}^n a_i \mu(X_i)$.

(ii) $\mathcal{I}_\mu(f+g) = \mathcal{I}_\mu(f) + \mathcal{I}_\mu(g)$ for all $f, g \in [X, \mathbf{Z}]$.

Proof. (i) Let $f = \sum_{j=1}^m b_j \chi_{Y_j}$ be the canonical decomposition of f; then, the Y_j's are mutually disjoint and cover X. It follows that X_i is the disjoint union of the family $(X_i \cap Y_j)_j$ for all $i = 1, \ldots, n$ and hence

$$f = \sum\nolimits_i a_i \chi_{X_i} = \sum\nolimits_i a_i \Big(\sum\nolimits_j \chi_{X_i \cap Y_j} \Big) = \sum\nolimits_{i,j} a_i \chi_{X_i \cap Y_j} \ . \tag{B.2}$$

Similarly, the X_i's being mutually disjoint and covering X, Y_j is the disjoint union of the family $(X_i \cap Y_j)_i$ for all $j = 1, \ldots, m$; hence,

$$f = \sum\nolimits_j b_j \chi_{Y_j} = \sum\nolimits_j b_j \Big(\sum\nolimits_i \chi_{X_i \cap Y_j} \Big) = \sum\nolimits_{i,j} b_j \chi_{X_i \cap Y_j} \ . \tag{B.3}$$

Since the family $(X_i \cap Y_j)_{i,j}$ consists of mutually disjoint sets, we may compare the decompositions of f in (B.2) and (B.3) in order to conclude that whenever $X_i \cap Y_j \neq \emptyset$ we have $a_i = b_j$. Since $\mu(\emptyset) = 0$, it follows that $a_i \mu(X_i \cap Y_j) = b_j \mu(X_i \cap Y_j)$ for all i, j. Therefore, using the additivity of μ (property (μ2)), we have

$$\begin{aligned}
\mathcal{I}_\mu(f) &= \sum\nolimits_j b_j \mu(Y_j) \\
&= \sum\nolimits_j b_j \Big(\sum\nolimits_i \mu(X_i \cap Y_j) \Big) \\
&= \sum\nolimits_{i,j} b_j \mu(X_i \cap Y_j) \\
&= \sum\nolimits_{i,j} a_i \mu(X_i \cap Y_j) \\
&= \sum\nolimits_i a_i \Big(\sum\nolimits_j \mu(X_i \cap Y_j) \Big) \\
&= \sum\nolimits_i a_i \mu(X_i) \, .
\end{aligned}$$

(ii) Let $f = \sum_{i=1}^n a_i \chi_{X_i}$ and $g = \sum_{j=1}^m b_j \chi_{Y_j}$ be the canonical decompositions of f and g respectively; then, $f + g = \sum_{i,j} (a_i + b_j) \chi_{X_i \cap Y_j}$. Since the family $(X_i \cap Y_j)_{i,j}$ consists of disjoint clopen subsets covering X, we may invoke (i) above and the additivity of μ in order to conclude that

$$\begin{aligned}
\mathcal{I}_\mu(f+g) &= \sum\nolimits_{i,j} (a_i + b_j) \mu(X_i \cap Y_j) \\
&= \sum\nolimits_{i,j} a_i \mu(X_i \cap Y_j) + \sum\nolimits_{i,j} b_j \mu(X_i \cap Y_j) \\
&= \sum\nolimits_i a_i \Big(\sum\nolimits_j \mu(X_i \cap Y_j) \Big) + \sum\nolimits_j b_j \Big(\sum\nolimits_i \mu(X_i \cap Y_j) \Big) \\
&= \sum\nolimits_i a_i \mu(X_i) + \sum\nolimits_j b_j \mu(Y_j) \\
&= \mathcal{I}_\mu(f) + \mathcal{I}_\mu(g) \, ,
\end{aligned}$$

as needed. □

With the notation established above, we can state the following discrete version of the Riesz representation theorem.

Proposition B.3 *Let X be a compact space and A an abelian group.*

(i) For any A-valued premeasure μ on $L(X)$ the associated discrete A-valued integral $\mathcal{I}_\mu : [X, \mathbf{Z}] \longrightarrow A$ is a homomorphism of abelian groups.

(ii) Conversely, for any group homomorphism $\varphi : [X, \mathbf{Z}] \longrightarrow A$ there is a unique A-valued premeasure μ on $L(X)$, such that $\varphi = \mathcal{I}_\mu$.

Proof. (i) This is precisely Lemma B.2(ii).

(ii) Given a homomorphism $\varphi : [X, \mathbf{Z}] \longrightarrow A$, define an A-valued map μ on $L(X)$ by letting $\mu(Y) = \varphi(\chi_Y)$ for all $Y \in L(X)$. Since $\chi_\emptyset$ is the constant function with value 0, it follows that $\mu(\emptyset) = 0$. If $Y_1, \ldots, Y_n$ are disjoint clopen subsets of X and $Y = \bigcup_{i=1}^n Y_i$, then $\chi_Y = \sum_{i=1}^n \chi_{Y_i}$; therefore,

$$\mu(Y) = \varphi(\chi_Y) = \sum\nolimits_{i=1}^n \varphi(\chi_{Y_i}) = \sum\nolimits_{i=1}^n \mu(Y_i)$$

and μ is indeed a premeasure. By the very definition of μ, it follows that the group homomorphisms $\mathcal{I}_\mu$ and φ coincide on the set $\{\chi_Y : Y \in L(X)\}$. Since this set generates the group $[X, \mathbf{Z}]$, we conclude that $\mathcal{I}_\mu = \varphi$. The uniqueness of μ satisfying that condition is clear. $\square$

For a topological space X and an abelian group A, we denote the set of A-valued premeasures on $L(X)$ by $\mathcal{M}(L(X); A)$. We note that $\mathcal{M}(L(X); A)$ has the structure of an abelian group, where the sum $\mu + \mu'$ of two premeasures $\mu, \mu' \in \mathcal{M}(L(X); A)$ is defined by letting $(\mu + \mu')(Y) = \mu(Y) + \mu'(Y)$ for all $Y \in L(X)$.

Corollary B.4 *Let X be a compact space and A an abelian group. Then, the map $\mu \mapsto \mathcal{I}_\mu$, $\mu \in \mathcal{M}(L(X); A)$, is an isomorphism of groups*

$$\mathcal{I} : \mathcal{M}(L(X); A) \longrightarrow Hom([X, \mathbf{Z}], A) .$$

Proof. In view of Proposition B.3, it only remains to show that $\mathcal{I}_{\mu+\mu'} = \mathcal{I}_\mu + \mathcal{I}_{\mu'}$ for all $\mu, \mu' \in \mathcal{M}(L(X); A)$. For any $Y \in L(X)$ we have

$$\mathcal{I}_{\mu+\mu'}(\chi_Y) = (\mu + \mu')(Y) = \mu(Y) + \mu'(Y) = \mathcal{I}_\mu(\chi_Y) + \mathcal{I}_{\mu'}(\chi_Y) .$$

Since the group $[X, \mathbf{Z}]$ is generated by the characteristic functions of clopen subsets $Y \in L(X)$, it follows that the homomorphisms $\mathcal{I}_{\mu+\mu'}$ and $\mathcal{I}_\mu + \mathcal{I}_{\mu'}$ are equal. $\square$

B.2 Idempotent-Valued Premeasures

In this section, we examine the special properties that are enjoyed by the integrals considered above, in the case where the abelian group A is endowed with the structure of a commutative ring.

Let $\mathcal{L}$ be a Boolean algebra of subsets of a set Ω, R a commutative ring and $\nu : \mathcal{L} \longrightarrow \text{Idem}(R)$ a morphism of Boolean algebras. Then, ν associates with any $Y \in \mathcal{L}$ an idempotent $\nu(Y) \in R$, in such a way that the following properties are satisfied:

(ν1) $\nu(\emptyset) = 0$ and $\nu(\Omega) = 1$,
(ν2) $\nu(Y \cup Y') = \nu(Y) + \nu(Y') - \nu(Y)\nu(Y')$ for all $Y, Y' \in \mathcal{L}$ and
(ν3) $\nu(Y \cap Y') = \nu(Y)\nu(Y')$ for all $Y, Y' \in \mathcal{L}$.

Lemma B.5 *Let $\mathcal{L}$ be a Boolean algebra of subsets of a set Ω and consider a commutative ring R.*

(i) If $\nu : \mathcal{L} \longrightarrow Idem(R)$ is a Boolean algebra morphism then ν is a premeasure on $\mathcal{L}$, such that $\nu(\Omega) = 1$.

(ii) Conversely, assume that ν is a premeasure on $\mathcal{L}$ with values in the set of idempotents of R, such that $\nu(\Omega) = 1$. If $2 \in R$ is not a zero-divisor then $\nu : \mathcal{L} \longrightarrow Idem(R)$ is a Boolean algebra morphism.

Proof. (i) It suffices to verify that ν satisfies property (μ2). To that end, let us consider two disjoint subsets $Y, Y' \in \mathcal{L}$. Since ν is $\wedge$-preserving (property (ν3)) and $\nu(\emptyset) = 0$, we have $\nu(Y)\nu(Y') = \nu(Y \cap Y') = 0$. But ν is $\vee$-preserving as well (property (ν2)) and hence $\nu(Y \cup Y') = \nu(Y) + \nu(Y') - \nu(Y)\nu(Y') = \nu(Y) + \nu(Y')$. Using induction on n, one can prove that whenever $Y_1, \ldots, Y_n \in \mathcal{L}$ are mutually disjoint and $Y = \bigcup_{i=1}^n Y_i$, then $\nu(Y) = \sum_{i=1}^n \nu(Y_i)$.

(ii) By assumption, ν satisfies property (ν1). Since property (ν2) is a consequence of properties (μ2) and (ν3),[1] it suffices to prove that ν satisfies property (ν3). To that end, we note that whenever $Y_1, Y_2 \in \mathcal{L}$ are disjoint, the idempotents $e_1 = \nu(Y_1)$ and $e_2 = \nu(Y_2)$ are orthogonal. Indeed, in that case, $e_1 + e_2 = \nu(Y_1) + \nu(Y_2) = \nu(Y_1 \cup Y_2)$ is an idempotent and hence

$$e_1 + e_2 = (e_1 + e_2)^2 = e_1^2 + e_2^2 + 2e_1e_2 = e_1 + e_2 + 2e_1e_2 \ .$$

Therefore, $2e_1e_2 = 0$ and hence $e_1e_2 = 0$. Now let $Y, Y' \in \mathcal{L}$ and $e = \nu(Y \cap Y')$. Then, $Y \setminus Y' \in \mathcal{L}$ is disjoint from $Y \cap Y'$ and $\nu(Y \setminus Y') = \nu(Y) - e$ (in view of property (μ2)). Therefore, $e(\nu(Y) - e) = 0$ and hence $e = e^2 = e\nu(Y)$. Similarly, one can show that $e = e\nu(Y')$. Finally, since the subsets $Y \setminus Y'$ and $Y' \setminus Y$ are disjoint, we have

$$\begin{aligned} 0 &= \nu(Y \setminus Y')\nu(Y' \setminus Y) \\ &= (\nu(Y) - e)(\nu(Y') - e) \\ &= \nu(Y)\nu(Y') - e\nu(Y) - e\nu(Y') + e^2 \\ &= \nu(Y)\nu(Y') - e - e + e \\ &= \nu(Y)\nu(Y') - e \end{aligned}$$

and hence $\nu(Y \cap Y') = e = \nu(Y)\nu(Y')$. □

We now consider a compact topological space X, a commutative ring R and study the discrete R-valued integral $\mathcal{I}_\nu$, associated with a Boolean algebra morphism ν defined on the algebra $\mathcal{L} = L(X)$ of clopen subsets of X with values in Idem(R).

Lemma B.6 *Let X be a compact space, R a commutative ring and consider a Boolean algebra morphism $\nu : L(X) \longrightarrow Idem(R)$. Then:*

(i) $\mathcal{I}_\nu(fg) = \mathcal{I}_\nu(f)\mathcal{I}_\nu(g)$ for all $f, g \in [X, \mathbf{Z}]$.

(ii) If $\mathbf{1}$ is the constant function on X with value $1 \in \mathbf{Z}$, then $\mathcal{I}_\nu(\mathbf{1}) = 1$.

Proof. (i) Let $f = \sum_{i=1}^n a_i \chi_{X_i}$ and $g = \sum_{j=1}^m b_j \chi_{Y_j}$ be the canonical decompositions of f and g respectively; then, $fg = \sum_{i,j} a_i b_j \chi_{X_i \cap Y_j}$. Using the additivity of $\mathcal{I}_\nu$ and property (ν3), we conclude that

$$\begin{aligned} \mathcal{I}_\nu(fg) &= \sum_{i,j} a_i b_j \nu(X_i \cap Y_j) \\ &= \sum_{i,j} a_i b_j \nu(X_i)\nu(Y_j) \\ &= \left(\sum_i a_i \nu(X_i)\right)\left(\sum_j b_j \nu(Y_j)\right) \\ &= \mathcal{I}_\nu(f)\mathcal{I}_\nu(g) \ . \end{aligned}$$

(ii) This is clear, since $\mathbf{1} = \chi_X$ and $\nu(X) = 1$. □

[1] Indeed, property (μ2) for ν is easily seen to imply that $\nu(Y \cup Y') = \nu(Y) + \nu(Y') - \nu(Y \cap Y')$ for all $Y, Y' \in \mathcal{L}$.

Proposition B.7 *Let X be a compact space and R a commutative ring.*

(i) For any Boolean algebra morphism $\nu : L(X) \longrightarrow Idem(R)$ the associated discrete R-valued integral $\mathcal{I}_\nu : [X, \mathbf{Z}] \longrightarrow R$ is a ring homomorphism.

(ii) Conversely, for any ring homomorphism $\varphi : [X, \mathbf{Z}] \longrightarrow R$ there is a unique Boolean algebra morphism $\nu : L(X) \longrightarrow Idem(R)$, such that $\varphi = \mathcal{I}_\nu$.

Proof. (i) This follows from Lemmas B.2(ii) and B.6.

(ii) Given a ring homomorphism $\varphi : [X, \mathbf{Z}] \longrightarrow R$, we may consider the premeasure $\nu : L(X) \longrightarrow R$ defined in the proof of Proposition B.3; recall that $\nu(Y) = \varphi(\chi_Y)$ for any $Y \in L(X)$. Then, ν is the unique premeasure satisfying $\mathcal{I}_\nu = \varphi$; we have to show that ν takes values in the set $\text{Idem}(R)$ and is a Boolean algebra morphism with values therein. Since χ_Y is an idempotent in the function ring $[X, \mathbf{Z}]$ and φ is multiplicative, it is clear that $\nu(Y) \in \text{Idem}(R)$ for all $Y \in L(X)$. But then ν is the composition

$$L(X) \xrightarrow{\chi} \text{Idem}([X, \mathbf{Z}]) \xrightarrow{Idem(\varphi)} \text{Idem}(R) ,$$

where χ is the isomorphism (B.1) and $\text{Idem}(\varphi)$ the morphism of Boolean algebras induced by φ. In particular, it follows that ν is a morphism of Boolean algebras, as needed. □

Remarks B.8 (i) Let X be a compact space and R a commutative ring. Then, we can reformulate Proposition B.7 as the assertion that the map

$$\mathcal{I} : \text{Hom}_{Boole}(L(X), \text{Idem}(R)) \longrightarrow \text{Hom}_{Ring}([X, \mathbf{Z}], R) ,$$

which is given by $\nu \mapsto \mathcal{I}_\nu$, $\nu \in \text{Hom}_{Boole}(L(X), \text{Idem}(R))$, is bijective.

(ii) The discussion about discrete ring-valued integrals in this Appendix was motivated by the various constructions associated with the geometric rank in §2.1. Having that special case in mind, we chose to consider only locally constant integer-valued functions. In fact, we could have replaced the ring $\mathbf{Z}$ by an arbitrary commutative ring k and insisted that the abelian group A (resp. the commutative ring R) be a k-module (resp. a commutative k-algebra). In exactly the same way as above, one can define for any A-valued premeasure (resp. for any $\text{Idem}(R)$-valued Boolean algebra morphism) on $L(X)$ a corresponding A-valued (resp. R-valued) integral defined on the class of locally constant k-valued functions on the compact space X and obtain identifications

$$\mathcal{M}(L(X); A) \simeq \text{Hom}_k([X, k], A)$$

and

$$\text{Hom}_{Boole}(L(X), \text{Idem}(R)) \simeq \text{Hom}_{k-Alg}([X, k], R) .$$

B.3 Exercises

1. Let X, X' be compact topological spaces and $f : X \longrightarrow X'$ a continuous map. We also consider the Boolean algebra morphism $L(f) : L(X') \longrightarrow$

$L(X)$, which is given by $Y' \mapsto f^{-1}(Y')$, $Y' \in L(X')$ (cf. Example 1.5(iii)).
(i) Let A be an abelian group and μ an A-valued premeasure on $L(X)$. Show that $\mu' = \mu \circ L(f)$ is an A-valued premeasure on $L(X')$ and

$$\mathcal{I}_{\mu'} = \mathcal{I}_{\mu} \circ [f, \mathbf{Z}] : [X', \mathbf{Z}] \longrightarrow A ,$$

where $[f, \mathbf{Z}] : [X', \mathbf{Z}] \longrightarrow [X, \mathbf{Z}]$ is the map $g \mapsto g \circ f$, $g \in [X', \mathbf{Z}]$.[2]
(ii) (naturality of $\mathcal{I}$ with respect to the topological space) Let A be an abelian group. Show that the following diagram is commutative

$$\begin{array}{ccc} \mathcal{M}(L(X); A) & \xrightarrow{\mathcal{I}} & \mathrm{Hom}([X, \mathbf{Z}], A) \\ {\scriptstyle L(f)^*} \downarrow & & \downarrow {\scriptstyle [f,\mathbf{Z}]^*} \\ \mathcal{M}(L(X'); A) & \xrightarrow{\mathcal{I}} & \mathrm{Hom}([X', \mathbf{Z}], A) \end{array}$$

where $L(f)^*$ is the map $\mu \mapsto \mu \circ L(f)$, $\mu \in \mathcal{M}(L(X); A)$, and $[f, \mathbf{Z}]^*$ the map $\varphi \mapsto \varphi \circ [f, \mathbf{Z}]$, $\varphi \in \mathrm{Hom}([X, \mathbf{Z}], A)$.
(iii) Let R be a commutative ring. Show that the following diagram is commutative

$$\begin{array}{ccc} \mathrm{Hom}_{Boole}(L(X), \mathrm{Idem}(R)) & \xrightarrow{\mathcal{I}} & \mathrm{Hom}_{Ring}([X, \mathbf{Z}], R) \\ {\scriptstyle L(f)^*} \downarrow & & \downarrow {\scriptstyle [f,\mathbf{Z}]^*} \\ \mathrm{Hom}_{Boole}(L(X'), \mathrm{Idem}(R)) & \xrightarrow{\mathcal{I}} & \mathrm{Hom}_{Ring}([X', \mathbf{Z}], R) \end{array}$$

where $L(f)^*$ and $[f, \mathbf{Z}]^*$ are the restrictions of the corresponding maps in (ii) above.

2. Let A, A' be abelian groups, $\sigma : A \longrightarrow A'$ a group homomorphism and X a compact topological space.
(i) Show that if μ is an A-valued premeasure on $L(X)$, then $\mu' = \sigma \circ \mu$ is an A'-valued premeasure on $L(X)$ and

$$\mathcal{I}_{\mu'} = \sigma \circ \mathcal{I}_{\mu} : [X, \mathbf{Z}] \longrightarrow A' .$$

(ii) (naturality of $\mathcal{I}$ with respect to the abelian group) Show that the following diagram is commutative

$$\begin{array}{ccc} \mathcal{M}(L(X); A) & \xrightarrow{\mathcal{I}} & \mathrm{Hom}([X, \mathbf{Z}], A) \\ {\scriptstyle \sigma_*} \downarrow & & \downarrow {\scriptstyle \sigma_*} \\ \mathcal{M}(L(X); A') & \xrightarrow{\mathcal{I}} & \mathrm{Hom}([X, \mathbf{Z}], A') \end{array}$$

where we denote by σ_* both maps $\mu \mapsto \sigma \circ \mu$, $\mu \in \mathcal{M}(L(X); A)$, and $\varphi \mapsto \sigma \circ \varphi$, $\varphi \in \mathrm{Hom}([X, \mathbf{Z}], A)$.

[2] If we denote the values of $\mathcal{I}_{\mu}$ and $\mathcal{I}_{\mu'}$ using the standard $\int$-sign, the equality $\mathcal{I}_{\mu'} = \mathcal{I}_{\mu} \circ [f, \mathbf{Z}]$ takes the familiar form of the *change of variables formula*: $\int_{X'} g(z)\, d\mu'(z) = \int_X g(f(t))\, d\mu(t)$ for all $g \in [X', \mathbf{Z}]$.

(iii) Let R, R' be commutative rings and $\tau : R \longrightarrow R'$ a ring homomorphism. Show that the following diagram is commutative

$$\begin{array}{ccc} \mathrm{Hom}_{Boole}(L(X), \mathrm{Idem}(R)) & \xrightarrow{\mathcal{I}} & \mathrm{Hom}_{Ring}([X, \mathbf{Z}], R) \\ {\scriptstyle Idem(\tau)_*} \downarrow & & \downarrow {\scriptstyle \tau_*} \\ \mathrm{Hom}_{Boole}(L(X), \mathrm{Idem}(R')) & \xrightarrow{\mathcal{I}} & \mathrm{Hom}_{Ring}([X, \mathbf{Z}], R') \end{array}$$

where $\mathrm{Idem}(\tau)$ is the Boolean algebra morphism induced by τ and $\mathrm{Idem}(\tau)_*$ (resp. τ_*) the map given by composing to the left with $\mathrm{Idem}(\tau)$ (resp. with τ).

3. Let $\mathcal{L}$ be a Boolean algebra of subsets of a set Ω and R a commutative ring. Prove the following strengthening of Lemma B.5:
(i) Let $\nu : \mathcal{L} \longrightarrow \mathrm{Idem}(R)$ be a function satisfying properties (ν2) and (ν3). If $\nu(\emptyset) = 0$, then ν is a premeasure.
(ii) Conversely, assume that ν is a premeasure on $\mathcal{L}$ with values in the set of idempotents of R and let $\nu(\Omega) = e \in \mathrm{Idem}(R)$. If $2 \in R$ is not a zero-divisor then $\nu(Y) \in Re$ for all $Y \in \mathcal{L}$ and ν is a Boolean algebra morphism from $\mathcal{L}$ to the algebra of idempotents $\mathrm{Idem}(Re)$ of the commutative ring Re.
4. The goal of this Exercise is to show that the regularity hypothesis about $2 \in R$ can't be omitted in Lemma B.5(ii). To that end, let Ω be a finite set and $\mathcal{L} = \mathcal{P}(\Omega)$ its power set. Consider the commutative ring $R = \mathbf{Z}/2\mathbf{Z} = \{0, 1\}$ and define an R-valued map ν on $\mathcal{L}$, by letting $\nu(Y) = 0$ (resp. 1) if the subset $Y \subseteq \Omega$ has an even (resp. odd) number of elements. Show that:
(i) ν is a premeasure on $\mathcal{L}$ with values in $\mathrm{Idem}(R)$.
(ii) If Ω has an odd number of elements then $\nu(\Omega) = 1$.
(iii) If Ω has more than one elements, then $\nu : \mathcal{L} \longrightarrow \mathrm{Idem}(R)$ is not a Boolean algebra morphism.

C

Frobenius' Density Theorem

Let $f(X) \in \mathbf{Z}[X]$ be a monic polynomial of degree n without multiple roots in $\mathbf{C}$. For any prime number p we may reduce $f(X)$ modulo p and obtain a polynomial $f_p(X) \in \mathbf{F}_p[X]$. Even if the original polynomial is irreducible in $\mathbf{Z}[X]$, it may very well happen that its reduction modulo p is reducible in $\mathbf{F}_p[X]$. Moreover, the partition of n induced by the degrees of the irreducible factors of $f_p(X)$ in $\mathbf{F}_p[X]$ may vary with p. We also consider the roots $a_1, \ldots, a_n$ of $f(X)$ in $\mathbf{C}$ and the corresponding splitting field $K = \mathbf{Q}(a_1, \ldots, a_n)$. The Galois group Γ of K over $\mathbf{Q}$ may be viewed as a subgroup of the group S_n of permutations on n letters, by restricting its action to the a_i's. Counting the lengths of the cycles in the cycle decomposition of an element $\gamma \in \Gamma \subseteq S_n$, we obtain a partition of n. In this way, we obtain partitions of n by two different methods:

(i) by factoring $f(X)$ modulo prime numbers and

(ii) by viewing elements of the Galois group Γ as permutations of the roots of $f(X)$.

It turns out that these two methods are related to each other; it is the goal of the present Appendix to describe this relationship. As a consequence, we prove that an irreducible monic polynomial $f(X) \in \mathbf{Z}[X]$ decomposes into the product of linear factors modulo p for all but finitely many prime numbers p only if $\deg f(X) = 1$. This fact played an important role in the arguments that were used in §3.1.2, in the proof of Zaleskii's theorem.

Frobenius' theorem is related to Dirichlet's theorem on primes in arithmetic progressions; for further details on these results, the reader may consult the lucid exposition [67].

C.1 The Density Theorem

Let us fix a monic polynomial $f(X) \in \mathbf{Z}[X]$ of degree n. We assume that $f(X)$ has n distinct roots $a_1, \ldots, a_n$ in $\mathbf{C}$. For any prime number p we consider the quotient map $\mathbf{Z} \longrightarrow \mathbf{F}_p$ and the induced map between the polynomial rings

$\mathbf{Z}[X] \longrightarrow \mathbf{F}_p[X]$. In this way, $f(X)$ induces a monic polynomial $f_p(X) \in \mathbf{F}_p[X]$ of degree n, its reduction modulo p. The polynomial ring $\mathbf{F}_p[X]$ being a unique factorization domain, we may write

$$f_p(X) = \prod_{i=1}^{s_p} g_i^{(p)}(X) ,$$

where s_p is a positive integer and $g_i^{(p)}(X)$ a monic irreducible polynomial in $\mathbf{F}_p[X]$ for all $i = 1, \dots, s_p$. Moreover, this decomposition is unique up to the ordering of the factors. We let $n_i^{(p)} = \deg g_i^{(p)}(X)$ for all i and note that $n = \sum_{i=1}^{s_p} n_i^{(p)}$. Therefore, assuming that the ordering is such that $n_i^{(p)} \geq n_j^{(p)}$ whenever $i \leq j$, we obtain a partition of n, in the sense of the following definition.

Definition C.1 *Let n be a positive integer. A partition δ of n of length s is a sequence $(n_1, \dots, n_s)$ of positive integers, such that $n = \sum_{i=1}^{s} n_i$ and $n_i \geq n_j$ for all $i \leq j$.*

Let Π be the set of all prime numbers and $\mathbf{\Delta}_n$ the set of all partitions of n. The above considerations show that the monic polynomial $f(X)$ induces a map

$$\delta_f : \Pi \longrightarrow \mathbf{\Delta}_n ,$$

where $\delta_f(p) = \left(n_1^{(p)}, \dots, n_{s_p}^{(p)}\right)$ is the partition of n associated with the degrees of the irreducible factors of the reduction $f_p(X) \in \mathbf{F}_p[X]$ of $f(X)$ modulo p for all prime numbers p. We say that $\delta_f(p)$ is the decomposition length type of the polynomial $f(X)$ modulo p. For example, if $f(X)$ is irreducible modulo p, then its decomposition length type modulo p is (n). On the other hand, if $f(X)$ decomposes into the product of linear factors modulo p, then $\delta_f(p) = (1, \dots, 1)$.

We now consider the splitting field $K = \mathbf{Q}(a_1, \dots, a_n)$ of $f(X)$ and the corresponding Galois group Γ. Any element $\gamma \in \Gamma$ permutes the roots $a_1, \dots, a_n$ and hence defines an element $\widetilde{\gamma}$ in the group S_n of permutations on n letters.[1] We may decompose $\widetilde{\gamma}$ into the product of disjoint cycles

$$\widetilde{\gamma} = \prod_{i=1}^{s_\gamma} c_i^{(\gamma)} ,$$

in such a way that each one of the n letters appears once and only once in the decomposition. (Hence, cycles of length 1 are allowed.) Moreover, this decomposition is unique up to the ordering of the $c_i^{(\gamma)}$'s. We let $n_i^{(\gamma)}$ be the length of the cycle $c_i^{(\gamma)}$ for all $i = 1, \dots, s_\gamma$ and assume that the ordering of the cycles is such that $n_i^{(\gamma)} \geq n_j^{(\gamma)}$ for all $i \leq j$. Since $n = \sum_{i=1}^{s_\gamma} n_i^{(\gamma)}$, the sequence $\left(n_1^{(\gamma)}, \dots, n_{s_\gamma}^{(\gamma)}\right)$ is a partition of n. In this way, we obtain a map

[1] The map $\gamma \mapsto \widetilde{\gamma}$ depends on the given parametrization of the roots of $f(X)$. If we relabel the roots, the permutation $\widetilde{\gamma}$ will change by an inner automorphism of S_n.

$$\delta'_f : \Gamma \longrightarrow \mathbf{\Delta}_n \ ,$$

which is defined by letting $\delta'_f(\gamma) = \left(n_1^{(\gamma)}, \ldots, n_{s_\gamma}^{(\gamma)}\right) \in \mathbf{\Delta}_n$ for all $\gamma \in \Gamma$.[2] We say that $\delta'_f(\gamma)$ is the cycle pattern type of γ. For example, the cycle pattern type of the identity element $1 \in \Gamma$ is $(1, \ldots, 1)$. In fact, the map $\gamma \mapsto \widetilde{\gamma}$ being an embedding of Γ into S_n, 1 is the only element $\gamma \in \Gamma$ with $\delta'_f(\gamma) = (1, \ldots, 1)$.

The relationship between the maps δ_f and δ'_f is described by Frobenius' density theorem. In order to state the result, we need the notion of density of a set of prime numbers.

Definition C.2 *Let Π be the set of all prime numbers. Then, a subset $\Pi_0 \subseteq \Pi$ is said to have density d if the limit*

$$\lim_n \frac{card\,(\Pi_0 \cap [0,n])}{card\,(\Pi \cap [0,n])} = \lim_n \frac{card\,\{p : p \in \Pi_0, p \leq n\}}{card\,\{p : p \ prime, p \leq n\}}$$

exists and equals d.

For example, a finite set of prime numbers has density 0. It follows that the density of a set Π_0 of prime numbers is 1 if the complement $\Pi \setminus \Pi_0$ is finite.

We are now ready to state Frobenius' density theorem.

Theorem C.3 *Let $f(X) \in \mathbf{Z}[X]$ be a monic polynomial of degree n without multiple roots in $\mathbf{C}$. We consider the Galois group Γ of $f(X)$ and the maps δ_f and δ'_f defined above. We fix a partition $\delta \in \mathbf{\Delta}_n$ and let $\Pi_\delta = \delta_f^{-1}(\delta)$ and $\Gamma_\delta = \delta_f'^{-1}(\delta)$. Then, Π_δ has a density which is equal to $\dfrac{card\,(\Gamma_\delta)}{card\,(\Gamma)}$.* □

The following consequence of the density theorem played an important role in the argumentation of §3.1.2.

Corollary C.4 *Let $f(X) \in \mathbf{Z}[X]$ be a monic irreducible polynomial, which splits completely into the product of linear factors modulo p for all but finitely many prime numbers p. Then, the polynomial $f(X)$ is linear.*

Proof. Being irreducible in $\mathbf{Z}[X]$, the polynomial $f(X)$ has distinct roots in $\mathbf{C}$; let Γ be its Galois group. Then, the order N of Γ is equal to the degree of the splitting field K of $f(X)$ over $\mathbf{Q}$. We apply Frobenius' density theorem to the special case of the partition $\delta = (1, \ldots, 1)$ of $n = \deg f(X)$. In view of our hypothesis, the set Π_δ in Theorem C.3 consists of all but finitely many prime numbers and hence its density is 1. Since the set Γ_δ is the singleton $\{1\}$, we have $1 = \frac{1}{N}$ and hence $N = 1$. It follows that $K = \mathbf{Q}$, in which case the roots $a_1, \ldots, a_n$ of $f(X)$ are rational numbers. The ring $\mathbf{Z}$ being integrally closed in $\mathbf{Q}$, in view of Lemma A.15, we conclude that $a_i \in \mathbf{Z}$ for all $i = 1, \ldots, n$ and hence $f(X) = \prod_{i=1}^n (X - a_i)$ in $\mathbf{Z}[X]$. Since the polynomial $f(X)$ is irreducible in $\mathbf{Z}[X]$, we must have $n = 1$. □

[2] Since the sequences of lengths of the cycles in the cycle decompositions of two conjugate permutations are the same, the map δ'_f does not depend on the labelling of the roots of $f(X)$ (cf. footnote (1)).

C.2 Exercises

1. Let Γ be a finite group acting on the non-empty finite set X. For any $\gamma \in \Gamma$ we consider the fixed set $\text{Fix}(\gamma) = \{x \in X : \gamma x = x\}$ and denote by ν_γ its cardinality. Similarly, for any $x \in X$ we consider the stabilizer $\text{Stab}(x) = \{\gamma \in \Gamma : \gamma x = x\}$ and denote by μ_x its order.
(i) Show that $\sum_{\gamma\in\Gamma} \nu_\gamma = \sum_{x\in X} \mu_x$.
(ii) If the action is transitive, then show that $\sum_{\gamma\in\Gamma} \nu_\gamma = |\Gamma|$.
(iii) Assume that the action is transitive. If $\text{Fix}(\gamma) \neq \emptyset$ for all $\gamma \in \Gamma$, then show that X is a singleton.
2. Let $f(X) \in \mathbf{Z}[X]$ be a monic irreducible polynomial, whose reduction $f_p(X) \in \mathbf{F}_p[X]$ has a root in $\mathbf{F}_p$ for all but finitely many prime numbers p. The goal of this Exercise is to prove that $f(X)$ is linear (generalizing thereby Corollary C.4).
(i) Let Γ be the Galois group of the polynomial $f(X)$. Show that any element of Γ fixes at least one root of $f(X)$ in $\mathbf{C}$.
(ii) Show that the polynomial $f(X)$ has only one root in $\mathbf{C}$ and hence conclude that $\deg f(X) = 1$.
(*Hint:* Use Exercise 1(iii) above.)
3. Let a be an integer with $\sqrt{a} \notin \mathbf{Z}$. Show that there are infinitely many prime numbers p for which a is the square of an integer modulo p and infinitely many prime numbers p for which a is not the square of any integer modulo p.

D

Homological Techniques

In this Appendix, we collect the basic results from Homological Algebra that were used in Chap. 4. Our goal is not to present a complete treatment on group homology, but rather to state the results needed in the book and place them in the perspective of the general theory. Consequently, we shall give no proofs of the statements to be made and refer instead the interested reader to specialized books on the subject, such as [9, 34] and [48].

D.1 Complexes and Homology

D.1.1 Chain Complexes

We fix a ring R. A chain complex of left R-modules is a pair (C, d), where $C = \bigoplus_{i \geq 0} C_i$ is a graded left R-module and $d = (d_n)_n$ a homogeneous R-linear endomorphism of C of degree -1, satisfying the equality $d^2 = 0$ (d is the differential of the complex). The chain complex (C, d) is presented pictorially as

$$C_0 \xleftarrow{d_1} C_1 \xleftarrow{d_2} \cdots \xleftarrow{d_n} C_n \xleftarrow{d_{n+1}} \cdots$$

The elements of the submodule $\ker d_n$ (resp. $\operatorname{im} d_{n+1}$) of C_n are referred to as n-cycles (resp. n-boundaries). The homology $H(C, d)$ of (C, d) is the graded R-module, which is given in degree n by $H_n(C, d) = \ker d_n / \operatorname{im} d_{n+1}$. The complex (C, d) is called acyclic if $H_n(C, d) = 0$ for all n.

Let (C, d) and (C', d') be two chain complexes. Then, a chain map

$$\varphi : (C, d) \longrightarrow (C', d')$$

is a homogeneous R-linear map of degree 0 from C to C', such that $\varphi d = d' \varphi$. A chain map φ as above induces R-linear maps

$$\varphi_n : H_n(C, d) \longrightarrow H_n(C', d')$$

for all n. If these latter maps are isomorphisms, the chain map φ is called a quasi-isomorphism. In particular, an isomorphism of chain complexes (defined in the obvious way) is a quasi-isomorphism. Two chain maps

$$\varphi, \psi : (C, d) \longrightarrow (C', d')$$

are called homotopic if there exists a homogeneous map $\Sigma : C \longrightarrow C'$ of degree $+1$, such that $\Sigma d + d'\Sigma = \varphi - \psi$. In that case, the maps induced in homology by φ and ψ are equal, i.e.

$$\varphi_n = \psi_n : H_n(C, d) \longrightarrow H_n(C', d')$$

for all n. A chain complex (C, d) is called contractible if the chain endomorphisms id_C and 0 of (C, d) are homotopic. It follows that a contractible chain complex is acyclic. A chain map $\varphi : (C, d) \longrightarrow (C', d')$ is called a homotopy equivalence if there exists a chain map $\psi : (C', d') \longrightarrow (C, d)$, such that the compositions $\varphi\psi$ and $\psi\varphi$ are homotopic with the identity maps $\mathrm{id}_{C'}$ and id_C respectively.

If $\varphi : (C, d) \longrightarrow (C', d')$ is a chain map then the kernel of the R-linear map $\varphi : C \longrightarrow C'$ is a graded d-invariant R-submodule of C; therefore, $(\ker \varphi, d)$ is a chain complex. Similarly, $(\mathrm{im}\, \varphi, d')$ is a chain subcomplex of (C', d'). In this way, one extends the notion of exactness to the category of chain complexes and maps. In particular, one may consider a short exact sequence of chain complexes

$$0 \longrightarrow (C', d') \xrightarrow{i} (C, d) \xrightarrow{p} (C'', d'') \longrightarrow 0 .$$

A short exact sequence as above induces a long exact sequence of R-modules

$$\cdots \longrightarrow H_n(C', d') \xrightarrow{i_n} H_n(C, d) \xrightarrow{p_n} H_n(C'', d'') \xrightarrow{\partial_n} H_{n-1}(C', d') \longrightarrow \cdots$$

The notions of cochain complexes, cochain maps and cohomology can be defined in the same way, by considering differentials of degree $+1$.

D.1.2 Double Complexes

A double chain complex (or chain bicomplex) of left R-modules consists of a bigraded left R-module $C = \bigoplus_{i,j \geq 0} C_{ij}$ together with R-linear maps d_h and d_v, which are homogeneous of degrees $(-1, 0)$ and $(0, -1)$ respectively and satisfy the equalities $d_h^2 = 0$, $d_v^2 = 0$ and $d_h d_v + d_v d_h = 0$. The map d_h (resp. d_v) is referred to as the horizontal (resp. vertical) differential of the double complex.

If (C, d_h, d_v) and (C', d'_h, d'_v) are chain bicomplexes, then a chain bicomplex map

$$\varphi : (C, d_h, d_v) \longrightarrow (C', d'_h, d'_v)$$

is a homogeneous R-linear map of degree $(0, 0)$ from C to C', such that $\varphi d_h = d'_h \varphi$ and $\varphi d_v = d'_v \varphi$. It is clear that a chain bicomplex map φ as above restricts in the horizontal direction to a chain map between the rows (C_{*j}, d_h) and (C'_{*j}, d'_h) for all j. Similarly, φ restricts in the vertical direction to a chain map between the columns (C_{i*}, d_v) and (C'_{i*}, d'_v) for all i.

For any double complex (C, d_h, d_v) there is an associated (total) chain complex $(\operatorname{Tot} C, d)$, which is defined by letting $(\operatorname{Tot} C)_n = \bigoplus_{i+j=n} C_{ij}$ for all n and $d = d_h + d_v$. Moreover, any chain bicomplex map

$$\varphi : (C, d_h, d_v) \longrightarrow (C', d'_h, d'_v)$$

induces a chain map

$$\operatorname{Tot} \varphi : (\operatorname{Tot} C, d) \longrightarrow (\operatorname{Tot} C', d') \; .$$

We say that φ is a quasi-isomorphism if this is the case for $\operatorname{Tot} \varphi$.

Proposition D.1 *Let $\varphi : (C, d_h, d_v) \longrightarrow (C', d'_h, d'_v)$ be a chain bicomplex map. Then, φ is a quasi-isomorphism if either one of the following two conditions is satisfied:*

(i) φ restricts to a quasi-isomorphism between the columns (C_{i*}, d_v) and (C'_{i*}, d'_v) for all i.

(ii) φ restricts to a quasi-isomorphism between the rows (C_{*j}, d_h) and (C'_{*j}, d'_h) for all j. □

Corollary D.2 *Let (C, d_h, d_v) be a double complex.*

(i) If the rows (C_{*j}, d_h) are acyclic in positive degrees for all j, then the chain complexes $(\operatorname{Tot} C, d)$ and $\left(\bigoplus_j C_{0j}/d_h C_{1j}, \overline{d_v}\right)$ are quasi-isomorphic.

(ii) If the columns (C_{i*}, d_v) are acyclic for all $i > 0$, then the complex $(\operatorname{Tot} C, d)$ is quasi-isomorphic with the 0-th column (C_{0*}, d_v). □

The notion of a double cochain complex can be defined in the same way, by considering differentials of degrees $(+1, 0)$ and $(0, +1)$.

Examples D.3 (i) Let R be a ring and (C, d) (resp. (C', d')) a chain complex of right (resp. left) R-modules. Then, there is a chain bicomplex of abelian groups $(C \otimes_R C', d \otimes 1, \pm 1 \otimes d')$, consisting of $C_i \otimes_R C'_j$ in degree (i, j); the signs $+$ and $-$ in the vertical differentials alternate in order for the operator $d_h d_v + d_v d_h$ to vanish. We note that there are natural maps (called Künneth maps)

$$K : H_i(C) \otimes_R H_j(C') \longrightarrow H_{i+j}(\operatorname{Tot}(C \otimes_R C'))$$

for all $i, j \geq 0$, which are given by letting $[x_i] \otimes [x'_j] \mapsto [x_i \otimes x'_j]$ for any homology classes $[x_i] \in H_i(C)$ and $[x'_j] \in H_j(C')$. Similar remarks apply to cochain complexes and cohomology.

(ii) Let R be a ring, (C, d) a chain complex and (C', d') a cochain complex of left R-modules. Then, there is a double cochain complex of abelian groups $(\operatorname{Hom}_R(C, C'), d^*, \pm d'_*)$, which consists of $\operatorname{Hom}_R(C_i, C'^j)$ in degree (i, j). Here,

d^* and d'_* denote the additive maps between the Hom-groups induced by d and d' respectively. We note that there are natural maps

$$H^{i+j}(\mathrm{Tot}\,\mathrm{Hom}_R(C,C')) \longrightarrow \mathrm{Hom}_R\big(H_i(C),H^j(C')\big)$$

for all $i,j \geq 0$, which are given by mapping a cohomology class $[f] \in H^{i+j}(\mathrm{Tot}\,\mathrm{Hom}_R(C,C'))$ onto the R-linear map from $H_i(C)$ to $H^j(C')$ induced by the component $f_{ij} \in \mathrm{Hom}_R(C_i,C'^j)$ of f.

D.1.3 Tor and Ext

As an example of the notions introduced above, we define the functors Tor and Ext. To that end, let us fix a right R-module M and a left R-module N. For any R-projective resolutions

$$0 \longleftarrow M \xleftarrow{\varepsilon} P_* \quad \text{and} \quad 0 \longleftarrow N \xleftarrow{\eta} Q_*$$

we may consider the chain complexes of abelian groups $P_* \otimes_R N$, $M \otimes_R Q_*$ and the double complex $P_* \otimes_R Q_*$ (cf. Example D.3(i)). Then, there are quasi-isomorphisms

$$P_* \otimes_R N \xleftarrow{1\otimes\eta} \mathrm{Tot}(P_* \otimes_R Q_*) \xrightarrow{\varepsilon\otimes 1} M \otimes_R Q_* \ .$$

In particular, we may define the Tor-groups by letting

$$\mathrm{Tor}_n^R(M,N) = H_n(P_* \otimes_R N) \simeq H_n(\mathrm{Tot}(P_* \otimes_R Q_*)) \simeq H_n(M \otimes_R Q_*)$$

for all n. If

$$0 \longleftarrow M \xleftarrow{\varepsilon'} P'_* \quad \text{and} \quad 0 \longleftarrow N \xleftarrow{\eta'} Q'_*$$

are also R-projective resolutions of M and N, then there are chain maps

$$\varphi : P_* \longrightarrow P'_* \quad \text{and} \quad \psi : Q_* \longrightarrow Q'_*$$

that satisfy the equalities $\varepsilon = \varepsilon'\varphi_0$ and $\eta = \eta'\psi_0$ and are unique up to homotopy with that property. These chain maps are homotopy equivalences and hence there is a commutative diagram of quasi-isomorphisms

$$\begin{array}{ccccc} P_* \otimes_R N & \xleftarrow{1\otimes\eta} & \mathrm{Tot}(P_* \otimes_R Q_*) & \xrightarrow{\varepsilon\otimes 1} & M \otimes_R Q_* \\ {\scriptstyle \varphi\otimes 1} \downarrow & & {\scriptstyle Tot(\varphi\otimes\psi)} \downarrow & & {\scriptstyle 1\otimes\psi} \downarrow \\ P'_* \otimes_R N & \xleftarrow{1\otimes\eta'} & \mathrm{Tot}(P'_* \otimes_R Q'_*) & \xrightarrow{\varepsilon'\otimes 1} & M \otimes_R Q'_* \end{array}$$

It follows that the definition of the Tor-groups is independent of the chosen resolutions, in the sense that the vertical quasi-isomorphisms in the diagram above induce identifications in homology.

The behavior of the Tor-groups with respect to direct sums is described in the next result.

Proposition D.4 *(i) Let R be a ring, $(M_i)_i$ a family of right R-modules and $(N_j)_j$ a family of left R-modules. If $M = \bigoplus_i M_i$ and $N = \bigoplus_j N_j$, then the inclusions $M_i \hookrightarrow M$ and $N_j \hookrightarrow N$ induce an isomorphism of abelian groups $Tor_n^R(M,N) \simeq \bigoplus_{i,j} Tor_n^R(M_i,N_j)$ for all n.*

(ii) Let $R_1,\ldots,R_s$ be rings and $R = \prod_{i=1}^s R_i$ their direct product. For each $i = 1,\ldots,s$ we consider a right R_i-module M_i and a left R_i-module N_i. Then, the abelian group $M = \bigoplus_{i=1}^s M_i$ (resp. $N = \bigoplus_{i=1}^s N_i$) has the structure of a right (resp. left) R-module and there is a natural isomorphism $Tor_n^R(M,N) \simeq \bigoplus_{i=1}^s Tor_n^{R_i}(M_i,N_i)$ for all n. □

In order to define the Ext-groups of two left R-modules M and N, one considers a projective resolution

$$0 \longleftarrow M \longleftarrow P_*$$

of M and an injective resolution

$$0 \longrightarrow N \longrightarrow I^*$$

of N. Then, there are induced quasi-isomorphisms of cochain complexes

$$\mathrm{Hom}_R(P_*,N) \longrightarrow \mathrm{Tot}\,\mathrm{Hom}_R(P_*,I^*) \longleftarrow \mathrm{Hom}_R(M,I^*)$$

(cf. Example D.3(ii)) and one defines for any n

$$\begin{aligned}\mathrm{Ext}_R^n(M,N) &= H^n(\mathrm{Hom}_R(P_*,N)) \\ &\simeq H^n(\mathrm{Tot}\,\mathrm{Hom}_R(P_*,I^*)) \\ &\simeq H^n(\mathrm{Hom}_R(M,I^*))\ .\end{aligned}$$

Remarks D.5 (i) Let R be a ring, M a right R-module and N a left R-module. In degree 0, there is an identification $\mathrm{Tor}_0^R(M,N) \simeq M \otimes_R N$. The groups $\mathrm{Tor}_n^R(M,N)$ vanish for all $n > 0$ if either M or N is projective (or, more generally, flat) as an R-module.

(ii) Let R be a ring and M,N two left R-modules. In degree 0, there is an identification $\mathrm{Ext}_R^0(M,N) \simeq \mathrm{Hom}_R(M,N)$. The groups $\mathrm{Ext}_R^n(M,N)$ vanish for all $n>0$ if either M is projective or N is injective as an R-module.

(iii) Let (C,d) and (C',d') be two chain complexes of abelian groups, such that either one of them is free. Then, the homology of the double complex $(C\otimes C', d\otimes 1, \pm 1 \otimes d')$ fits into a natural short exact sequence

$$0\rightarrow(H_*(C)\otimes H_*(C'))_n \xrightarrow{K} H_n(\mathrm{Tot}(C\otimes C'))\rightarrow(\mathrm{Tor}(H_*(C),H_*(C')))_{n-1}\rightarrow 0\ ,$$

where

$$(H_*(C)\otimes H_*(C'))_n = \bigoplus_{i+j=n} H_i(C)\otimes H_j(C')\ ,$$

K is the Künneth map (cf. Example D.3(i)) and

$$(\mathrm{Tor}(H_*(C),H_*(C')))_{n-1} = \bigoplus_{i+j=n-1} \mathrm{Tor}_1^{\mathbf{Z}}(H_i(C),H_j(C'))$$

for all n. In particular, if the complexes (C,d) and (C',d') are free resolutions of the abelian groups M and M' respectively, then the chain complex $\mathrm{Tot}(C\otimes C')$ is a free resolution of $M\otimes M'$, provided that $\mathrm{Tor}_1^{\mathbf{Z}}(M,M') = 0$.

D.2 Group Homology and Cohomology

D.2.1 Basic Definitions

We now consider a commutative ring k, a group G and specialize the above discussion to the case where R is the group algebra kG. For any left kG-module M we define the homology groups $H_n(G,M)$ and the cohomology groups $H^n(G,M)$ of G with coefficients in M, by letting

$$H_n(G,M) = \mathrm{Tor}_n^{kG}(k,M) \quad \text{and} \quad H^n(G,M) = \mathrm{Ext}_{kG}^n(k,M)$$

for all n. Here, k is viewed as a (right and left) kG-module, by means of the trivial G-action. In particular, if

$$0 \longleftarrow k \stackrel{\varepsilon}{\longleftarrow} P_*$$

is a resolution of k by projective right kG-modules, then

$$H_n(G,M) = H_n(P_* \otimes_{kG} M)$$

for all n. This definition doesn't depend upon the chosen resolution. More precisely, if

$$0 \longleftarrow k \stackrel{\varepsilon'}{\longleftarrow} P'_*$$

is another kG-projective resolution of k, then there is a unique up to homotopy chain map $\varphi : P_* \longrightarrow P'_*$ satisfying $\varepsilon = \varepsilon'\varphi_0$, which is a homotopy equivalence and induces a canonical identification

$$H_n(P_* \otimes_{kG} M) \simeq H_n(P'_* \otimes_{kG} M)$$

for all n. Similarly, the cohomology groups $H^n(G,M)$ of G with coefficients in the left kG-module M can be computed by using a projective resolution Q_* of the trivial left kG-module k, as the cohomology groups of the cochain complex $\mathrm{Hom}_{kG}(Q_*,M)$.

In order to describe the so-called standard resolution of k, we let

$$S_n(G,k) = k[G^{n+1}] = \bigoplus \left\{ k \cdot (g_0,\ldots,g_n) : (g_0,\ldots,g_n) \in G^{n+1} \right\}$$

for all $n \geq 0$, with left (resp. right) kG-module structure induced by the left (resp. right) diagonal action of G on G^{n+1}; in particular, $S_0(G,k) = kG$. For all $n \geq 1$ and $i \in \{0,\ldots,n\}$ we define a k-linear map

$$\delta_i^n : S_n(G,k) \longrightarrow S_{n-1}(G,k) \ ,$$

by letting

$$\delta_i^n(g_0,\ldots,g_n) = (g_0,\ldots,\widehat{g_i},\ldots,g_n)$$

for any element $(g_0, \dots, g_n) \in G^{n+1}$; here, the symbol $\widehat{\ }$ over an element denotes omission of that element. It is clear that the k-linear maps δ_i^n are, in fact, kG-linear for both left and right actions. We now define the operators

$$\delta_n, \delta'_n : S_n(G,k) \longrightarrow S_{n-1}(G,k) ,$$

by letting

$$\delta_n = \sum\nolimits_{i=0}^{n} (-1)^i \delta_i^n \quad \text{and} \quad \delta'_n = \sum\nolimits_{i=0}^{n-1} (-1)^i \delta_i^n$$

for all $n \geq 1$.

Proposition D.6 *Let k be a commutative ring and G a group.*

(i) The chain complex

$$k \xleftarrow{\varepsilon} S_0(G,k) \xleftarrow{\delta_1} S_1(G,k) \xleftarrow{\delta_2} \cdots \xleftarrow{\delta_n} S_n(G,k) \xleftarrow{\delta_{n+1}} \cdots ,$$

where ε is the augmentation, is a free resolution $(S(G,k), \delta) = (S_*(G,k), \delta)$ of k as a trivial left or right kG-module.

(ii) The chain complex

$$S_0(G,k) \xleftarrow{\delta'_1} S_1(G,k) \xleftarrow{\delta'_2} \cdots \xleftarrow{\delta'_n} S_n(G,k) \xleftarrow{\delta'_{n+1}} \cdots$$

is contractible as a complex of left or right kG-modules. In particular, it is acyclic. □

In order to describe the functoriality of the (co-)homology groups, let us consider a group G and a homomorphism $f : M \longrightarrow M'$ of left kG-modules. Then, there are induced additive maps

$$f_* : H_n(G,M) \longrightarrow H_n(G,M') \quad \text{and} \quad f_* : H^n(G,M) \longrightarrow H^n(G,M')$$

for all n. On the other hand, let $\phi : G \longrightarrow G'$ be a group homomorphism. Then, ϕ induces a k-linear chain map

$$\widetilde{\phi} : S(G,k) \longrightarrow S(G',k) .$$

For any kG'-module M we denote by M_ϕ the kG-module obtained from M by restriction of scalars along ϕ. Then, the chain maps

$$\widetilde{\phi} \otimes 1 : S(G,k) \otimes_{kG} M_\phi \longrightarrow S(G',k) \otimes_{kG'} M$$

and

$$\mathrm{Hom}\left(\widetilde{\phi}, 1\right) : \mathrm{Hom}_{kG'}(S(G',k), M) \longrightarrow \mathrm{Hom}_{kG}(S(G,k), M_\phi)$$

induce additive maps

$$\phi_* : H_n(G, M_\phi) \longrightarrow H_n(G', M) \quad \text{and} \quad \phi^* : H^n(G', M) \longrightarrow H^n(G, M_\phi)$$

respectively for all n.

Remarks D.7 (i) Let k be a commutative ring, G a group and M a left kG-module. Then, the homology groups $H_n(G, M)$ and the cohomology groups $H^n(G, M)$ depend only upon the action of G on the abelian group M. In order to make this assertion precise, let us denote by M' the $\mathbf{Z}G$-module obtained from the kG-module M by restriction of scalars. Since

$$S_*(G, k) = S_*(G, \mathbf{Z}) \otimes_{\mathbf{Z}G} kG \quad \text{and} \quad S_*(G, k) = kG \otimes_{\mathbf{Z}G} S_*(G, \mathbf{Z})$$

as right and left kG-modules respectively, we have

$$\begin{aligned} \mathrm{Tor}_n^{kG}(k, M) &= H_n(S_*(G, k) \otimes_{kG} M) \\ &= H_n(S_*(G, \mathbf{Z}) \otimes_{\mathbf{Z}G} M') \\ &= \mathrm{Tor}_n^{\mathbf{Z}G}(\mathbf{Z}, M') \end{aligned}$$

and

$$\begin{aligned} \mathrm{Ext}_{kG}^n(k, M) &= H^n(\mathrm{Hom}_{kG}(S_*(G, k), M)) \\ &= H^n(\mathrm{Hom}_{\mathbf{Z}G}(S_*(G, \mathbf{Z}), M')) \\ &= \mathrm{Ext}_{\mathbf{Z}G}^n(\mathbf{Z}, M'), \end{aligned}$$

i.e. $H_n(G, M) = H_n(G, M')$ and $H^n(G, M) = H^n(G, M')$ for all n.

(ii) Let G be a group, M a left $\mathbf{Z}G$-module and $g \in G$ a fixed element. We consider the inner automorphism (conjugation) $I_g \in \mathrm{Aut}(G)$ and let $M_g = M_{I_g}$ be the $\mathbf{Z}G$-module obtained from M by restriction of scalars along I_g. We also consider the $\mathbf{Z}G$-linear map

$$\lambda_g : M \longrightarrow M_g \ ,$$

which is defined by $m \mapsto gm$, $m \in M$. Then, the compositions

$$H_n(G, M) \stackrel{(\lambda_g)_*}{\longrightarrow} H_n(G, M_g) \stackrel{(I_g)_*}{\longrightarrow} H_n(G, M)$$

and

$$H^n(G, M) \stackrel{(\lambda_g)_*}{\longrightarrow} H^n(G, M_g) \stackrel{[(I_g)^*]^{-1}}{\longrightarrow} H^n(G, M)$$

can be shown to be the identity operators for all n.

Examples D.8 (i) If G is a group and M a left $\mathbf{Z}G$-module, then

$$H_0(G, M) = \mathbf{Z} \otimes_{\mathbf{Z}G} M \simeq M / < gm - m : g \in G, m \in M >$$

is the coinvariance M_G of M (cf. Remark D.5(i)) and

$$H^0(G, M) = \mathrm{Hom}_{\mathbf{Z}G}(\mathbf{Z}, M) \simeq \{m \in M : gm = m \ \text{ for all } g \in G\}$$

is the invariance M^G of M (cf. Remark D.5(ii)).

(ii) Let k be a field of characteristic 0 and G a finite group. Then, in view of Maschke's theorem (Theorem 1.9), the groups $H_n(G,M)$ and $H^n(G,M)$ vanish for all $n > 0$ and all kG-modules M (cf. Remarks D.5(i),(ii)).

(iii) Let G be a finite cyclic group with generator τ. Then, the chain complex

$$\mathbf{Z} \xleftarrow{\varepsilon} \mathbf{Z}G \xleftarrow{1-\tau} \mathbf{Z}G \xleftarrow{N} \mathbf{Z}G \xleftarrow{1-\tau} \mathbf{Z}G \xleftarrow{N} \mathbf{Z}G \xleftarrow{1-\tau} \cdots ,$$

where $N = \sum\{t : t \in G\}$, is a $\mathbf{Z}G$-free resolution of $\mathbf{Z}$. In particular, for any $\mathbf{Z}G$-module M the homology groups of G with coefficients in M are computed as the homology groups of the chain complex

$$M \xleftarrow{1-\tau} M \xleftarrow{N} M \xleftarrow{1-\tau} M \xleftarrow{N} M \xleftarrow{1-\tau} \cdots$$

Similarly, the cohomology groups of G with coefficients in M are computed as the cohomology groups of the cochain complex

$$M \xrightarrow{1-\tau} M \xrightarrow{N} M \xrightarrow{1-\tau} M \xrightarrow{N} M \xrightarrow{1-\tau} \cdots$$

In particular, $H_n(G,M) = H_{n+2}(G,M)$ and $H^n(G,M) = H^{n+2}(G,M)$ for all $n > 0$.

Let k be a commutative ring and G a group. Then, G is said to have finite homological dimension over k if there exists an integer $n \geq 0$, such that $H_i(G,M) = 0$ for all $i > n$ and all kG-modules M. The smallest n with this property is the homological dimension $\text{hd}_k G$ of G over k. In this way, Example D.8(ii) implies that $\text{hd}_k G = 0$ if G is a finite group and k a field of characteristic 0.

Proposition D.9 *Let k be a commutative ring.*

(i) If G is a group of finite homological dimension over k and $H \leq G$ a subgroup, then H has finite homological dimension over k as well; in fact, $hd_k H \leq hd_k G$.

(ii) If $(G_i)_i$ is a family of groups of uniformly bounded homological dimension over k and $G = *_i G_i$ the corresponding free product, then G has finite homological dimension over k; in fact, $hd_k G \leq \max\{1, \max_i hd_k G_i\}$.

(iii) If $(G_i)_i$ is a directed system of groups of uniformly bounded homological dimension over k and $G = \varinjlim_i G_i$ the corresponding direct limit, then G has finite homological dimension over k; in fact, $hd_k G \leq \max_i hd_k G_i$. □

D.2.2 H^2 and Extensions

Let G be a group and M a left $\mathbf{Z}G$-module. Then, an extension of G by M is a group X having M as a normal subgroup with $X/M \simeq G$, in such a way that conjugation induces the given action of G on M. Two extensions

$$1 \longrightarrow M \longrightarrow X \longrightarrow G \longrightarrow 1 \quad \text{and} \quad 1 \longrightarrow M \longrightarrow X' \longrightarrow G \longrightarrow 1$$

are called equivalent if there is a group homomorphism $f : X \longrightarrow X'$ that fits into a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M & \longrightarrow & X & \longrightarrow & G & \longrightarrow & 1 \\ & & \| & & f \downarrow & & \| & & \\ 1 & \longrightarrow & M & \longrightarrow & X' & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

There is a bijective correspondence between the set of equivalence classes of extensions of G by M and the cohomology group $H^2(G,M)$, such that the equivalence class of the semi-direct product $M \times G$ corresponds to the zero element of $H^2(G,M)$. In this way, the functorial behavior of H^2 corresponds to certain operations on extensions. In order to explicit these operations, let us consider an extension

$$1 \longrightarrow M \xrightarrow{\imath} X \xrightarrow{\pi} G \longrightarrow 1$$

and the corresponding cohomology class $\alpha \in H^2(G,M)$.

Functoriality in the coefficient module: Let M' be another $\mathbf{Z}G$-module and $f : M \longrightarrow M'$ a $\mathbf{Z}G$-linear map. We consider the $\mathbf{Z}X$-module M'_π obtained from M' by restricting its G-module structure along π and note that $\{(-f(m), \imath(m)) : m \in M\}$ is a normal subgroup of the semi-direct product $M'_\pi \times X$. The corresponding quotient group X' fits into the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M & \xrightarrow{\imath} & X & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & f \downarrow & & f' \downarrow & & \| & & \\ 1 & \longrightarrow & M' & \xrightarrow{\imath'} & X' & \xrightarrow{\pi'} & G & \longrightarrow & 1 \end{array}$$

where $\imath'$ and f' are obtained by composing the natural maps into $M' \times X$ with the projection onto X', whereas π' maps the class of an element (m', x) in X' onto $\pi(x) \in G$. Then, the G-module structure induced on M' by the extension in the bottom row of the above diagram is its original G-module structure and the element of $H^2(G, M')$ which classifies that extension is the image $f_*\alpha$ of α under the map

$$f_* : H^2(G,M) \longrightarrow H^2(G,M') \, .$$

Functoriality in the group: Let G' be another group and $\phi : G' \longrightarrow G$ a group homomorphism. We consider the subgroup $X'' = \{(x, g') \in X \times G' : \pi(x) = \phi(g')\}$ of the direct product $X \times G'$ and note that it fits into the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M & \xrightarrow{\imath''} & X'' & \xrightarrow{\pi''} & G' & \longrightarrow & 1 \\ & & \| & & \phi'' \downarrow & & \phi \downarrow & & \\ 1 & \longrightarrow & M & \xrightarrow{\imath} & X & \xrightarrow{\pi} & G & \longrightarrow & 1 \end{array}$$

where ϕ'' and π'' are the restrictions to X'' of the projections of $X \times G'$ onto X and G' respectively, whereas $\imath''$ maps $m \in M$ onto $(\imath(m), 1) \in X''$. Then, the G'-module structure induced on M by the extension in the top row of the above diagram is the one obtained by restricting its original G-module structure along ϕ, thereby identifying it with M_ϕ. Moreover, the element of $H^2(G', M_\phi)$ which classifies that extension is the image $\phi^*\alpha$ of α under the map

$$\phi^* : H^2(G, M) \longrightarrow H^2(G', M_\phi) .$$

Proposition D.10 *Consider a morphism of group extensions with abelian kernels*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M & \longrightarrow & X & \longrightarrow & G & \longrightarrow & 1 \\ & & {\scriptstyle f}\downarrow & & \downarrow & & {\scriptstyle \phi}\downarrow & & \\ 1 & \longrightarrow & M' & \longrightarrow & X' & \longrightarrow & G' & \longrightarrow & 1 \end{array}$$

If $\alpha \in H^2(G, M)$ and $\alpha' \in H^2(G', M')$ are the cohomology classes classifying these extensions, then $f_*\alpha = \phi^*\alpha' \in H^2(G, M')$. □

D.2.3 Products

We fix a group G and consider the standard resolution $S_* = (S_*(G, \mathbf{Z}), \delta)$ of the trivial G-module $\mathbf{Z}$. We recall that $S_n = \mathbf{Z}[G^{n+1}]$ is projective both as a left and as a right $\mathbf{Z}G$-module. The chain complex $\mathrm{Tot}(S_* \otimes S_*)$ is a resolution of $\mathbf{Z} \otimes \mathbf{Z} = \mathbf{Z}$ (cf. Remark D.5(iii)), consisting of projective left (and right) $\mathbf{Z}G$-modules (the group G acts diagonally on the tensor product; cf. Lemma 1.8(ii)). Hence, there is a left $\mathbf{Z}G$-linear chain map

$$\Delta' : S_* \longrightarrow \mathrm{Tot}(S_* \otimes S_*) ,$$

which commutes with the augmentation maps to $\mathbf{Z}$ and is unique up to homotopy with this property. Similarly, there is a right $\mathbf{Z}G$-linear chain map

$$\Delta'' : S_* \longrightarrow \mathrm{Tot}(S_* \otimes S_*) ,$$

which commutes with the augmentation maps to $\mathbf{Z}$ and is unique up to homotopy with this property. Chain maps Δ' and Δ'' as above are homotopy equivalences and are referred to as diagonal approximations.

We now construct a specific diagonal approximation

$$\Delta : S_* \longrightarrow \mathrm{Tot}(S_* \otimes S_*) ,$$

called the Alexander-Whitney map. To that end, we define in degree n the additive map

$$\Delta_n : S_n \longrightarrow \bigoplus\nolimits_{i=0}^{n} S_i \otimes S_{n-i} ,$$

by letting $\Delta_n(g_0, \ldots, g_n) = \sum_{i=0}^{n} (g_0, \ldots, g_i) \otimes (g_i, \ldots, g_n)$ for all $(n+1)$-tuples $(g_0, \ldots, g_n) \in G^{n+1}$.

Lemma D.11 *The Alexander-Whitney map $\Delta = (\Delta_n)_n$ is a chain map, which is $\mathbf{Z}G$-linear for both left and right actions and commutes with the augmentation maps to $\mathbf{Z}$.* □

Using the Alexander-Whitney map, we define the cup- and cap-products.

Cup-products: Let M, N be left $\mathbf{Z}G$-modules and $M \otimes N$ the corresponding tensor product, viewed as a left $\mathbf{Z}G$-module with diagonal action. Then, there is a morphism of cochain complexes

$$\_ \cup \_ : \mathrm{Tot}(\mathrm{Hom}_{\mathbf{Z}G}(S_*, M) \otimes \mathrm{Hom}_{\mathbf{Z}G}(S_*, N)) \longrightarrow \mathrm{Hom}_{\mathbf{Z}G}(S_*, M \otimes N)$$

(cf. Example D.3(i)), which is defined as follows: For any $a \in \mathrm{Hom}_{\mathbf{Z}G}(S_i, M)$ and $b \in \mathrm{Hom}_{\mathbf{Z}G}(S_j, N)$, the element $a \cup b \in \mathrm{Hom}_{\mathbf{Z}G}(S_{i+j}, M \otimes N)$ maps any $x \in G^{i+j+1} \subseteq S_{i+j}$ with $\Delta_{i+j} x = \sum_{k+l=i+j} x_k \otimes x'_l \in \bigoplus_{k+l=i+j} S_k \otimes S_l$ onto $(-1)^{ij} a(x_i) \otimes b(x'_j) \in M \otimes N$. The induced additive maps

$$\_ \cup \_ : H^i(G, M) \otimes H^j(G, N) \longrightarrow H^{i+j}(G, M \otimes N), \;\; i, j \geq 0 \, ,$$

are called cup-product maps. Some basic properties of them are summarized in the next result.

Proposition D.12 *The cup-product maps have the following properties:*

(i) (associativity) Let L, M and N be left $\mathbf{Z}G$-modules. Then, for any cohomology classes $\alpha \in H^i(G, L)$, $\beta \in H^j(G, M)$ and $\gamma \in H^k(G, N)$, we have $(\alpha \cup \beta) \cup \gamma = \alpha \cup (\beta \cup \gamma) \in H^{i+j+k}(G, L \otimes M \otimes N)$.

(ii) (graded-commutativity) Let M, N be left $\mathbf{Z}G$-modules. Then, for any cohomology classes $\alpha \in H^i(G, M)$ and $\beta \in H^j(G, N)$, we have $\alpha \cup \beta = (-1)^{ij} \tau_*(\beta \cup \alpha)$, where $\tau : N \otimes M \longrightarrow M \otimes N$ is the flip map.

(iii) (naturality with respect to the coefficient modules) Let M, N, M' and N' be left $\mathbf{Z}G$-modules. Then, for any $\mathbf{Z}G$-linear maps $f : M \longrightarrow M'$ and $h : N \longrightarrow N'$ there is a commutative diagram

$$\begin{array}{ccc} H^i(G, M) \otimes H^j(G, N) & \xrightarrow{\_\cup\_} & H^{i+j}(G, M \otimes N) \\ {\scriptstyle f_* \otimes h_*} \downarrow & & \downarrow {\scriptstyle (f \otimes h)_*} \\ H^i(G, M') \otimes H^j(G, N') & \xrightarrow{\_\cup\_} & H^{i+j}(G, M' \otimes N') \end{array}$$

for all $i, j \geq 0$.

(iv) (naturality with respect to the group) Let G' be another group and $\varphi : G' \longrightarrow G$ a group homomorphism. Then, for any $\mathbf{Z}G$-modules M, N there is a commutative diagram

$$\begin{array}{ccc} H^i(G, M) \otimes H^j(G, N) & \xrightarrow{\_\cup\_} & H^{i+j}(G, M \otimes N) \\ {\scriptstyle \varphi^* \otimes \varphi^*} \downarrow & & \downarrow {\scriptstyle \varphi^*} \\ H^i(G', M') \otimes H^j(G', N') & \xrightarrow{\_\cup\_} & H^{i+j}(G', M' \otimes N') \end{array}$$

for all $i, j \geq 0$. Here, $M' = M_\varphi$ and $N' = N_\varphi$ denote the $\mathbf{Z}G'$-modules obtained from M and N respectively by restriction of scalars along φ. □

In particular, let us consider a commutative ring k, viewed as a trivial G-module. Then, the multiplication $k \otimes k \longrightarrow k$ enables one to consider the composition

$$H^i(G,k) \otimes H^j(G,k) \xrightarrow{-\cup-} H^{i+j}(G, k \otimes k) \longrightarrow H^{i+j}(G,k)$$

for all $i, j \geq 0$; these maps are referred to as cup-product maps as well.

Corollary D.13 *Let k be a commutative ring.*

(i) (k-algebra structure) The cup-product maps defined above endow the cohomology $H^\bullet(G,k) = \bigoplus_i H^i(G,k)$ with the structure of an associative and graded-commutative k-algebra.

(ii) (naturality with respect to the coefficient ring) Let K be another commutative ring and $f : k \longrightarrow K$ a ring homomorphism. Then, the induced map

$$f_* : H^\bullet(G,k) \longrightarrow H^\bullet(G,K)$$

is a ring homomorphism as well.

(iii) (naturality with respect to the group) Let G' be another group and $\varphi : G' \longrightarrow G$ a group homomorphism. Then, the induced map

$$\varphi^* : H^\bullet(G,k) \longrightarrow H^\bullet(G',k)$$

is a homomorphism of k-algebras. □

Cap-products: We consider again two left $\mathbf{Z}G$-modules M, N and their tensor product $M \otimes N$ (with diagonal G-action). Let $\alpha \in H^n(G,M)$ be a cohomology class, represented by a $\mathbf{Z}G$-linear map $a : S_n \longrightarrow M$. We denote by $S_*[n]$ the complex, which is given in degree i by S_{i-n} and whose differential is $(-1)^n \delta$, and consider the composition

$$S_* \otimes_{\mathbf{Z}G} N \xrightarrow{\Delta \otimes 1} \mathrm{Tot}(S_* \otimes S_*) \otimes_{\mathbf{Z}G} N \overset{(1 \otimes a \otimes 1)^{gr}}{\longrightarrow} S_*[n] \otimes_{\mathbf{Z}G} (M \otimes N) \ ,$$

where $(1 \otimes a \otimes 1)^{gr}$ maps an elementary tensor $(x_i \otimes x_j) \otimes y \in (S_i \otimes S_j) \otimes_{\mathbf{Z}G} N$ onto the tensor $(-1)^{ni} x_i \otimes (a(x_j) \otimes y) \in S_i \otimes_{\mathbf{Z}G} (M \otimes N)$ (resp. onto 0) if $j = n$ (resp. if $j \neq n$).[1] The induced additive maps

$$\alpha \cap \_ : H_i(G,N) \longrightarrow H_{i-n}(G, M \otimes N), \ \ i \geq 0 \ ,$$

depend only upon the cohomology class α and are called cap-product maps. Some basic properties of them are summarized in the next result.

[1] Here, we regard S_* and $\mathrm{Tot}(S_* \otimes S_*)$ as complexes of right $\mathbf{Z}G$-modules by letting any element $g \in G$ act as left multiplication by g^{-1}. As such, the complexes S_* and $\mathrm{Tot}(S_* \otimes S_*)$ provide us with projective resolutions of the trivial right $\mathbf{Z}G$-module $\mathbf{Z}$; cf. the discussion at the beginning of §D.2.4.

Proposition D.14 *The cap-product maps have the following properties:*

(i) (naturality with respect to the coefficient modules) Let M, N, M' *and* N' *be left* $\mathbf{Z}G$*-modules. Then, for any* $\mathbf{Z}G$*-linear maps* $f : M \longrightarrow M'$ *and* $h : N \longrightarrow N'$ *and any cohomology class* $\alpha \in H^n(G, M)$ *there is a commutative diagram*

$$\begin{array}{ccc} H_i(G,N) & \stackrel{\alpha\cap\_}{\longrightarrow} & H_{i-n}(G, M\otimes N) \\ {\scriptstyle h_*}\downarrow & & \downarrow {\scriptstyle (f\otimes h)_*} \\ H_i(G,N') & \stackrel{f_*\alpha\cap\_}{\longrightarrow} & H_{i-n}(G, M'\otimes N') \end{array}$$

for all $i \geq 0$.

(ii) (naturality with respect to the group) Let G' *be another group and* $\varphi : G' \longrightarrow G$ *a group homomorphism. Then, for any left* $\mathbf{Z}G$*-modules* M, N *and any cohomology class* $\alpha \in H^n(G, M)$ *there is a commutative diagram*

$$\begin{array}{ccc} H_i(G',N') & \stackrel{\varphi^*\alpha\cap\_}{\longrightarrow} & H_{i-n}(G', M'\otimes N') \\ {\scriptstyle \varphi_*}\downarrow & & \downarrow {\scriptstyle \varphi_*} \\ H_i(G,N) & \stackrel{\alpha\cap\_}{\longrightarrow} & H_{i-n}(G, M\otimes N) \end{array}$$

for all $i \geq 0$*. Here,* $M' = M_\varphi$ *and* $N' = N_\varphi$ *denote the* $\mathbf{Z}G'$*-modules obtained from* M *and* N *respectively by restriction of scalars along* φ*.*

(iii) (composition) Let L, M *and* N *be left* $\mathbf{Z}G$*-modules. Then, for any cohomology classes* $\alpha \in H^n(G, M)$ *and* $\beta \in H^m(G, L)$*, the composition*

$$H_i(G,N) \stackrel{\alpha\cap\_}{\longrightarrow} H_{i-n}(G, M\otimes N) \stackrel{\beta\cap\_}{\longrightarrow} H_{i-n-m}(G, L\otimes M\otimes N)$$

coincides with the cap-product map

$$\gamma\cap\_ : H_i(G,N) \longrightarrow H_{i-n-m}(G, L\otimes M\otimes N) \, ,$$

where $\gamma = \beta \cup \alpha \in H^{n+m}(G, L\otimes M)$*, for all* $i \geq 0$. □

In particular, let k be a commutative ring (viewed as a trivial G-module) and $\alpha \in H^n(G, k)$ a cohomology class. Then, we may consider for all $i \geq 0$ the composition

$$H_i(G,k) \stackrel{\alpha\cap\_}{\longrightarrow} H_{i-n}(G, k\otimes k) \longrightarrow H_{i-n}(G,k) \, ,$$

where the latter map is induced by the multiplication of k. These maps are referred to as cap-product maps as well.

Corollary D.15 *Let* k *be a commutative ring.*

(i) (naturality with respect to the coefficient ring) Let K *be another commutative ring and* $f : k \longrightarrow K$ *a ring homomorphism. Then, for any cohomology class* $\alpha \in H^n(G, k)$ *there is a commutative diagram*

$$\begin{array}{ccc} H_i(G,k) & \stackrel{\alpha\cap\_}{\longrightarrow} & H_{i-n}(G,k) \\ {\scriptstyle f_*}\downarrow & & \downarrow {\scriptstyle f_*} \\ H_i(G,K) & \stackrel{\alpha_K\cap\_}{\longrightarrow} & H_{i-n}(G,K) \end{array}$$

for all $i \geq 0$. *Here,* $\alpha_K = f_*\alpha$ *is the image of* α *in the cohomology group* $H^n(G, K)$.

(ii) (naturality with respect to the group) Let G' *be another group and* $\varphi : G' \longrightarrow G$ *a group homomorphism. Then, for any cohomology class* $\alpha \in H^n(G, k)$ *there is a commutative diagram*

$$\begin{array}{ccc} H_i(G', k) & \xrightarrow{\alpha' \cap \_} & H_{i-n}(G', k) \\ \varphi_* \downarrow & & \downarrow \varphi_* \\ H_i(G, k) & \xrightarrow{\alpha \cap \_} & H_{i-n}(G, k) \end{array}$$

for all $i \geq 0$. *Here,* $\alpha' = \varphi^*\alpha$ *is the image of* α *in the cohomology group* $H^n(G', k)$.

(iii) (composition) For any cohomology classes $\alpha \in H^n(G, k)$ *and* $\beta \in H^m(G, k)$, *the composition*

$$H_i(G, k) \xrightarrow{\alpha \cap \_} H_{i-n}(G, k) \xrightarrow{\beta \cap \_} H_{i-n-m}(G, k)$$

coincides with the cap-product map

$$\gamma \cap \_ : H_i(G, k) \longrightarrow H_{i-n-m}(G, k) \, ,$$

where $\gamma = \beta \cup \alpha \in H^{n+m}(G, k)$, *for all* $i \geq 0$. □

D.2.4 Duality

In this subsection, we briefly investigate the extent to which group cohomology is dual to group homology.

We fix a commutative ring k and a group G. First of all, we define the (co-)homology groups of G with coefficients in right kG-modules. To that end, we consider the involution

$$\tau : kG \longrightarrow kG$$

of the k-algebra kG, which is defined by letting $\tau(g) = g^{-1}$ for all $g \in G$. If U is a right kG-module, we let $\widetilde{U}$ be the left kG-module obtained from U by pulling back its right kG-module structure along τ. In other words, we define $g \cdot u = ug^{-1}$ for all $g \in G$ and $u \in U$. Then, the (co-)homology of G with coefficients in U is defined as the (co-)homology of G with coefficients in $\widetilde{U}$. We note that the right kG-module U is projective if and only if the left kG-module $\widetilde{U}$ is projective. Moreover, if U' is another right kG-module then a k-linear map $f : U \longrightarrow U'$ is a homomorphism of right kG-modules if and only if the map $f : \widetilde{U} \longrightarrow \widetilde{U'}$ is a homomorphism of left kG-modules. Therefore, we conclude that

$$\text{Hom}_{kG}(U, U') = \text{Hom}_{kG}\left(\widetilde{U}, \widetilde{U'}\right) \, .$$

It follows that the cohomology groups $H^n(G, U)$, $n \geq 0$, of G with coefficients in the right kG-module U can be computed using a resolution

$$0 \longleftarrow k \overset{\varepsilon}{\longleftarrow} P_*$$

of k by projective right kG-modules, as the cohomology of the cochain complex $\mathrm{Hom}_{kG}(P_*, U)$. In a similar way, it turns out that the homology groups $H_n(G,U)$, $n \geq 0$, of G with coefficients in the right kG-module U can be computed using a resolution

$$0 \longleftarrow k \overset{\varepsilon}{\longleftarrow} Q_*$$

of k by projective left kG-modules, as the homology of the chain complex $U \otimes_{kG} Q_*$.

We now consider a left kG-module M and a k-module J. Then, the k-module $U = \mathrm{Hom}_k(M, J)$ has a natural structure of a right kG-module, which is obtained by using the left G-action on M (cf. Exercise 1.3.1(i)). If

$$0 \longleftarrow k \overset{\varepsilon}{\longleftarrow} P_*$$

is a resolution of k by projective right kG-modules, then there is a natural identification of cochain complexes

$$\mathrm{Hom}_{kG}(P_*, \mathrm{Hom}_k(M, J)) \overset{\sim}{\longrightarrow} \mathrm{Hom}_k(P_* \otimes_{kG} M, J)$$

(cf. Exercise 1.3.1(iii)). In this way, we obtain k-linear maps

$$\theta_{G,M,J} : H^n(G, \mathrm{Hom}_k(M, J)) \longrightarrow \mathrm{Hom}_k(H_n(G, M), J)$$

for all $n \geq 0$ (cf. Example D.3(ii)).

Proposition D.16 *Let M be a left kG-module, J a k-module and consider the k-linear maps $\theta = \theta_{G,M,J}$ defined above.*

(i) For any cohomology class $\alpha \in H^n(G, Hom_k(M, J))$ the k-linear map $\theta(\alpha) \in Hom_k(H_n(G, M), J)$ is the composition

$$H_n(G, M) \overset{\alpha \cap -}{\longrightarrow} H_0\Big(G, \widetilde{Hom_k(M, J)} \otimes M\Big) = Hom_k(M, J) \otimes_{kG} M \overset{ev}{\longrightarrow} J \ ,$$

where ev denotes the evaluation homomorphism.

(ii) If J is an injective k-module, then θ is an isomorphism for all n. □

Corollary D.17 *Assume that k is a field, viewed as a trivial G-module. Then, there is an isomorphism $H^n(G, k) \simeq Hom_k(H_n(G, k), k)$, which identifies a cohomology class $\alpha \in H^n(G, k)$ with the cap-product map*

$$\alpha \cap \_ : H_n(G, k) \longrightarrow H_0(G, k) = k$$

for all $n \geq 0$. □

D.2.5 The (co-)homology of an Extension

Let us now consider a group G, a normal subgroup $N \trianglelefteq G$ and the corresponding quotient $Q = G/N$. Our goal is to describe the relationship between the (co-)homology groups of G with coefficients in a $\mathbf{Z}G$-module M and certain (co-)homology groups of N and Q. This relationship can be properly described by using the notion of a spectral sequence. Instead of giving the details of the construction of the Lyndon-Hochschild-Serre spectral sequence, we adopt an ad hoc point of view and state a few results that make the techniques used in Chap. 4 intelligible.

Our first objective is to compute the homology groups $H_n(G, M)$, $n \geq 0$. We denote by M' the $\mathbf{Z}N$-module obtained from M by restriction of scalars and consider the homology groups $H_j(N, M')$, $j \geq 0$. For any $g \in G$ we let $I_g \in \mathrm{Aut}(N)$ be the conjugation by g and define $M'_g = M'_{I_g}$ to be the $\mathbf{Z}N$-module obtained from M' by restriction of scalars along I_g. If

$$\lambda_g : M' \longrightarrow M'_g$$

is the $\mathbf{Z}N$-linear map, which is defined by letting $\lambda_g(x) = gx$ for all $x \in M'$, then the composition

$$H_j(N, M') \xrightarrow{(\lambda_g)_*} H_j\big(N, M'_g\big) \xrightarrow{(I_g)_*} H_j(N, M')$$

is an additive endomorphism ϱ_g of the group $H_j(N, M')$. In this way, we obtain an action ϱ of G on the homology group $H_j(N, M')$. This action being trivial on N (cf. Remark D.7(ii)), we conclude that the group $H_j(N, M')$ admits a natural $\mathbf{Z}Q$-module structure for all $j \geq 0$. In particular, we may consider the homology groups $H_i(Q, H_j(N, M'))$ for all $i, j \geq 0$.

Theorem D.18 *Let G be a group, $N \trianglelefteq G$ a normal subgroup and $Q = G/N$ the corresponding quotient. We consider a $\mathbf{Z}G$-module M and let M' be the $\mathbf{Z}N$-module obtained from M by restriction of scalars. Then, for all $n \geq 0$ the homology group $H_n(G, M)$ admits a natural increasing filtration*

$$0 = F_{-1}H_n \subseteq F_0H_n \subseteq F_1H_n \subseteq \cdots \subseteq F_{n-1}H_n \subseteq F_nH_n = H_n(G, M) ,$$

having the following properties:

(i) The group $F_pH_n/F_{p-1}H_n$ is a certain subquotient of the homology group $H_p(Q, H_{n-p}(N, M'))$ for all p, n.

(ii) The group F_0H_n is the image of the map

$$H_n(N, M') \longrightarrow H_n(G, M) ,$$

which is induced by the inclusion $N \hookrightarrow G$.

(iii) The group $F_{n-1}H_n$ is the kernel of the map

$$H_n(G, M) \longrightarrow H_n(Q, M_N) ,$$

which is induced by the natural maps $G \longrightarrow Q$ and $M \longrightarrow M_N$. □

Corollary D.19 *Let k be a commutative ring, G a group, $N \trianglelefteq G$ a normal subgroup and $Q = G/N$ the corresponding quotient. If the groups N, Q have finite homological dimension over k, then G has also finite homological dimension over k; in fact, $hd_k G \leq hd_k N + hd_k Q$.* □

There is a result analogous to Theorem D.18 for the cohomology groups of G with coefficients in M. As in the homology case, the conjugation action of G induces a natural $\mathbf{Z}Q$-module structure on the groups $H^j(N, M')$. More precisely, for any element $g \in G$ the action of $q = gN \in Q$ on $H^j(N, M')$ is given by the composition

$$H^j(N, M') \xrightarrow{(\lambda_g)_*} H^j\left(N, M'_g\right) \xrightarrow{[(I_g)^*]^{-1}} H^j(N, M') \,,$$

where M'_g, λ_g and I_g are defined as above.[2] In this way, we may consider the cohomology groups $H^i(Q, H^j(N, M'))$ for all $i, j \geq 0$.

Theorem D.20 *Let G be a group, $N \trianglelefteq G$ a normal subgroup and $Q = G/N$ the corresponding quotient. We consider a $\mathbf{Z}G$-module M and let M' be the $\mathbf{Z}N$-module obtained from M by restriction of scalars. Then, for all $n \geq 0$ the cohomology group $H^n(G, M)$ admits a natural decreasing filtration*

$$H^n(G, M) = F^0 H^n \supseteq F^1 H^n \supseteq \cdots \supseteq F^n H^n \supseteq F^{n+1} H^n = 0 \,,$$

having the following properties:

(i) The group $F^p H^n / F^{p+1} H^n$ is a certain subquotient of the cohomology group $H^p(Q, H^{n-p}(N, M'))$ for all p, n.

(ii) The group $F^1 H^n$ is the kernel of the map

$$H^n(G, M) \longrightarrow H^n(N, M') \,,$$

which is induced by the inclusion $N \hookrightarrow G$.

(iii) The group $F^n H^n$ is the image of the map

$$H^n\left(Q, M^N\right) \longrightarrow H^n(G, M) \,,$$

which is induced by the natural maps $G \longrightarrow Q$ and $M^N \hookrightarrow M$.

(iv) Assume that $M = k$ is a commutative ring, viewed as a trivial $\mathbf{Z}G$-module. Then, for any cohomology classes $\alpha \in F^p H^n$ and $\alpha' \in F^{p'} H^{n'}$ we have $\alpha \cup \alpha' \in F^{p+p'} H^{n+n'}$. □

We conclude our discussion with two results concerning the special cases of an extension as above, where the normal subgroup $N \trianglelefteq G$ is either finite or infinite cyclic.

---

[2] We note that the $\mathbf{Z}Q$-module structures defined on the (co-)homology groups of N with coefficients in M' are compatible with the duality maps θ; cf. Exercise D.3.6.

Proposition D.21 *Let k be a field of characteristic 0 and $\pi : G \longrightarrow Q$ a surjective group homomorphism with finite kernel. We consider a kQ-module V and let V_π be the kG-module obtained from V by restriction of scalars along π. Then, the natural maps*

$$\pi_* : H_n(G, V_\pi) \longrightarrow H_n(Q, V) \quad \textit{and} \quad \pi^* : H^n(Q, V) \longrightarrow H^n(G, V_\pi)$$

are isomorphisms for all $n \geq 0$. □

Proposition D.22 *Let*

$$1 \longrightarrow \mathbf{Z} \longrightarrow G \xrightarrow{\pi} Q \longrightarrow 1$$

be a central extension and $\alpha \in H^2(Q, \mathbf{Z})$ the corresponding cohomology class.[3] *We consider a $\mathbf{Z}Q$-module V and let V_π be the $\mathbf{Z}G$-module obtained from V by restriction of scalars along π. Then, there are exact sequences*

$$H_n(G, V_\pi) \xrightarrow{\pi_*} H_n(Q, V) \xrightarrow{\alpha \cap \_} H_{n-2}(Q, V) \longrightarrow H_{n-1}(G, V_\pi)$$

for all $n \geq 0$. □

D.3 Exercises

1. Let G be an abelian group. The goal of this Exercise is to prove that G has finite homological dimension over $\mathbf{Q}$ if and only if it has finite rank.
   (i) If $T \subseteq G$ is a torsion subgroup, then show that $\text{hd}_{\mathbf{Q}} T = 0$ and hence conclude that $\text{hd}_{\mathbf{Q}} G \leq \text{hd}_{\mathbf{Q}}(G/T)$.
   (ii) If $G = \mathbf{Z}^n$, show that $\text{hd}_k G = n$ for any commutative ring k.
   (iii) If $G = \mathbf{Q}^n$, show that $\text{hd}_k G = n$ for any commutative ring k.
   (iv) If G has finite rank, show that G has finite homological dimension over $\mathbf{Q}$.
   (v) If G is an abelian group of infinite rank, then show that G does not have finite homological dimension over any commutative ring k.
2. (i) Let (C, d), (C', d') and (C'', d'') be chain complexes of abelian groups. Show that the associativity isomorphisms

   $$(C_i \otimes C'_j) \otimes C''_k \simeq C_i \otimes (C'_j \otimes C''_k), \quad i, j, k \geq 0 \ ,$$

   induce an isomorphism of chain complexes

   $$\text{Tot}(\text{Tot}(C \otimes C') \otimes C'') \simeq \text{Tot}(C \otimes \text{Tot}(C' \otimes C'')) \ .$$

   We view this isomorphism as an identification and denote the resulting chain complex by $\text{Tot}(C \otimes C' \otimes C'')$.

[3] We note that Q acts trivially on $\mathbf{Z}$, since the extension is assumed to be central.

(ii) (coassociativity of the Alexander-Whitney map) Let G be a group and $S_* = (S_*(G,\mathbf{Z}),\delta)$ the standard resolution of the trivial G-module $\mathbf{Z}$. Show that the Alexander-Whitney map

$$\Delta : S_* \longrightarrow \mathrm{Tot}(S_* \otimes S_*)$$

induces a commutative diagram

$$\begin{array}{ccc} S_* & \stackrel{\Delta}{\longrightarrow} & \mathrm{Tot}(S_* \otimes S_*) \\ {\scriptstyle\Delta}\downarrow & & {\scriptstyle Tot(\Delta\otimes 1)}\downarrow \\ \mathrm{Tot}(S_* \otimes S_*) & \stackrel{Tot(1\otimes\Delta)}{\longrightarrow} & \mathrm{Tot}(S_* \otimes S_* \otimes S_*) \end{array}$$

(iii) (existence of counit for the Alexander-Whitney map) Let G be a group and $S_* = (S_*(G,\mathbf{Z}),\delta)$ the standard resolution of the trivial G-module $\mathbf{Z}$. Note that $S_0 = \mathbf{Z}G$ and define

$$\varepsilon : S_* \longrightarrow \mathbf{Z}[0]$$

to be the chain map which is given by the usual augmentation in degree 0 and vanishes in positive degrees. Show that there is a commutative diagram

$$\begin{array}{ccccc} \mathrm{Tot}(S_* \otimes S_*) & \stackrel{\Delta}{\longleftarrow} & S_* & \stackrel{\Delta}{\longrightarrow} & \mathrm{Tot}(S_* \otimes S_*) \\ {\scriptstyle Tot(\varepsilon\otimes 1)}\downarrow & & \| & & \downarrow{\scriptstyle Tot(1\otimes\varepsilon)} \\ \mathrm{Tot}(\mathbf{Z}[0] \otimes S_*) & \simeq & S_* & \simeq & \mathrm{Tot}(S_* \otimes \mathbf{Z}[0]) \end{array}$$

where Δ is the Alexander-Whitney map.

3. Let G be a group and $S_* = (S_*(G,\mathbf{Z}),\delta)$ the standard resolution of the trivial G-module $\mathbf{Z}$. We consider three $\mathbf{Z}G$-modules L, M and N and two cohomology classes $\alpha \in H^n(G,M)$ and $\beta \in H^m(G,L)$. The goal of this Exercise is to prove Proposition D.14(iii). To that end, let us fix representatives $a : S_n \longrightarrow M$ and $b : S_m \longrightarrow L$ of α and β respectively and consider the representative $c = b \cup a : S_{n+m} \longrightarrow L \otimes M$ of $\gamma = \beta \cup \alpha \in H^{n+m}(G, L \otimes M)$.
(i) Show that the following diagram is commutative

$$\begin{array}{ccc} \mathrm{Tot}(S_* \otimes S_*) \otimes_{\mathbf{Z}G} N & \stackrel{(1\otimes a\otimes 1)^{gr}}{\longrightarrow} & S_*[n] \otimes_{\mathbf{Z}G} (M \otimes N) \\ {\scriptstyle Tot(\Delta\otimes 1)\otimes 1}\downarrow & & \downarrow{\scriptstyle \Delta\otimes 1\otimes 1} \\ \mathrm{Tot}(S_* \otimes S_* \otimes S_*) \otimes_{\mathbf{Z}G} N & \stackrel{(1\otimes 1\otimes a\otimes 1)^{gr}}{\longrightarrow} & \mathrm{Tot}(S_* \otimes S_*)[n] \otimes_{\mathbf{Z}G} (M \otimes N) \end{array}$$

Here, $(1 \otimes 1 \otimes a \otimes 1)^{gr}$ maps an elementary tensor $(x_i \otimes x_j \otimes x_k) \otimes y \in (S_i \otimes S_j \otimes S_k) \otimes_{\mathbf{Z}G} N$ onto the tensor $(-1)^{ni+nj}(x_i \otimes x_j) \otimes (a(x_k) \otimes y) \in (S_i \otimes S_j) \otimes_{\mathbf{Z}G} (M \otimes N)$ (resp. onto 0) if $k = n$ (resp. if $k \neq n$).
(ii) Show that the composition

$$H_i(G,N) \stackrel{\alpha\cap\_}{\longrightarrow} H_{i-n}(G, M \otimes N) \stackrel{\beta\cap\_}{\longrightarrow} H_{i-n-m}(G, L \otimes M \otimes N)$$

is induced by the composition

$$S_* \otimes_{\mathbf{Z}G} N \longrightarrow \mathrm{Tot}(S_* \otimes S_* \otimes S_*) \otimes_{\mathbf{Z}G} N \longrightarrow S_*[n+m] \otimes_{\mathbf{Z}G} (L \otimes M \otimes N) \ ,$$

where the first chain map is $(\mathrm{Tot}(\Delta \otimes 1) \circ \Delta) \otimes 1$ and the second one is $(1 \otimes b \otimes a \otimes 1)^{gr}$. Here, $(1 \otimes b \otimes a \otimes 1)^{gr}$ maps an elementary tensor $(x_i \otimes x_j \otimes x_k) \otimes y \in (S_i \otimes S_j \otimes S_k) \otimes_{\mathbf{Z}G} N$ onto $(-1)^{ni+nj+mi} x_i \otimes (b(x_j) \otimes a(x_k) \otimes y) \in S_i \otimes_{\mathbf{Z}G} (L \otimes M \otimes N)$ (resp. onto 0) if $j = m$ and $k = n$ (resp. if $j \neq m$ or $k \neq n$).
(iii) Show that the cap-product map

$$\gamma \cap \_ : H_i(G, N) \longrightarrow H_{i-n-m}(G, L \otimes M \otimes N)$$

is induced by the composition

$$S_* \otimes_{\mathbf{Z}G} N \longrightarrow \mathrm{Tot}(S_* \otimes S_* \otimes S_*) \otimes_{\mathbf{Z}G} N \longrightarrow S_*[n+m] \otimes_{\mathbf{Z}G} (L \otimes M \otimes N) \ ,$$

where the first chain map is $(\mathrm{Tot}(1 \otimes \Delta) \circ \Delta) \otimes 1$ and the second one is $(1 \otimes b \otimes a \otimes 1)^{gr}$.
(iv) Prove Proposition D.14(iii).
(*Hint:* Use the coassociativity of Δ; cf. Exercise 2(ii) above.)

4. Let G be a group and $S_* = (S_*(G, \mathbf{Z}), \delta)$ the standard resolution of the trivial G-module $\mathbf{Z}$. We consider a left $\mathbf{Z}G$-module M, an abelian group J and the right $\mathbf{Z}G$-module $U = \mathrm{Hom}_{\mathbf{Z}}(M, J)$. The goal of this Exercise is to prove Proposition D.16(i), in the case where the coefficient ring k therein is that of integers (the proof for a general k is similar). To that end, let us fix a cohomology class $\alpha \in H^n(G, U)$, represented by a homomorphism $a : S_n \longrightarrow U$ of right $\mathbf{Z}G$-modules.
(i) Show that the map

$$(1 \otimes a \otimes 1)^{gr} : \mathrm{Tot}(S_* \otimes S_*)_n \otimes_{\mathbf{Z}G} M \longrightarrow S_0 \otimes_{\mathbf{Z}G} \left(\widetilde{U} \otimes M \right) \ ,$$

followed by the natural quotient map

$$S_0 \otimes_{\mathbf{Z}G} \left(\widetilde{U} \otimes M \right) \simeq \widetilde{U} \otimes M \longrightarrow U \otimes_{\mathbf{Z}G} M \ ,$$

coincides with the composition

$$\mathrm{Tot}(S_* \otimes S_*)_n \otimes_{\mathbf{Z}G} M \stackrel{\widetilde{\varepsilon} \otimes 1}{\longrightarrow} S_n \otimes_{\mathbf{Z}G} M \stackrel{a \otimes 1}{\longrightarrow} U \otimes_{\mathbf{Z}G} M \ .$$

Here, $\widetilde{\varepsilon}$ denotes the map

$$\mathrm{Tot}(\varepsilon \otimes 1) : \mathrm{Tot}(S_* \otimes S_*)_n \longrightarrow \mathrm{Tot}(\mathbf{Z}[0] \otimes S_*)_n \simeq S_n \ ,$$

where ε is the counit defined in Exercise 2(iii) above.

(ii) Show that the cap-product map

$$\alpha \cap \_ : H_n(G,M) \longrightarrow H_0\Big(G, \widetilde{U} \otimes M\Big)$$

is induced by the additive map

$$a \otimes 1 : S_n \otimes_{\mathbf{Z}G} M \longrightarrow U \otimes_{\mathbf{Z}G} M = H_0\Big(G, \widetilde{U} \otimes M\Big) .$$

(iii) Prove Proposition D.16(i), in the case where $k = \mathbf{Z}$.

5. The goal of this Exercise is to show that the duality homomorphisms $\theta_{G,M,J}$ of Proposition D.16 are natural with respect to the group G, the coefficient module M and the dualizing module J.

(i) (naturality with respect to the group) Let k be a commutative ring, $\phi : G' \longrightarrow G$ a group homomorphism, M a left kG-module and J a k-module. We denote by M' the left kG'-module obtained from M by restriction of scalars along ϕ and consider the right kG-module $U = \mathrm{Hom}_k(M,J)$. Then, the right kG'-module U' obtained from U by restriction of scalars along ϕ is identified with $\mathrm{Hom}_k(M',J)$. Show that the following diagram is commutative for all $n \geq 0$

$$\begin{array}{ccc} H^n(G,U) & \xrightarrow{\phi^*} & H^n(G',U') \\ \theta_{G,M,J} \downarrow & & \downarrow \theta_{G',M',J} \\ \mathrm{Hom}_k(H_n(G,M),J) & \xrightarrow{(\phi_*)^t} & \mathrm{Hom}_k(H_n(G',M'),J) \end{array}$$

Here, $(\phi_*)^t$ denotes the transpose of $\phi_* : H_n(G',M') \longrightarrow H_n(G,M)$.

(ii) (naturality with respect to the coefficient module) Let k be a commutative ring, G a group, $f : M' \longrightarrow M$ a homomorphism of left kG-modules and J a k-module. We consider the right kG-modules $U' = \mathrm{Hom}_k(M',J)$ and $U = \mathrm{Hom}_k(M,J)$ and note that the transpose $F = f^t : U \longrightarrow U'$ of f is kG-linear. Show that the following diagram is commutative for all $n \geq 0$

$$\begin{array}{ccc} H^n(G,U) & \xrightarrow{F_*} & H^n(G,U') \\ \theta_{G,M,J} \downarrow & & \downarrow \theta_{G,M',J} \\ \mathrm{Hom}_k(H_n(G,M),J) & \xrightarrow{(f_*)^t} & \mathrm{Hom}_k(H_n(G,M'),J) \end{array}$$

Here, $(f_*)^t$ denotes the transpose of $f_* : H_n(G,M') \longrightarrow H_n(G,M)$.

(iii) (naturality with respect to the dualizing module) Let k be a commutative ring, G a group, M a left kG-module and $\tau : J \longrightarrow J'$ a homomorphism of k-modules. We consider the right kG-modules $U = \mathrm{Hom}_k(M,J)$ and $U' = \mathrm{Hom}_k(M,J')$ and note that the induced map $T = \tau_* : U \longrightarrow U'$ is kG-linear. Show that the following diagram is commutative for all $n \geq 0$

$$\begin{array}{ccc} H^n(G,U) & \xrightarrow{T_*} & H^n(G,U') \\ \theta_{G,M,J} \downarrow & & \downarrow \theta_{G,M,J'} \\ \mathrm{Hom}_k(H_n(G,M),J) & \xrightarrow{\tau_*} & \mathrm{Hom}_k(H_n(G,M),J') \end{array}$$

Here, the map τ_* in the bottom row is that induced by τ between the Hom-groups.

6. Let G be a group, $N \trianglelefteq G$ a normal subgroup and $Q = G/N$. The goal of this Exercise is to show that the $\mathbf{Z}Q$-module structures defined in §D.2.5 on the (co-)homology groups of N with coefficients in restricted $\mathbf{Z}G$-modules are compatible with the duality homomorphisms θ of Proposition D.16. To that end, we consider a left $\mathbf{Z}G$-module M, an abelian group J and the right $\mathbf{Z}G$-module $U = \mathrm{Hom}_{\mathbf{Z}}(M, J)$. We fix an element $g \in G$ and let $q = gN \in Q$.
(i) Show that the left $\mathbf{Z}Q$-module structure on $H_n(N, M')$ defined in the text induces a right $\mathbf{Z}Q$-module structure on the abelian group $\mathrm{Hom}_{\mathbf{Z}}(H_n(N, M'), J)$, in such a way that $q \in Q$ acts as the composition of the transpose

$$((I_g)_*)^t : \mathrm{Hom}_{\mathbf{Z}}(H_n(N, M'), J) \longrightarrow \mathrm{Hom}_{\mathbf{Z}}\big(H_n\big(N, M'_g\big), J\big)$$

of $(I_g)_* : H_n\big(N, M'_g\big) \longrightarrow H_n(N, M')$, followed by the transpose

$$((\lambda_g)_*)^t : \mathrm{Hom}_{\mathbf{Z}}\big(H_n\big(N, M'_g\big), J\big) \longrightarrow \mathrm{Hom}_{\mathbf{Z}}(H_n(N, M'), J)$$

of $(\lambda_g)_* : H_n(N, M') \longrightarrow H_n\big(N, M'_g\big)$.
(ii) Show that the right $\mathbf{Z}N$-module U'_g obtained from the right $\mathbf{Z}N$-module $U' = \mathrm{Hom}_{\mathbf{Z}}(M', J)$ by restriction of scalars along the automorphism $I_g : N \longrightarrow N$ is identified with $\mathrm{Hom}_{\mathbf{Z}}\big(M'_g, J\big)$, whereas the transpose

$$\rho_g : U'_g \longrightarrow U'$$

of the map $\lambda_g : M' \longrightarrow M'_g$ defined in the text is a homomorphism of right $\mathbf{Z}G$-modules.
(iii) Show that the cohomology group $H^n(N, U')$ admits a right $\mathbf{Z}Q$-module structure, in such a way that $q \in Q$ acts as the composition

$$H^n(N, U') \xrightarrow{(I_g)^*} H^n\big(N, U'_g\big) \xrightarrow{(\rho_g)_*} H^n(N, U') \ .$$

(iv) Show that the duality homomorphism

$$\theta_{N,M',J} : H^n(N, U') \longrightarrow \mathrm{Hom}_{\mathbf{Z}}(H_n(N, M'), J)$$

is a homomorphism of right $\mathbf{Z}Q$-modules for all $n \geq 0$.
(*Hint:* Use the naturality of θ with respect to the group and the coefficient module; cf. Exercise 5(i),(ii) above.)

E

Comparison of Projections

In this Appendix, we examine a few basic properties of the lattice of projections in a von Neumann algebra $\mathcal{N}$. We begin by reviewing the concepts of equivalence and weak ordering and then consider the notion of the central carrier of a projection. Our main goal is to prove the comparison theorem, which states that any two projections in $\mathcal{N}$ can be cut by a central projection into comparable sub-projections (for the precise statement, see Theorem E.7). This fact was used in a crucial way in §5.2.2, in order to prove the injectivity of the additive map t_*, which is induced in K-theory by the center-valued trace t on the von Neumann algebra of a group.

Of course, our presentation here is very limited, aiming only at those results that are necessary for the proof of the comparison theorem. For a more complete treatment of the structure theory of projections in a von Neumann algebra, the reader may consult specialized books on the subject, such as [18] and [36].

E.1 Equivalence and Weak Ordering

Let $\mathcal{B}(\mathcal{H})$ be the algebra of bounded linear operators on a Hilbert space $\mathcal{H}$. Any projection $e \in \mathcal{B}(\mathcal{H})$ is completely determined by its range $V = \operatorname{im} e$, which is a closed linear subspace of $\mathcal{H}$; indeed, e maps identically V onto itself and vanishes on the orthogonal complement $V^\perp$. Conversely, for any closed linear subspace $V \subseteq \mathcal{H}$ there is a (unique) projection in $\mathcal{B}(\mathcal{H})$ whose range is V; we denote that projection by p_V. Two projections e, f are orthogonal (i.e. $ef = 0$) if and only if $\operatorname{im} e \perp \operatorname{im} f$. If e, f are two commuting projections, then ef is the projection onto the subspace $\operatorname{im} e \cap \operatorname{im} f$. Given two projections e and f, we write $e \leq f$ if $ef = fe = e$ (cf. §1.1.1.II); in that case, the (closed) subspace $\operatorname{im} e$ is contained in $\operatorname{im} f$, whereas the operator $f - e$ is the orthogonal projection onto the subspace $(\operatorname{im} e)^\perp \cap \operatorname{im} f$. If e, f, c are projections in $\mathcal{B}(\mathcal{H})$, such that $e \leq f$ and c commutes with both e and f, then $ce \leq cf$. The correspondence $V \mapsto p_V$ defines an isomorphism of lattices between the lattice of closed subspaces of $\mathcal{H}$ and that of projections in $\mathcal{B}(\mathcal{H})$. For example, if $(e_i)_i$ is a family of projections and $V_i = \operatorname{im} e_i$ for all i, then the supremum $e = \sup_i e_i$ is the projection onto the closed linear subspace V of $\mathcal{H}$, which is generated by the V_i's (i.e. $V = \overline{\sum_i V_i}$). In the special case where the e_i's are orthogonal to each other, V is the orthogonal direct sum of the V_i's and $e = \sum_i e_i$.[1]

Recall that a linear operator $u \in \mathcal{B}(\mathcal{H})$ is called a partial isometry if there are closed linear subspaces $V, V' \subseteq \mathcal{H}$, such that u maps V isometrically onto V' and vanishes on the orthogonal complement $V^\perp$. In that case, the adjoint u^* maps V' isometrically onto V and vanishes on the orthogonal complement $V'^\perp$; therefore, we have $u^*u = p_V$ and $uu^* = p_{V'}$.[2] Let $e = p_V$ and $e' = p_{V'}$ be two projections in $\mathcal{B}(\mathcal{H})$. Then, the existence of a partial isometry u, such that $u^*u = e$ and $uu^* = e'$, is easily seen to be equivalent to the condition $\dim V = \dim V'$, where dim denotes the Hilbert space dimension.

We work with a fixed von Neumann algebra $\mathcal{N}$ of operators acting on the Hilbert space $\mathcal{H}$.

Lemma E.1 *The following conditions are equivalent for a closed subspace $V \subseteq \mathcal{H}$:*

(i) $p_V \in \mathcal{N}$,
(ii) the subspaces V and $V^\perp$ are $\mathcal{N}'$-invariant and
(iii) the subspace V is $\mathcal{N}'$-invariant.

Proof. (i)→(ii): For any vector $\xi \in V$ and any operator $a \in \mathcal{N}'$ we have $a(\xi) = ap_V(\xi) = p_V a(\xi) \in \operatorname{im} p_V = V$; therefore, V is $\mathcal{N}'$-invariant. The same argument, applied to the complementary projection $1 - p_V$, shows that $V^\perp = \operatorname{im}(1 - p_V)$ is $\mathcal{N}'$-invariant as well.

(ii)→(iii): This is obvious.

(iii)→(i): In view of Lemma 1.17(ii), the $\mathcal{N}'$-invariance of V implies that the projection p_V is contained in $\mathcal{N}'' = \mathcal{N}$. □

Corollary E.2 *Let $(e_i)_i$ be a family of projections in $\mathcal{N}$. If $e \in \mathcal{B}(\mathcal{H})$ is the supremum of the e_i's, then $e \in \mathcal{N}$. In particular, if $e_i e_j = 0$ for $i \neq j$, then $\sum_i e_i \in \mathcal{N}$.*

Proof. Since $e_i \in \mathcal{N}$, Lemma E.1 implies that the subspace $V_i = \operatorname{im} e_i$ is $\mathcal{N}'$-invariant for all i. Then, the closed linear subspace $V = \overline{\sum_i V_i}$ is easily seen to be $\mathcal{N}'$-invariant as well. The result follows from another application of Lemma E.1, since $e = p_V$. □

We recall that two projections $e, f \in \mathcal{N}$ are called equivalent rel $\mathcal{N}$ if there is a partial isometry $u \in \mathcal{N}$, such that $e = u^*u$ and $f = uu^*$; in that case, we write $e \sim f$. Equivalently, $e \sim f$ if there is a partial isometry $u \in \mathcal{N}$, which maps $\operatorname{im} e$ isometrically onto $\operatorname{im} f$ and vanishes on the orthogonal complement

[1] Here, the infinite sum is understood as the SOT-limit of the net of finite sums.
[2] An algebraic description of partial isometries is provided in Exercise E.2.1.

$(\operatorname{im} e)^{\perp}$. It follows easily that the *equivalence rel* $\mathcal{N}$ is indeed an equivalence relation. We now state and prove a few basic properties of that relation, that are needed in the sequel.

Proposition E.3 *(i) Assume that $e, f \in \mathcal{N}$ are projections with $e \sim f$. Then, for any central projection $c \in \mathcal{N}$ we have $ce \sim cf$.*

(ii) Consider an operator $a \in \mathcal{N}$ and let V (resp. U) be the closure of the range $\operatorname{im} a$ of a (resp. of the range $\operatorname{im} a^*$ of a^*). Then, $p_V, p_U \in \mathcal{N}$ and $p_V \sim p_U$.

Proof. (i) Let $u \in \mathcal{N}$ be a partial isometry which maps $\operatorname{im} e$ isometrically onto $\operatorname{im} f$ and vanishes on the orthogonal complement $(\operatorname{im} e)^{\perp}$. We shall prove that $ce \sim cf$, by showing that $cu \in \mathcal{N}$ maps $\operatorname{im} ce$ isometrically onto $\operatorname{im} cf$ and vanishes on the orthogonal complement $(\operatorname{im} ce)^{\perp}$. Since $ue(\mathcal{H}) = u(\operatorname{im} e) = \operatorname{im} f = f(\mathcal{H})$, we have

$$cu(ce(\mathcal{H})) = cuce(\mathcal{H}) = c^2ue(\mathcal{H}) = cue(\mathcal{H}) = cf(\mathcal{H}).$$

For any vector $\xi \in \operatorname{im} ce = \operatorname{im} c \cap \operatorname{im} e$ we have $cu(\xi) = uc(\xi) = u(\xi)$ and hence $\| cu(\xi) \| = \| u(\xi) \| = \| \xi \|$. It follows that cu maps the subspace $\operatorname{im} ce$ isometrically onto $\operatorname{im} cf$. Since u vanishes on $(\operatorname{im} e)^{\perp} = \operatorname{im}(1-e)$, we have $u(1-e) = 0$ and hence

$$cu(1-ce) = cu - cuce = cu - c^2ue = cu - cue = cu(1-e) = 0 .$$

Therefore, cu vanishes on the subspace $\operatorname{im}(1-ce) = (\operatorname{im} ce)^{\perp}$, as needed.

(ii) Since $a, a^* \in \mathcal{N}$, the subspaces $V = \overline{\operatorname{im} a}$ and $U = \overline{\operatorname{im} a^*}$ are easily seen to be $\mathcal{N}'$-invariant. Therefore, Lemma E.1 implies that $p_V, p_U \in \mathcal{N}$. If $a = u\,|a|$ is the polar decomposition of a (cf. Proposition 1.11), then u maps U isometrically onto V and vanishes on the orthogonal complement $U^{\perp}$. The proof is finished, since the partial isometry u is contained in the von Neumann algebra $\mathcal{N}$ (cf. Proposition 1.19). □

Proposition E.4 *Let $(V_i)_i$ and $(V_i')_i$ be two orthogonal families of closed subspaces of $\mathcal{H}$, which are such that $p_{V_i}, p_{V_i'} \in \mathcal{N}$ and $p_{V_i} \sim p_{V_i'}$ for all i. Then, $\sum_i p_{V_i} \sim \sum_i p_{V_i'}$.*

Proof. In view of Corollary E.2, we know that $\sum_i p_{V_i}, \sum_i p_{V_i'} \in \mathcal{N}$. For any index i there is a partial isometry $u_i \in \mathcal{N}$, which maps V_i isometrically onto V_i' and vanishes on the orthogonal complement $V_i^{\perp}$. Let V (resp. V') be the orthogonal direct sum of the family $(V_i)_i$ (resp. $(V_i')_i$). Then, any vector $\xi \in \mathcal{H}$ admits an orthogonal decomposition $\xi = \sum_i \xi_i + \eta$, where $\xi_i \in V_i$ for all i and $\eta \in V^{\perp}$. Then, we have

$$\sum_i \| u_i(\xi_i) \|^2 = \sum_i \| \xi_i \|^2 \leq \| \xi \|^2 , \tag{E.1}$$

with equality if and only if $\eta = 0$ (i.e. if and only if $\xi \in V$). It follows that the sum $\sum_i u_i(\xi_i)$ is a well-defined element of V'. Hence, we may consider the linear map $u : \mathcal{H} \longrightarrow \mathcal{H}$, which is defined by mapping any element $\xi \in \mathcal{H}$ onto $\sum_i u_i(\xi_i)$, where $\xi = \sum_i \xi_i + \eta$ is the orthogonal decomposition of ξ as above. In view of (E.1), the operator u is bounded; in fact, u maps V isometrically onto V' and vanishes on the orthogonal complement $V^\perp$. Since $\sum_i p_{V_i} = p_V$ and $\sum_i p_{V_i'} = p_{V'}$, it only remains to prove that the partial isometry $u \in \mathcal{B}(\mathcal{H})$ is an element of the von Neumann algebra $\mathcal{N}$. To that end, we consider an operator a in the commutant $\mathcal{N}'$ and prove that $ua = au$. Since the projections p_V and p_{V_i} are contained in $\mathcal{N}$, Lemma E.1 implies that the subspaces $V^\perp$ and V_i are a-invariant for all i. We now fix a vector $\xi \in \mathcal{H}$ and consider the decomposition $\xi = \sum_i \xi_i + \eta$, where $\xi_i \in V_i$ for all i and $\eta \in V^\perp$. Then, $a(\xi) = \sum_i a(\xi_i) + a(\eta)$ is the associated decomposition of $a(\xi)$, since $a(\xi_i) \in V_i$ for all i and $a(\eta) \in V^\perp$. Hence,

$$\begin{aligned} ua(\xi) &= u\Big(\sum\nolimits_i a(\xi_i) + a(\eta)\Big) \\ &= \sum\nolimits_i u_i a(\xi_i) \\ &= \sum\nolimits_i a u_i(\xi_i) \\ &= a\Big(\sum\nolimits_i u_i(\xi_i)\Big) \\ &= au(\xi) , \end{aligned}$$

where the third equality follows since the operator $u_i \in \mathcal{N}$ commutes with $a \in \mathcal{N}'$ for all i and the fourth one is a consequence of the continuity of a. This is the case for any vector $\xi \in \mathcal{H}$ and hence $ua = au$, as needed. □

We now define the central carrier of a projection in $\mathcal{N}$; this notion will be our main technical tool in the proof of the comparison theorem.

Proposition E.5 *Let $e \in \mathcal{N}$ be a projection with range V (so that $e = p_V$) and consider the closed linear subspace $U = [\mathcal{N}V]^-$ of $\mathcal{H}$ generated by the set $\mathcal{N}V = \{a(\xi) : a \in \mathcal{N}, \xi \in V\}$. Then, the projection $c = p_U \in \mathcal{B}(\mathcal{H})$ has the following properties:*

(i) c is a projection in the center of the algebra $\mathcal{N}$,

(ii) $e \le c$ and

(iii) if c' is a projection in the center of $\mathcal{N}$ with $e \le c'$, then $c \le c'$.

The projection c is called the central carrier of e.

Proof. (i) In order to show that $c \in \mathcal{N} \cap \mathcal{N}'$, we shall prove that the closed linear subspace U is invariant under both $\mathcal{N}'$ and $\mathcal{N}'' = \mathcal{N}$ (cf. Lemma E.1). To that end, it suffices to show that the set $\mathcal{N}V$ is invariant under $\mathcal{N}'$ and $\mathcal{N}$. It is clear that $\mathcal{N}V$ is $\mathcal{N}$-invariant. On the other hand, $e = p_V$ is a projection in $\mathcal{N}$ and hence the subspace V is $\mathcal{N}'$-invariant (loc.cit.). It follows easily from this that $\mathcal{N}V$ is $\mathcal{N}'$-invariant as well.

(ii) The algebra $\mathcal{N}$ is unital and hence $V \subseteq \mathcal{N}V \subseteq [\mathcal{N}V]^- = U$; therefore, $e = p_V \le p_U = c$.

(iii) Let c' be a central projection in $\mathcal{N}$ with range U' and assume that $e \leq c'$. Since $c' \in \mathcal{N}'$, the subspace U' is invariant under $\mathcal{N}'' = \mathcal{N}$ (loc.cit.). Moreover, $e \leq c'$ and hence $V \subseteq U'$. It follows that

$$\mathcal{N}V = \{a(\xi) : a \in \mathcal{N}, \xi \in V\} \subseteq \{a(\xi) : a \in \mathcal{N}, \xi \in U'\} \subseteq U'$$

and hence $U = [\mathcal{N}V]^- \subseteq U'$. Therefore, $c = p_U \leq p_{U'} = c'$. □

We now relate the orthogonality of the central carriers of two projections in $\mathcal{N}$ to the existence of non-zero equivalent sub-projections.

Proposition E.6 *The following conditions are equivalent for two projections $e, f \in \mathcal{N}$:*

(i) The projections e and f have no non-zero sub-projections, which are equivalent rel $\mathcal{N}$.

(ii) We have $eaf = 0$ for all $a \in \mathcal{N}$.

(iii) $c(e)c(f) = 0$, where $c(e)$ and $c(f)$ are the central carriers of e and f respectively.

Proof. (i)→(ii): Assume that there is an operator $a \in \mathcal{N}$ with $eaf \neq 0$ and consider the projection p_V onto the closed linear subspace $V = \overline{\operatorname{im} eaf}$; then, $0 \neq p_V \leq e$. The subspace V is easily seen to be $\mathcal{N}'$-invariant and hence Lemma E.1 implies that $p_V \in \mathcal{N}$. Since the operator $fa^*e = (eaf)^* \in \mathcal{N}$ is non-zero as well, the same argument shows that the projection p_U onto the closed linear subspace $U = \overline{\operatorname{im} fa^*e}$ is a projection in $\mathcal{N}$ with $0 \neq p_U \leq f$. Therefore, p_V and p_U are non-zero sub-projections of e and f respectively, which are equivalent rel $\mathcal{N}$, in view of Proposition E.3(ii). It follows that if (i) holds then $eaf = 0$ for all $a \in \mathcal{N}$.

(ii)→(iii): Assume that $eaf = 0$ for all $a \in \mathcal{N}$. Then, for any $a, b \in \mathcal{N}$ we have $ea^*bf = 0$ and hence for any vectors $\xi, \eta \in \mathcal{H}$ we compute

$$< ae(\xi), bf(\eta) > = < \xi, ea^*bf(\eta) > = 0 \ .$$

It follows that the closed linear subspaces $[\mathcal{N}e(\mathcal{H})]^-$ and $[\mathcal{N}f(\mathcal{H})]^-$, which are generated by the sets $\mathcal{N}e(\mathcal{H}) = \{ae(\xi) : a \in \mathcal{N}, \xi \in \mathcal{H}\}$ and $\mathcal{N}f(\mathcal{H}) = \{bf(\eta) : b \in \mathcal{N}, \eta \in \mathcal{H}\}$ respectively, are orthogonal to each other. Since $c(e), c(f)$ are the orthogonal projections onto $[\mathcal{N}e(\mathcal{H})]^-$ and $[\mathcal{N}f(\mathcal{H})]^-$, it follows that $c(e)c(f) = 0$.

(iii)→(i): Assume that $c(e)c(f) = 0$ and consider two projections $e', f' \in \mathcal{N}$ with $e' \leq e$, $f' \leq f$ and $e' \sim f'$. Then, there is a partial isometry $u \in \mathcal{N}$, which maps $\operatorname{im} e'$ isometrically onto $\operatorname{im} f'$ and vanishes on the orthogonal complement $(\operatorname{im} e')^\perp$; in particular, we have $u = f'ue'$. Since $e' \leq e \leq c(e)$ (cf. Proposition E.5(ii)), we have $e' = e'c(e)$. Arguing similarly, we conclude that $f' = f'c(f)$. We now compute

$$u = f'ue' = f'c(f)ue'c(e) = f'ue'c(e)c(f) = 0 \ ,$$

where the third equality follows since $c(f)$ is central (cf. Proposition E.5(i)). Hence, we conclude that $e' = u^*u = 0$ and $f' = uu^* = 0$. □

Recall that, given two projections $e, f \in \mathcal{N}$, we say that e is weaker than f rel $\mathcal{N}$ if there is a projection $e' \in \mathcal{N}$, such that $e \sim e'$ and $e' \leq f$; in that case, we write $e \preceq f$. The projection e is strictly weaker than f rel $\mathcal{N}$ if $e \preceq f$ and $e \not\sim f$; in that case, we write $e \prec f$.

We are now ready to state and prove the main result of this Appendix.

Theorem E.7 *(comparison theorem) For any two projections $e, f \in \mathcal{N}$ there is a central projection $c \in \mathcal{N}$, such that $ce \preceq cf$ and $(1-c)f \preceq (1-c)e$.*

Proof. We consider sets of ordered pairs $P = \{(e_i, f_i) : i \in I\}$, such that:
(i) e_i, f_i are projections in $\mathcal{N}$ with $e_i \sim f_i$ for all i,
(ii) $e_i \leq e$ and $f_i \leq f$ for all i and
(iii) $e_i e_j = 0$ and $f_i f_j = 0$ for all $i \neq j$.
Let $\mathcal{P}$ be the collection consisting of the sets P as above; then, $\mathcal{P} \neq \emptyset$, since $\{(0,0)\} \in \mathcal{P}$. Ordering the set $\mathcal{P}$ by inclusion, we note that it satisfies the assumptions of Zorn's lemma. Therefore, $\mathcal{P}$ has a maximal element $\overline{P} = \left\{ \left(\overline{e_i}, \overline{f_i}\right) : i \in \overline{I} \right\}$. We now consider the projections $e_0 = e - \sum_i \overline{e_i}$ and $f_0 = f - \sum_i \overline{f_i}$, which are contained in $\mathcal{N}$ (cf. Corollary E.2). If $e', f' \in \mathcal{N}$ are non-zero sub-projections of e_0 and f_0 respectively with $e' \sim f'$, then $\overline{P} \cup \{(e', f')\}$ is an element of $\mathcal{P}$ which is strictly bigger than $\overline{P}$. In view of the maximality of $\overline{P}$, we conclude that the projections $e_0, f_0 \in \mathcal{N}$ have no non-zero equivalent sub-projections. Hence, Proposition E.6 implies that $c(e_0)c(f_0) = 0$, where $c(e_0)$ (resp. $c(f_0)$) is the central carrier of e_0 (resp. of f_0); since $e_0 = e_0 c(e_0)$ (cf. Proposition E.5(ii)), we have

$$c(f_0)e_0 = e_0 c(f_0) = e_0 c(e_0) c(f_0) = 0 \; .$$

Using Propositions E.3(i) and E.4, we conclude that

$$\begin{aligned} c(f_0)e &= c(f_0)e_0 + c(f_0)\sum\nolimits_i \overline{e_i} \\ &= c(f_0)\sum\nolimits_i \overline{e_i} \\ &\sim c(f_0)\sum\nolimits_i \overline{f_i} \\ &\leq c(f_0)f \; . \end{aligned}$$

Since $(1 - c(f_0))f_0 = f_0 - c(f_0)f_0 = 0$ (cf. Proposition E.5(ii)), we also have

$$\begin{aligned} (1 - c(f_0))f &= (1 - c(f_0))f_0 + (1 - c(f_0))\sum\nolimits_i \overline{f_i} \\ &= (1 - c(f_0))\sum\nolimits_i \overline{f_i} \\ &\sim (1 - c(f_0))\sum\nolimits_i \overline{e_i} \\ &\leq (1 - c(f_0))e \; . \end{aligned}$$

This finishes the proof, by letting $c = c(f_0)$. □

Corollary E.8 *Let $e, f \in \mathcal{N}$ be two projections, which are not equivalent rel $\mathcal{N}$. Then, there is a central projection $c \in \mathcal{N}$, such that $ce \prec cf$ or $cf \prec ce$.*

Proof. In view of Theorem E.7, there is a central projection $c_0 \in \mathcal{N}$, such that $c_0 e \preceq c_0 f$ and $(1-c_0)f \preceq (1-c_0)e$. We shall finish the proof by showing that $c_0 e \prec c_0 f$ or $(1-c_0)f \prec (1-c_0)e$. To that end, we argue by contradiction and assume that $c_0 e \sim c_0 f$ and $(1-c_0)f \sim (1-c_0)e$. In that case, we may invoke Proposition E.4 and conclude that

$$e = c_0 e + (1-c_0)e \sim c_0 f + (1-c_0)f = f ,$$

contradicting our assumption that $e \not\sim f$. □

E.2 Exercises

1. Let $\mathcal{H}$ be a Hilbert space and $u \in \mathcal{B}(\mathcal{H})$ a bounded linear operator. Show that the following conditions are equivalent:
   (i) u is a partial isometry,
   (i)' u^* is a partial isometry,
   (ii) $u = uu^*u$,
   (ii)' $u^* = u^*uu^*$,
   (iii) u^*u is a projection and
   (iii)' uu^* is a projection.
2. Let $\mathcal{N}$ be a von Neumann algebra of operators acting on the Hilbert space $\mathcal{H}$. Two projections $e, f \in \mathcal{N}$ are called unitarily equivalent in $\mathcal{N}$ if there is a unitary operator $u \in \mathcal{N}$, such that $f = u^*eu$. Show that the relation of unitary equivalence in $\mathcal{N}$ implies that of equivalence rel $\mathcal{N}$.
3. Let $\mathcal{N}$ be a von Neumann algebra of operators acting on the Hilbert space $\mathcal{H}$. Then, $\mathcal{N}$ is called finite if there is no projection $e \in \mathcal{N}$ with $e \neq 1$, which is equivalent to 1 rel $\mathcal{N}$.
   (i) Assume that $\mathcal{N}$ is finite and let $e, f \in \mathcal{N}$ be two projections, such that $e \leq f$ and $e \sim f$. Then, show that $e = f$.
   (*Hint:* Use Proposition E.4.)
   (ii) Assume that two projections in $\mathcal{N}$ are equivalent rel $\mathcal{N}$ if and only if they are unitarily equivalent in $\mathcal{N}$ (cf. Exercise 2 above). Then, show that $\mathcal{N}$ is finite.
   (iii) Let G be a group and $\mathcal{N}G$ the associated von Neumann algebra. Show that the von Neumann algebra $\mathbf{M}_n(\mathcal{N}G)$ of $n \times n$ matrices with entries in $\mathcal{N}G$ is finite for all $n \geq 1$.
   (*Hint:* Use Proposition 5.43(i),(ii).)
4. Let $\mathcal{N}$ be a finite von Neumann algebra of operators acting on the Hilbert space $\mathcal{H}$ (cf. Exercise 3 above). The goal of this Exercise is to show that two projections in $\mathcal{N}$ are equivalent rel $\mathcal{N}$ if and only if they are unitarily

equivalent in $\mathcal{N}$ (cf. Exercise 2 above).[3] To that end, let $e, f \in \mathcal{N}$ be two projections with $e \sim f$.
(i) Show that $1 - e \sim 1 - f$.
(*Hint:* Argue by contradiction, using Corollary E.8.)
(ii) Show that e and f are unitarily equivalent in $\mathcal{N}$.

[3] In view of Exercise 3(ii) above, it follows that a von Neumann algebra $\mathcal{N}$ is finite if and only if the relation *equivalence rel* $\mathcal{N}$ coincides with *unitary equivalence in* $\mathcal{N}$.

References

1. Adem, A., Karoubi, M.: Periodic cyclic cohomology of group rings. C. R. Acad. Sci. Paris Ser. I Math. **326**, 13–17 (1998)
2. Alexander, G.M.: Semisimple elements in group algebras. Comm. Algebra **21**, 2417–2435 (1993)
3. Atiyah, M.F., Macdonald, I.G.: Introduction to Commutative Algebra. Addison-Wesley 1969
4. Bass, H.: Euler characteristics and characters of discrete groups. Invent. Math. **35**, 155–196 (1976)
5. Bass, H.: Traces and Euler characteristics. Homological Group Theory (Ed. C.T.C. Wall), London Math. Soc. Lecture Notes Series **36**, 1–26 (1979)
6. Baum, P., Connes, A.: Geometric K-theory for Lie groups and foliations. IHES preprint 1982
7. Borel, A., Serre, J.-P.: Le Théorème de Riemann-Roch. Bull. Soc. Math. de France **86**, 97–136 (1958)
8. Bourbaki, N.: Éléments de mathématique. Algèbre Commutative. Paris: Masson 1985
9. Brown, K.S.: Cohomology of groups. (Grad. Texts Math. **87**) Berlin Heidelberg New York: Springer 1982
10. Burghelea, D.: The cyclic homology of the group rings. Comment. Math. Helv. **60**, 354–365 (1985)
11. Chadha, G.K., Passi, I.B.S.: Centralizers and homological dimension. Comm. Alg. **22**(14), 5703–5708 (1994)
12. Cliff, G.H.: Zero divisors and idempotents in group rings. Can. J. Math. **32**, 596–602 (1980)
13. Cliff, G.H.: Ranks of projective modules over group rings. Comm. Alg. **13**(5), 1115–1130 (1985)
14. Cliff, G.H., Sehgal, S.K.: On the trace of an idempotent in a group ring. Proc. Amer. Math. Soc. **62**, 11–14 (1977)
15. Connes, A.: Non-commutative differential geometry. Publ. Math. IHES **62**, 41–144 (1985)
16. Connes, A., Moscovici, H.: The L^2-index theorem for homogeneous spaces of Lie groups. Ann. of Math. **115**, 291–330 (1982)
17. Cuntz, J.: K-theoretic amenability for discrete groups. J. für Reine und Angew. Math. **344**, 180–195 (1983)

18. Dixmier, J.: Les Algèbres d' Opérateurs dans l'Espace Hilbertien. Gauthier-Villars, Paris 1969
19. Eckmann, B.: Cyclic homology of groups and the Bass conjecture. Comment. Math. Helv. **61**, 193–202 (1986)
20. Eckmann, B.: Projective and Hilbert modules over group algebras, and finitely dominated spaces. Comment. Math. Helv. **71**, 453–462 (1996). Addendum. Comment. Math. Helv. **72**, 329 (1997)
21. Eckmann, B.: Idempotents in a complex group algebra, projective modules, and the group von Neumann algebra. Arch. Math. (Basel) **76**, 241–249 (2001)
22. Emmanouil, I.: On a class of groups satisfying Bass' conjecture. Invent. Math. **132**, 307–330 (1998)
23. Emmanouil, I.: Projective modules, augmentation and idempotents in group algebras. J. Pure Appl. Alg. **158**, 151–160 (2001)
24. Emmanouil, I.: Traces and idempotents in group algebras. Math. Z. **245**, 293–307 (2003)
25. Emmanouil, I.: Induced projective modules over group von Neumann algebras. (to appear in K-Theory)
26. Emmanouil, I.: On the trace of idempotent matrices over group algebras. (preprint)
27. Emmanouil, I., Passi, I.B.S.: A contribution to Bass' conjecture. J. Group Theory **7**, 409–429 (2004)
28. Farrell, F.T., Linnell, P.A.: Whitehead groups and the Bass conjecture. Math. Ann. **326**, 723–757 (2003)
29. Formanek, E.: Idempotents in Noetherian group rings. Can. J. Math. **25**, 366–369 (1973)
30. Hall, P.: On the finiteness of certain soluble groups. Proc. London Math. Soc. (3) **9**, 595–622 (1959)
31. Hartshorne, R.: Algebraic Geometry. (Grad. Texts Math. **52**) Berlin Heidelberg New York: Springer 1977
32. Hattori, A: Rank element of a projective module. Nagoya J. Math. **25**, 113–120 (1965)
33. Hewitt, E., Ross, K.A.: Abstract Harmonic Analysis (vol. 1). Berlin Heidelberg New York: Springer 1963
34. Hilton, P., Stammbach, U.: A Course in Homological Algebra. (Grad. Texts Math. **4**) Berlin Heidelberg New York: Springer 1976
35. Ji, R.: Nilpotency of Connes' periodicity operator and the idempotent conjectures. K-Theory **9**, 59–76 (1995)
36. Kadison, R.V., Ringrose, J.R.: Fundamentals of the Theory of Operator Algebras. (2 volumes) San Diego Orlando: Academic Press 1983, 1986
37. Kaplansky, I.: Projective modules. Ann. Math. **68**, 372–377 (1958)
38. Kaplansky, I.: Fields and Rings. University of Chicago Press, Chicago 1969
39. Karoubi, M.: K-Theory: An Introduction. (Grundlehren der Math. Wissenschaften **226**) Berlin Heidelberg New York: Springer 1978
40. Karoubi, M., Villamayor, O.: Homologie cyclique d'algèbres de groupes. C.R. Acad. Sci. Paris **311**, 1–3 (1990)
41. Lam, T.Y.: A First Course in Noncommutative Rings. (Grad. Texts Math. **131**) Berlin Heidelberg New York: Springer 1991
42. Lang, S.: Algebra. Addison-Wesley 1993
43. Linnell, P.A.: Decomposition of augmentation ideals and relation modules. Proc. London Math. Soc. (3) **47**, 83–127 (1983)

44. Loday, J.L.: Cyclic homology. (Grundl. Math. Wiss. **301**) Berlin Heidelberg New York: Springer 1992
45. Loday J.L., Quillen, D.: Cyclic homology and the Lie algebra homology of matrices. Comment. Math. Helv. **59**, 565–591 (1984)
46. Lück, W.: The relation between the Baum-Connes conjecture and the trace conjecture. Invent. Math. **149**, 123–152 (2002)
47. Mac Carthy, R.: Morita equivalence and cyclic homology. C.R. Acad. Sci. Paris **307**, 211–215 (1988)
48. Mac Lane, S.: Homology. (Grundlehren der mathematischen Wissenschaften **114**) Berlin Heidelberg New York: Springer 1995
49. Malcev, A.I.: On faithful representations of infinite groups my matrices. Math. Sb. **8**(50), 405–422 (1940)
50. Marciniak, Z.: Cyclic homology and idempotents in group rings. Springer Lect. Notes in Math. **1217**, 253–257 (1985)
51. Marciniak, Z.: Cyclic homology of group rings. Banach Center Publications **18**, 305–312 (1986)
52. Matsumura, H.: Commutative ring theory. Cambridge Stud. Adv. Math. **8**, Cambridge University Press 1992
53. Moody, J.A.: Ph.D. thesis. Columbia University, 1986
54. Passi, I.B.S., Passman, D.S.: Algebraic elements in group rings. Proc. Amer. Math. Soc. **108**, 871–877 (1990)
55. Passman, D.S.: The algebraic structure of group rings. (Pure Appl. Math.) Wiley-Interscience, New York 1977
56. Pedersen, G.K.: Analysis Now. (Grad. Texts Math. **118**) Berlin Heidelberg New York: Springer 1989
57. Pimsner, M., Voiculescu, D.: K-groups of reduced crossed products by free groups. J. Oper. Theory **8**, 131–156 (1982)
58. Rosenberg, J.: Algebraic K-Theory and its Applications. (Grad. Texts Math. **147**) Berlin Heidelberg New York: Springer 1994
59. Roy, R.: The Trace Conjecture – A Counterexample. K-Theory **17**, 209–213 (1999)
60. Rudin, W.: Functional Analysis. McGraw-Hill 1973
61. Rudin, W.: Real and Complex Analysis. McGraw-Hill 1987
62. Schafer, J.A.: Traces and the Bass conjecture. Michigan Math. J. **38**, 103–109 (1991)
63. Schafer, J.A.: Relative cyclic homology and the Bass conjecture. Comment. Math. Helv. **67**, 214–225 (1992)
64. Schafer, J.A.: The Bass conjecture and group von Neumann algebras. K-Theory **19**, 211–217 (2000)
65. Serre, J.P.: Arbres, Amalgames, SL_2. Astérisque **46**, 1977
66. Stallings, J.: Centerless groups – an algebraic formulation of Gottlieb's theorem. Topology **4**, 129–134 (1965)
67. Stevenhagen, P. and Lenstra, H.W.Jr.: Chebotarëv and his Density Theorem. Math. Intelligencer **18**, 26–37 (1996)
68. Strebel, R.: Homological methods applied to the derived series of groups. Comment. Math. Helv. **49**, 302–332 (1974)
69. Strojnowski, A.: Idempotents and zero divisors in group rings. Comm. Alg. **14**(7), 1171–1185 (1986)
70. Swan, R.G.: Induced representations and projective modules. Ann. Math. **71**, 552–578 (1960)

71. Swan, R.G.: Vector bundles and projective modules. Trans. Amer. Math. Soc. **105**, 264–277 (1962)
72. Wall, C.T.C.: Finiteness conditions for CW-complexes I. Ann. of Math. **81**, 56–69 (1965); Finiteness conditions for CW-complexes II. Proc. Royal Soc. Ser. A **295**, 129–139 (1966)
73. Weibel, C.: An introduction to algebraic K-theory. (book in progress, `http://math.rutgers.edu/~weibel/Kbook.html`)
74. Weiss, A.: Idempotents in group rings. J. Pure Appl. Algebra **16**, 207–213 (1980)
75. Zaleskii, A.E.: On a problem of Kaplansky. Soviet. Math. **13**, 449–452 (1972)

Index

Universitext

Aguilar, M.; Gitler, S.; Prieto, C.: Algebraic Topology from a Homotopical Viewpoint

Aksoy, A.; Khamsi, M. A.: Methods in Fixed Point Theory

Alevras, D.; Padberg M. W.: Linear Optimization and Extensions

Andersson, M.: Topics in Complex Analysis

Aoki, M.: State Space Modeling of Time Series

Arnold, V. I.: Lectures on Partial Differential Equations

Audin, M.: Geometry

Aupetit, B.: A Primer on Spectral Theory

Bachem, A.; Kern, W.: Linear Programming Duality

Bachmann, G.; Narici, L.; Beckenstein, E.: Fourier and Wavelet Analysis

Badescu, L.: Algebraic Surfaces

Balakrishnan, R.; Ranganathan, K.: A Textbook of Graph Theory

Balser, W.: Formal Power Series and Linear Systems of Meromorphic Ordinary Differential Equations

Bapat, R.B.: Linear Algebra and Linear Models

Benedetti, R.; Petronio, C.: Lectures on Hyperbolic Geometry

Benth, F. E.: Option Theory with Stochastic Analysis

Berberian, S. K.: Fundamentals of Real Analysis

Berger, M.: Geometry I, and II

Bliedtner, J.; Hansen, W.: Potential Theory

Blowey, J. F.; Coleman, J. P.; Craig, A. W. (Eds.): Theory and Numerics of Differential Equations

Blowey, J.; Craig, A.: Frontiers in Numerical Analysis. Durham 2004

Blyth, T. S.: Lattices and Ordered Algebraic Structures

Börger, E.; Grädel, E.; Gurevich, Y.: The Classical Decision Problem

Böttcher, A; Silbermann, B.: Introduction to Large Truncated Toeplitz Matrices

Boltyanski, V.; Martini, H.; Soltan, P. S.: Excursions into Combinatorial Geometry

Boltyanskii, V. G.; Efremovich, V. A.: Intuitive Combinatorial Topology

Bonnans, J. F.; Gilbert, J. C.; Lemarchal, C.; Sagastizbal, C. A.: Numerical Optimization

Booss, B.; Bleecker, D. D.: Topology and Analysis

Borkar, V. S.: Probability Theory

Brunt B. van: The Calculus of Variations

Carleson, L.; Gamelin, T. W.: Complex Dynamics

Cecil, T. E.: Lie Sphere Geometry: With Applications of Submanifolds

Chae, S. B.: Lebesgue Integration

Chandrasekharan, K.: Classical Fourier Transform

Charlap, L. S.: Bieberbach Groups and Flat Manifolds

Chern, S.: Complex Manifolds without Potential Theory

Chorin, A. J.; Marsden, J. E.: Mathematical Introduction to Fluid Mechanics

Cohn, H.: A Classical Invitation to Algebraic Numbers and Class Fields

Curtis, M. L.: Abstract Linear Algebra

Curtis, M. L.: Matrix Groups

Cyganowski, S.; Kloeden, P.; Ombach, J.: From Elementary Probability to Stochastic Differential Equations with MAPLE

Dalen, D. van: Logic and Structure

Das, A.: The Special Theory of Relativity: A Mathematical Exposition

Debarre, O.: Higher-Dimensional Algebraic Geometry

Deitmar, A.: A First Course in Harmonic Analysis

Demazure, M.: Bifurcations and Catastrophes

Devlin, K. J.: Fundamentals of Contemporary Set Theory

DiBenedetto, E.: Degenerate Parabolic Equations

Diener, F.; Diener, M.(Eds.): Nonstandard Analysis in Practice

Dimca, A.: Sheaves in Topology

Dimca, A.: Singularities and Topology of Hypersurfaces

DoCarmo, M. P.: Differential Forms and Applications

Duistermaat, J. J.; Kolk, J. A. C.: Lie Groups

Edwards, R. E.: A Formal Background to Higher Mathematics Ia, and Ib

Edwards, R. E.: A Formal Background to Higher Mathematics IIa, and IIb

Emery, M.: Stochastic Calculus in Manifolds

Emmanouil, I.: Idempotent Matrices over Complex Group Algebras

Endler, O.: Valuation Theory

Erez, B.: Galois Modules in Arithmetic

Everest, G.; Ward, T.: Heights of Polynomials and Entropy in Algebraic Dynamics

Farenick, D. R.: Algebras of Linear Transformations

Foulds, L. R.: Graph Theory Applications

Franke, J.; Hrdle, W.; Hafner, C. M.: Statistics of Financial Markets: An Introduction

Frauenthal, J. C.: Mathematical Modeling in Epidemiology

Freitag, E.; Busam, R.: Complex Analysis

Friedman, R.: Algebraic Surfaces and Holomorphic Vector Bundles

Fuks, D. B.; Rokhlin, V. A.: Beginner's Course in Topology

Fuhrmann, P. A.: A Polynomial Approach to Linear Algebra

Gallot, S.; Hulin, D.; Lafontaine, J.: Riemannian Geometry

Gardiner, C. F.: A First Course in Group Theory

Gårding, L.; Tambour, T.: Algebra for Computer Science

Godbillon, C.: Dynamical Systems on Surfaces

Godement, R.: Analysis I, and II

Goldblatt, R.: Orthogonality and Spacetime Geometry

Gouvêa, F. Q.: p-Adic Numbers

Gross, M. et al.: Calabi-Yau Manifolds and Related Geometries

Gustafson, K. E.; Rao, D. K. M.: Numerical Range. The Field of Values of Linear Operators and Matrices

Gustafson, S. J.; Sigal, I. M.: Mathematical Concepts of Quantum Mechanics

Hahn, A. J.: Quadratic Algebras, Clifford Algebras, and Arithmetic Witt Groups

Hájek, P.; Havránek, T.: Mechanizing Hypothesis Formation

Heinonen, J.: Lectures on Analysis on Metric Spaces

Hlawka, E.; Schoißengeier, J.; Taschner, R.: Geometric and Analytic Number Theory

Holmgren, R. A.: A First Course in Discrete Dynamical Systems

Howe, R., Tan, E. Ch.: Non-Abelian Harmonic Analysis

Howes, N. R.: Modern Analysis and Topology

Hsieh, P.-F.; Sibuya, Y. (Eds.): Basic Theory of Ordinary Differential Equations

Humi, M., Miller, W.: Second Course in Ordinary Differential Equations for Scientists and Engineers

Hurwitz, A.; Kritikos, N.: Lectures on Number Theory

Huybrechts, D.: Complex Geometry: An Introduction

Isaev, A.: Introduction to Mathematical Methods in Bioinformatics

Istas, J.: Mathematical Modeling for the Life Sciences

Iversen, B.: Cohomology of Sheaves

Jacod, J.; Protter, P.: Probability Essentials

Jennings, G. A.: Modern Geometry with Applications

Jones, A.; Morris, S. A.; Pearson, K. R.: Abstract Algebra and Famous Inpossibilities

Jost, J.: Compact Riemann Surfaces

Jost, J.: Dynamical Systems. Examples of Complex Behaviour

Jost, J.: Postmodern Analysis

Jost, J.: Riemannian Geometry and Geometric Analysis

Kac, V.; Cheung, P.: Quantum Calculus

Kannan, R.; Krueger, C. K.: Advanced Analysis on the Real Line

Kelly, P.; Matthews, G.: The Non-Euclidean Hyperbolic Plane

Kempf, G.: Complex Abelian Varieties and Theta Functions

Kitchens, B. P.: Symbolic Dynamics

Kloeden, P.; Ombach, J.; Cyganowski, S.: From Elementary Probability to Stochastic Differential Equations with MAPLE

Kloeden, P. E.; Platen; E.; Schurz, H.: Numerical Solution of SDE Through Computer Experiments

Kostrikin, A. I.: Introduction to Algebra

Krasnoselskii, M. A.; Pokrovskii, A. V.: Systems with Hysteresis

Kurzweil, H.; Stellmacher, B.: The Theory of Finite Groups. An Introduction

Lang, S.: Introduction to Differentiable Manifolds

Luecking, D. H., Rubel, L. A.: Complex Analysis. A Functional Analysis Approach

Ma, Zhi-Ming; Roeckner, M.: Introduction to the Theory of (non-symmetric) Dirichlet Forms

Mac Lane, S.; Moerdijk, I.: Sheaves in Geometry and Logic

Marcus, D. A.: Number Fields

Martinez, A.: An Introduction to Semiclassical and Microlocal Analysis

Matoušek, J.: Using the Borsuk-Ulam Theorem

Matsuki, K.: Introduction to the Mori Program

Mazzola, G.; Milmeister G.; Weissman J.: Comprehensive Mathematics for Computer Scientists 1

Mazzola, G.; Milmeister G.; Weissman J.: Comprehensive Mathematics for Computer Scientists 2

Mc Carthy, P. J.: Introduction to Arithmetical Functions

McCrimmon, K.: A Taste of Jordan Algebras

Meyer, R. M.: Essential Mathematics for Applied Field

Meyer-Nieberg, P.: Banach Lattices

Mikosch, T.: Non-Life Insurance Mathematics

Mines, R.; Richman, F.; Ruitenburg, W.: A Course in Constructive Algebra

Moise, E. E.: Introductory Problem Courses in Analysis and Topology

Montesinos-Amilibia, J. M.: Classical Tessellations and Three Manifolds

Morris, P.: Introduction to Game Theory

Nikulin, V. V.; Shafarevich, I. R.: Geometries and Groups

Oden, J. J.; Reddy, J. N.: Variational Methods in Theoretical Mechanics

Øksendal, B.: Stochastic Differential Equations

Øksendal, B.; Sulem, A.: Applied Stochastic Control of Jump Diffusions

Poizat, B.: A Course in Model Theory

Polster, B.: A Geometrical Picture Book

Porter, J. R.; Woods, R. G.: Extensions and Absolutes of Hausdorff Spaces

Radjavi, H.; Rosenthal, P.: Simultaneous Triangularization

Ramsay, A.; Richtmeyer, R. D.: Introduction to Hyperbolic Geometry

Rees, E. G.: Notes on Geometry

Reisel, R. B.: Elementary Theory of Metric Spaces

Rey, W. J. J.: Introduction to Robust and Quasi-Robust Statistical Methods

Ribenboim, P.: Classical Theory of Algebraic Numbers

Rickart, C. E.: Natural Function Algebras

Rotman, J. J.: Galois Theory

Rubel, L. A.: Entire and Meromorphic Functions

Ruiz-Tolosa, J. R.; Castillo E.: From Vectors to Tensors

Runde, V.: A Taste of Topology

Rybakowski, K. P.: The Homotopy Index and Partial Differential Equations

Sagan, H.: Space-Filling Curves

Samelson, H.: Notes on Lie Algebras

Schiff, J. L.: Normal Families

Sengupta, J. K.: Optimal Decisions under Uncertainty

Séroul, R.: Programming for Mathematicians

Seydel, R.: Tools for Computational Finance

Shafarevich, I. R.: Discourses on Algebra

Shapiro, J. H.: Composition Operators and Classical Function Theory

Simonnet, M.: Measures and Probabilities

Smith, K. E.; Kahanpää, L.; Kekäläinen, P.; Traves, W.: An Invitation to Algebraic Geometry

Smith, K. T.: Power Series from a Computational Point of View

Smoryński, C.: Logical Number Theory I. An Introduction

Stichtenoth, H.: Algebraic Function Fields and Codes

Stillwell, J.: Geometry of Surfaces

Stroock, D. W.: An Introduction to the Theory of Large Deviations

Sunder, V. S.: An Invitation to von Neumann Algebras

Tamme, G.: Introduction to Étale Cohomology

Tondeur, P.: Foliations on Riemannian Manifolds

Toth, G.: Finite Mbius Groups, Minimal Immersions of Spheres, and Moduli

Verhulst, F.: Nonlinear Differential Equations and Dynamical Systems

Wong, M. W.: Weyl Transforms

Xambó-Descamps, S.: Block Error-Correcting Codes

Zaanen, A.C.: Continuity, Integration and Fourier Theory

Zhang, F.: Matrix Theory

Zong, C.: Sphere Packings

Zong, C.: Strange Phenomena in Convex and Discrete Geometry

Zorich, V. A.: Mathematical Analysis I

Zorich, V. A.: Mathematical Analysis II