Structure of finitely generated abelian groups

July 9, 2006

French developped version.

http://hlombardi.free.fr/publis/IntroPtdeVueConstr.pdf

Printable version of these slides:

http://hlombardi.free.fr/publis/LectureDoc1.pdf

Basic reference for constructive algebra

[MRR] *A Course in Constructive Algebra*
Mines R., Richman F., Ruitenburg W. (1985) Springer

Plan

- – Statement of the theorem for abelian groups

  – Generalized form: Principal Ideal Domains

- Case of finitely generated subgroups or modules:
  Smith diagonalization.

- Solutions of linear systems. Coherence.

- Case of finite intersections of finitely generated subgroups.

- General case: notheriannity.

Structure theorem for finitely generated abelian groups

Theorem 1. (Existence of a good basis, 1).
Let G be a subgroup of $(\mathbb{Z}^n, +)$.

1. *There exist a $\mathbb{Z}$-basis $(e_1, \ldots, e_n)$ of $\mathbb{Z}^n$, an integer r $(0 \leq r \leq n)$, and positive integers $a_1, \ldots, a_r$ such that:*
   - *a_i divides a_{i+1} $(1 \leq i < r)$*
   - *$(a_1 e_1, \ldots, a_r e_r)$ is a $\mathbb{Z}$-basis of G.*
2. *The subgroup $\tilde{G} = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_r$ of $\mathbb{Z}^n$ depends uniquely of G: it is equal to $\{\, x \,|\, \exists k > 0,\, kx \in G \,\}$.*
3. $\mathbb{Z}^n/G \simeq \mathbb{Z}^{n-r} \oplus \tilde{G}/G \simeq \mathbb{Z}^{n-r} \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_r\mathbb{Z}$.
4. *The list $[a_1, \ldots, a_r]$ is uniquely determined, $(\tilde{G} : G) = a_1 \cdots a_r$.*

Principal ideal domains

- $\mathbf{A}$ is a discrete domain: every element is regular or equal to 0. Equivalently, $\forall x \in \mathbf{A} \quad \mathrm{Ann}(x) = 0$ or $\langle 1 \rangle$.

- $\mathbf{A}$ is Bezout: each finitely generated ideal is principal. Equivalently (for a discrete domain) $\forall a, b,\ \exists u, v, s, t, g$ such that

$$\begin{bmatrix} u & v \\ s & t \end{bmatrix} \cdot \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} g \\ 0 \end{bmatrix}, \quad \begin{vmatrix} u & v \\ s & t \end{vmatrix} = 1$$

- $\mathbf{A}$ is RS-Noetherian: each ascending chain of finitely generated ideals has two consecutive terms equal.

Remark : We don't need an explicit divisibility relation, but without this condition the last item is a bit disturbing.

Structure theorem: finitely generated modules over a PID

Theorem 2. (Existence of a good basis, 2).
Let $\mathbf{A}$ be a PID and M a submodule of $\mathbf{A}^n$.

1. *There exist an $\mathbf{A}$-basis $(e_1, \ldots, e_n)$ of $\mathbf{A}^n$, an integer r $(0 \leq r \leq n)$, and regular elements $a_1, \ldots, a_r \in \mathbf{A}$ such that:*
   - *a_i divides a_{i+1} $(1 \leq i < r)$*
   - *$(a_1 e_1, \ldots, a_r e_r)$ is an $\mathbf{A}$-basis of M.*
2. *The submodule $\widetilde{M} = \mathbf{A}e_1 \oplus \cdots \oplus \mathbf{A}e_r$ of $\mathbf{A}^n$ depends uniquely of M: it is equal to $\{\, x \,|\, \exists a \in \mathbf{A}, a$ regular, $ax \in M \,\}$.*
3. $\mathbf{A}^n/M \simeq \mathbf{A}^{n-r} \oplus \widetilde{M}/M \simeq \mathbf{A}^{n-r} \oplus \mathbf{A}/a_1\mathbf{A} \oplus \cdots \oplus \mathbf{A}/a_r\mathbf{A}$.
4. *Either the list $[a_1\mathbf{A}, \ldots, a_r\mathbf{A}]$ is uniquely determined, or $\mathbf{A}$ is trivial.*

NB: M and $\widetilde{M}$ are free.

Smith diagonalization of matrices

Theorem 3. (Smith reduction over $\mathbb{Z}$)
Let M be a matrix $\in \mathbb{Z}^{n\times m}$. It admits a Smith reduction*:*
there exist two invertible matrices $C \in \mathbb{Z}^{m\times m}$ and $L \in \mathbb{Z}^{n\times n}$ such that the matrix $D = LMC$ is in Smith reduced form, *i.e., all entries $d_{i,j}$ where $i \neq j$ are zero, and $d_{i,i}$ divides $d_{i+1,i+1}$ $(1 \leq i \leq \min(m,n)-1)$. Moreover, taking nonnegative $d_{i,i}$ they are uniquely determined by M. (the product $d_{1,1}\cdots d_{k,k}$ is equal to the gcd of all $k\times k$ minors of M).*

Theorem 4. (Smith reduction over a PID $\mathbf{A}$)
Let M be a matrix $\in \mathbf{A}^{n\times m}$. It admits a Smith reduction*:*
there exist two invertible matrices $C \in \mathbf{A}^{m\times m}$ and $L \in \mathbf{A}^{n\times n}$ such that the matrix $D = LMC$ is in Smith reduced form, *i.e., all entries $d_{i,j}$ where $i \neq j$ are zero, and $d_{i,i}$ divides $d_{i+1,i+1}$ $(1 \leq i \leq \min(m,n)-1)$. Moreover, the ideals $d_{i,i}\mathbf{A}$ are uniquely determined by M. (the product $d_{1,1}\cdots d_{k,k}$ is equal to the gcd of all $k\times k$ minors of M).*

Consequences of Smith diagonalization

If $\mathbf{A}$ is a PID, the good basis theorem applies for submodules $M \subseteq \mathbf{A}^n$ which are finitely generated.

Moreover a submodule $M \subseteq \mathbf{A}^n$ which is a finite intersection of finitely generated submodules is itself finitely generated.

The problem of computing generators for an intersection of finitely generated submodules of a free module is a basic one. This leads to the notion of **coherent rings**.

Solutions of linear systems, coherence

Definition 5.

1. *A ring* $\mathbf{A}$ *is* **coherent** *if every linear form* $\mathbf{A}^n \to \mathbf{A}$ *has a finitely generated kernel.*

2. *An* $\mathbf{A}$*-module* M *is* **coherent** *if every linear map* $\mathbf{A}^n \to M$ *has a finitely generated kernel.*

3. *A ring* $\mathbf{A}$ *is* **strongly discrete** *if for every linear form* $\alpha : \mathbf{A}^n \to \mathbf{A}$ *and every* $x \in \mathbf{A}$*, either* $x \in \operatorname{Im} \alpha$ *or* $((x \in \operatorname{Im} \alpha) \Rightarrow 1 =_{\mathbf{A}} 0)$*.*

4. *An* $\mathbf{A}$*-module* M *is* **strongly discrete** *if for every linear map* $\alpha : \mathbf{A}^n \to M$ *and every* $x \in M$*, either* $x \in \operatorname{Im} \alpha$ *or* $((x \in \operatorname{Im} \alpha) \Rightarrow 1 =_{\mathbf{A}} 0)$*.*

Coherence is what is needed to control homogeneous linear systems.

If you add strong discreteness you control all linear systems.

Coherence

A ring is coherent if and only if

1. The intersection of two finitely generated ideals is always a finitely generated ideal.
2. The annihilator of any element $x \in \mathbf{A}$, *i.e.*, $\{\, y \in \mathbf{A} \,|\, yx = 0 \,\}$ is a finitely generated ideal.

An $\mathbf{A}$-module is coherent if and only if

1. The intersection of two finitely generated submodules is always a finitely generated submodule.
2. The annihilator of any element $x \in M$, *i.e.*, $\{\, y \in \mathbf{A} \,|\, yx = 0 \,\}$ is a finitely generated ideal.

From rings to finitely presented modules

Theorem 6.

1. *If* $\mathbf{A}$ *is a coherent ring, then so is any finitely presented* $\mathbf{A}$*-module.*

2. *If* $\mathbf{A}$ *is a strongly discrete coherent ring, then so is any finitely presented* $\mathbf{A}$*-module.*

Noetherianity

The good basis theorem can be seen as:

- Each finitely generated subgroup of $\mathbb{Z}^n$ admits a good basis.
- Each subgroup of $\mathbb{Z}^n$ is finitely generated.

In order to understand constructively the second item let us consider the five following variants for an $\mathbf{A}$-module M.

N1: Each submodule of M is finitely generated.

N2: Each nondecreasing chain of submodules

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$$

is eventually constant.

N3: Each nondecreasing chain of finitely generated submodules is eventually constant.

N4: In each nondecreasing chain of finitely generated submodules there are two equal consecutive terms.

N5: A strictly increasing chain of finitely generated submodules is impossible.

Coherence and Noetheriannity

In classical mathematics Noetheriannity implies coherence. But strong "counterexamples" show that this implication has no computationnal content.

From a computational point of view, coherence is much more usefull than Noetheriannity.

Nevertheless Noetheriannity is interesting for obtaining proofs of termination for certain algorithms

Hilbert Noether Basis Theorem

Here Noetherian means RS-Noetherian.

Proposition 7. *If $\mathbf{A}$ is a Noetherian coherent ring, then so is any finitely presented $\mathbf{A}$-module.*

Theorem 8. (Hilbert, Noether, Richman, Seidenberg)

1. *If $\mathbf{A}$ is a Noetherian coherent ring, then so is $\mathbf{A}[X]$.*
2. *If $\mathbf{A}$ is a strongly discrete Noetherian coherent ring, then so is $\mathbf{A}[X]$.*

Corollary 9.

1. *If $\mathbf{A}$ is a Noetherian coherent ring, then so is any finitely presented $\mathbf{A}$-algebra.*
2. *If $\mathbf{A}$ is a strongly discrete Noetherian coherent ring, then so is any finitely presented $\mathbf{A}$-algebra.*