A short and elementary proof of the structure theorem for finitely generated modules over PIDs

Autor(en): **Spindler, Karlheinz**

Objekttyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **73 (2018)**

Heft 3

PDF erstellt am: **21.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-780945

Elem. Math. 73 (2018) 136 – 138
0013-6018/18/030136-3
DOI 10.4171/EM/364

Elemente der Mathematik

Short note

A short and elementary proof of the structure theorem for finitely generated modules over PIDs

Karlheinz Spindler

Dedicated to Prof. Karl Heinrich Hofmann on the Occasion of His 85th Birthday

While preparing an algebra class, I was looking for a way to adapt the slick proof in [1, Chapter 6, Theorem 6.9], attributed to Schenkman, of the structure theorem for finitely generated abelian groups to the corresponding structure theorem for finitely generated modules over principal ideal domains (PIDs). A research on the internet (see [2]) and in the literature (see [3]) confirmed that such a proof (requiring only minimal prerequisites, i.e., neither much theoretical background nor computations involving the Smith normal form for matrices over PIDs) is indeed available. The proof presented here is a modification of the one outlined in [3], with an extra corner cut off. It is hard to see how this proof could still be shortened. To make the presentation self-contained, we include the two auxiliary results used in [3].

Lemma 1. *Let R be a PID and let $r_1, \dots, r_n$ be relatively prime elements of R. Then there is a matrix $A \in R^{n\times n}$ which has $(r_1, \dots, r_n)$ as its first row and a unit of R as its determinant (which can be chosen to be 1 if $n \geq 2$).*

Proof. We use induction on n, the case $n = 1$ being trivial. Assume that the statement is true for some number n and consider $n + 1$ relatively prime elements $r_0, r_1, \dots, r_n \in R$. Let d be a gcd of $r_1, \dots, r_n$; then $r_i = d\rho_i$ with relatively prime elements $\rho_1, \dots, \rho_n$. By induction hypothesis, there is a matrix $B \in R^{n\times n}$ with $\det(B) = \xi \in R^\times$ whose first row is $(\rho_1, \dots, \rho_n)$. Let $B_0 \in R^{(n-1)\times n}$ be the matrix which is obtained from B by striking out the first row. Now $1 = \gcd(r_0, r_1, \dots, r_n) = \gcd\big(r_0, \gcd(r_1, \dots, r_n)\big) = \gcd(r_0, d)$. Since a gcd is only determined up to multiplication by a unit, we may as well write $\gcd(r_0, d) = \xi^{-1}$; hence there are elements $u, v \in R$ such that $ur_0 - vd = \xi^{-1}$, due to the linear representation of the gcd of two elements. Then the matrix

$$A := \begin{bmatrix} r_0 & r_1 & \cdots & r_n \\ v & u\rho_1 & \cdots & u\rho_n \\ 0 & \star & \cdots & \star \\ \vdots & \vdots & & \vdots \\ 0 & \star & \cdots & \star \end{bmatrix} = \begin{bmatrix} r_0 & d\rho_1 & \cdots & d\rho_n \\ v & u\rho_1 & \cdots & u\rho_n \\ 0 & \star & \cdots & \star \\ \vdots & \vdots & & \vdots \\ 0 & \star & \cdots & \star \end{bmatrix}$$

with B_0 in its lower-right corner has $(r_0, r_1, \ldots, r_n)$ as its first row. Using expansion by the first column, the determinant of this matrix is seen to be $\det(A) = r_0 u \det(B) - v d \det(B) = (r_0 u - v d)\det(B) = \xi^{-1}\xi = 1$, so that A has the desired property. This concludes the induction step. □

Lemma 2. *Let R be a PID, let $r_1, \ldots, r_n$ be relatively prime elements of R and let M be a finitely generated R-module. If $(x_1, \ldots, x_n)$ is a system of generators for M, then there is also a system of generators $(y_1, \ldots, y_n)$ for M such that $y_1 = r_1 x_1 + \cdots + r_n x_n$.*

Proof. By Lemma 1 there is a matrix $A \in R^{n\times n}$ whose first row is $(r_1, \ldots, r_n)$ and which possesses a matrix inverse $B = A^{-1}$ in $R^{n\times n}$. Let

$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} := A \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} r_1 & \cdots & r_n \\ \star & \cdots & \star \\ \vdots & & \vdots \\ \star & \cdots & \star \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \quad \text{so that} \quad \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = B \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}.$$

Then each element x_i is a linear combination of $y_1, \ldots, y_n$ over R. Consequently, $(y_1, \ldots, y_n)$ is a system of generators for M which has the desired property. □

We are now ready to give a succinct proof of the structure theorem for finitely generated modules over PIDs. We follow the convention of allowing the formation of greatest common divisors of elements which are not necessarily nonzero. Then clearly

$$\gcd(a_1, \ldots, a_m, 0, \ldots, 0) = \gcd(a_1, \ldots, a_m)$$

whenever $a_1, \ldots, a_m$ are nonzero elements, and $\gcd(a_1, \ldots, a_n) = 0$ if and only if $a_1 = \cdots = a_n = 0$. Also, we say that the zero element of a PID has an infinite number of prime factors, because each prime element divides the zero element with arbitrarily high multiplicity. These conventions allow us to carry out a proof by induction without having to distinguish between free modules and modules with torsion elements.

Theorem. *Let R be a PID, and let M be a module over R. If M is generated by n but not by $n-1$ elements, then M decomposes into a direct sum of n cyclic modules.*

Proof. We use induction on n, the case $n = 1$ being trivial. Let $n \geq 2$ and consider a module M generated by n but not by $n-1$ elements. Then a system $(x_1, \ldots, x_n)$ of generators can be chosen for which the annihilator $\mathrm{Ann}(x_1)$ of x_1 in R (which is an ideal and hence a principal ideal of R) has a generator d with a minimal number of prime factors (counted with multiplicity) amongst all elements of minimal generating sets. (Note that if $d = 0$ then $\mathrm{Ann}(x_i) = \{0\}$ for $1 \leq i \leq n$, this being the case of a torsion-free module.) We claim that we then have a direct sum decomposition

$$M = (Rx_1) \oplus (Rx_2 + \cdots + Rx_n)\,. \qquad (\star)$$

We prove this claim by showing that in each relation

$$r_1 x_1 + r_2 x_2 + \cdots + r_n x_n = 0 \qquad (\star\star)$$

we must have $d \mid r_1$ and hence $r_1 x_1 = 0$. Let $g := \gcd(r_1, d)$. By the linear representation of a gcd, there are elements $u, v \in R$ with $g = ur_1 + vd$, which implies that $gx_1 = ur_1 x_1$. Hence multiplying $(\star\star)$ with u becomes $gx_1 + ur_2 x_2 + \cdots + ur_n x_n = 0$. Let $\gamma := \gcd(g, ur_2, \ldots, ur_n)$. If $\gamma = 0$ then $g = ur_2 = \cdots = ur_n = 0$, and $g = 0$ implies $r_1 = d = 0$; hence we are done in this case (which is the case of a torsion-free module). Let $\gamma \neq 0$. Then, according to Lemma 2, there is a generating system $(y_1, \ldots, y_n)$ for M such that $y_1 = (g/\gamma)x_1 + (ur_2/\gamma)x_2 + \cdots + (ur_n/\gamma)x_n$, and by construction we have $\gamma y_1 = 0$. Due to the minimality property of x_1 (or d), the element γ cannot have less prime divisors than d. (Thus necessarily $d \neq 0$.) On the other hand, we have $\gamma \mid g$ and $g \mid d$, so that γ is a divisor of d. These two facts imply that d and γ are associates, i.e., differ only by multiplication with a unit of R. Since γ is a divisor of r_1 by construction, then so is d, as claimed. Thus the directness of the sum $(\star)$ is established. Since, by induction hypothesis, the submodule $Rx_2 + \cdots + Rx_n$ decomposes into a direct sum of $n-1$ cyclic submodules, the induction step is concluded. (Note that $Rx_2 + \cdots + Rx_n$ is not generated by less than $n-1$ elements because otherwise M would be generated by less than n elements.) □

The argument in the proof can be easily extended to show that d divides each coefficient r_i in any relation $r_1 x_1 + \cdots + r_n x_n = 0$. This observation can be exploited to derive the invariant factor decomposition for the module under consideration. However, the form of the theorem presented here fully suffices to derive the Jordan canonical form for nilpotent endomorphisms of a finite-dimensional vector space over a field K (and hence the Jordan canonical form for arbitrary endomorphisms if the field K is algebraically closed).

References

[1] Joseph R. Rotman: *An Introduction to the Theory of Groups*; Springer, New York 1995.

[2] `https://mathoverflow.net/questions/12009/is-there-a-slick-proof-of-the-classification-of-finitely-generated-abelian-group`

[3] Louis Halle Rowen: *Graduate Algebra: Commutative View*, American Mathematical Society, Providence (Rhode Island) 2006; Chapter 2, Exercises 15–17.

Karlheinz Spindler
Hochschule RheinMain
Kurt-Schumacher-Ring 18
D-65197 Wiesbaden, Germany