

AN ELEMENTARY AND CONSTRUCTIVE PROOF OF GROTHENDIECK'S GENERIC FREENESS LEMMA

INGO BLECHSCHMIDT

ABSTRACT. We present a new and direct proof of Grothendieck's generic freeness lemma in its general form. Unlike the previously published proofs, it does not proceed in a series of reduction steps and is fully constructive, not using the axiom of choice or even the law of excluded middle. It was found by unwinding the result of a general topos-theoretic technique.

We prove Grothendieck's generic freeness lemma in the following form.

Theorem 1. *Let A be a reduced ring (commutative, with unit). Let B be an A -algebra of finite type. Let M be a finitely generated B -module. If $f = 0$ is the only element of A such that*

- (1) *the $A[f^{-1}]$ -modules $B[f^{-1}]$ and $M[f^{-1}]$ are free,*
- (2) *the $A[f^{-1}]$ -algebra $B[f^{-1}]$ is of finite presentation and*
- (3) *the $B[f^{-1}]$ -module $M[f^{-1}]$ is finitely presented,*

then $1 = 0$ in A .

Previously known proofs either only cover the case where A is a Noetherian integral domain, where one can argue by *dévissage* (see for instance [5, Lemme 6.9.2], [7, Thm. 24.1] or [6, Thm. 14.4]), or proceed in a series of intermediate steps, reducing to that case (see for instance [9] or [10, Tag 051Q]); but in fact, a direct proof is possible and shorter. The new proof unveils a certain combinatorial aspect to Grothendieck's generic freeness lemma, does not require any advanced prerequisites in commutative algebra and does not use the axiom of choice or the law of excluded middle. It is purely element-based, not referring to ideals of A , and doesn't use Noether normalization.

Grothendieck's generic freeness lemma is often presented in contrapositive form or in the following geometric variant:

Theorem 2. *Let A be a reduced ring. Let B be an A -algebra of finite type. Let M be a finitely generated B -module. Then the space $\mathrm{Spec}(A)$ contains a dense open U such that over U ,*

- (a) *B^\sim and M^\sim are locally free as sheaves of A^\sim -modules,*
- (b) *B^\sim is of finite presentation as a sheaf of A^\sim -algebras and*
- (c) *M^\sim is finitely presented as a sheaf of B^\sim -modules.*

Theorem 2 immediately follows from Theorem 1 by defining U as the union of all those basic opens $D(f)$ such that (1), (2) and (3) hold. It is clear that (a), (b) and (c) hold over U , and U is dense for if V is an arbitrary open such that $U \cap V = \emptyset$, the open V is itself empty: Let $h \in A$ be such that $D(h) \subseteq V$. The hypothesis implies the assumptions of Theorem 1 for the datum $(A[h^{-1}], B[h^{-1}], M[h^{-1}])$. Thus $1 = 0 \in A[h^{-1}]$, so h is nilpotent and $D(h) = \emptyset$.

The new proof was found using a general topos-theoretic technique which we believe to be useful in other situations as well. This technique allows to view reduced rings and their modules from a different point of view, one from which reduced rings look like fields. Since Grothendieck's generic freeness is trivial for fields, this technique yields a trivial proof for reduced rings. The proof presented here was obtained by unwinding the topos-theoretic proof, yielding a self-contained argument without any references to topos theory. We refer readers who want to learn about this technique to a forthcoming companion paper [2].

Acknowledgments. The proof presented here was prompted by a question by user HeinrichD on MathOverflow [4] and greatly benefited from discussions with Martin Brandenburg, who employed the constructive version in a paper of his [3]. We are grateful to Thierry Coquand and Peter Schuster for valuable advice and to Marc Nieper-Wißkirchen for carefully guiding my PhD studies [1] at the University of Augsburg, where most of the work for this paper was carried out.

1. THE PROOF OF THE FINITELY-GENERATED CASE

The following proposition is just a special instance of Grothendieck's generic freeness lemma. Its proof is easier and shorter than the proof of the general case, which is why we present it here. The general proof will not refer to this one.

Proposition 3. *Let A be a reduced ring. Let M be a finitely generated A -module. If $f = 0$ is the only element of A such that $M[f^{-1}]$ is a finite free $A[f^{-1}]$ -module, then $1 = 0$ in A .*

Proof. We proceed by induction on the length of a given generating family of M . Let M be generated by (v_1, \dots, v_m) .

We show that the family (v_1, \dots, v_m) is linearly independent. Let $\sum_i a_i v_i = 0$. Over $A[a_i^{-1}]$, the vector $v_i \in M[a_i^{-1}]$ is a linear combination of the other generators. Thus $M[a_i^{-1}]$ can be generated as an $A[a_i^{-1}]$ -module by fewer than m generators. The induction hypothesis, applied to this module, yields that $1 = 0$ in $A[a_i^{-1}]$. Since A is reduced, this amounts to $a_i = 0$.

We finish by using the assumption for $f = 1$. \square

We remark that the proof takes a somewhat curious course: Our goal is to verify $1 = 0$, but as an intermediate step we verify that M is free, which after the fact will be a trivial statement. The general proof in the next section will have a similar style. This approach is reminiscent of Richman's uses of trivial rings [8].

2. THE PROOF OF THE GENERAL CASE

Proof of Theorem 1. Let B be generated by (x_1, \dots, x_n) as an A -algebra and let M be generated by (v_1, \dots, v_m) as a B -module. We endow the sets

$$\mathcal{I} := \{(i_1, \dots, i_n) \mid i_1, \dots, i_n \geq 0\} \quad \text{and} \\ \mathcal{J} := \{(\ell, i_1, \dots, i_n) \mid 1 \leq \ell \leq m, i_1, \dots, i_n \geq 0\}$$

with the lexicographic order. The family $(w_J)_{J \in \mathcal{J}} := (x_1^{i_1} \cdots x_n^{i_n} v_\ell)_{(\ell, i_1, \dots, i_n) \in \mathcal{J}}$ generates M as an A -module, and we will call a subfamily $(w_J)_{J \in \mathcal{J}' \subseteq \mathcal{J}}$ *good* if and only if for all $J \in \mathcal{J}$, the vector w_J is a linear combination of the vectors $(w_{J'})_{J' \in \mathcal{J}', J' \preceq J}$, and if $(\ell, i_1, \dots, i_n) \notin \mathcal{J}'$ implies $(\ell, k_1, \dots, k_n) \notin \mathcal{J}'$ for all $k_1 \geq i_1, \dots, k_n \geq i_n$. Figure 1 shows how a good generating family can look like. Similarly, we define

when a subfamily of the canonical generating family $(x_1^{i_1} \cdots x_n^{i_n})_{(i_1, \dots, i_n) \in \mathcal{I}}$ of B is good (which is just the special case $m = 1$).

We then proceed by induction on the shapes of a given good generating family $(w_J)_{J \in \mathcal{J}'}$ for M and a given good generating family $(s_I)_{I \in \mathcal{I}'}$ for B , starting with the canonical ones. It is reasonably obvious that this induction is well-founded; the formal statement that it is so is known as *Dickson's Lemma* (see, for instance, [11, Thm. 1.1]).

We show that $(w_J)_{J \in \mathcal{J}'}$ is a basis of M by verifying linear independence. Thus let $\sum_J a_J w_J = 0$ in M . We show that all coefficients in this sum are zero, starting with the largest appearing index J : In the module $M[a_J^{-1}]$ over the localized ring $A[a_J^{-1}]$, the vector w_J is a linear combination of generators with smaller index. Removing $w_J = x_1^{i_1} \cdots x_n^{i_n} v_\ell$ and also all vectors $x_1^{k_1} \cdots x_n^{k_n} v_\ell$ where $k_1 \geq i_1, \dots, k_n \geq i_n$, we obtain a subfamily which is still good for the localized module. The induction hypothesis, applied to $A[a_J^{-1}]$ and its module $M[a_J^{-1}]$, therefore implies that $A[a_J^{-1}] = 0$. Thus $a_J = 0$ since A is reduced.

Similarly, we show that the given good generating family $(s_I)_{I \in \mathcal{I}'}$ is a basis. Thus M and B are free over A . We fix for any corner J of \mathcal{J}' , as indicated in Figure 1, a way of expressing $w_J = \sum_K a_{JK} w_K$ as a linear combination of generators with strictly smaller index. Let $\widehat{w}_{(\ell, i_1, \dots, i_n)} := x_1^{i_1} \cdots x_n^{i_n} v_\ell$ in the free B -module $B\langle V_1, \dots, V_m \rangle$. The canonical map

$$\widehat{M} := B\langle V_1, \dots, V_m \rangle / (\widehat{w}_J - \sum_K a_{JK} \widehat{w}_K)_{J \text{ corner of } \mathcal{J}'} \longrightarrow M$$

is trivially well-defined and surjective. It is also injective, since any element of \widehat{M} can be written as an A -linear combination of the vectors $(\widehat{w}_J)_{J \in \mathcal{J}'}$ by employing the corner relations a finite number of times. Therefore M is finitely presented as a B -module.

In a similar vein, a quotient algebra of $A[X_1, \dots, X_n]$, where we mod out by a suitable ideal with as many generators as corners of \mathcal{I}' , is isomorphic to B . Thus B is finitely presented as an A -algebra.

We finish by using the assumption for $f = 1$. □

3. CONCLUSION

Commutative algebra abounds with techniques which allow us to reduce quite general situations to easier ones. These techniques often yield short and slick proofs; however, they come at an expense: They are typically nonconstructive in nature, employing for instance the axiom of choice, and do not argue using only the data at hand, but using additional auxiliary objects such as maximal ideals. We feel that once a subject is better understood, it is desirable to have more informative, direct proofs available which illuminate the statement more clearly; similar as to how bijective proofs are preferred over calculational inductive ones in combinatorics.

Let us consider as a specific example the statement that the existence of a linear surjection $A^n \rightarrow A^m$ with $n < m$ between finite free modules over an arbitrary ring A implies $1 = 0 \in A$. The standard proof of this fact proceeds by contradiction and passes to the quotient A/\mathfrak{m} , where \mathfrak{m} is a maximal ideal of A , thereby reducing to the situation that the ring is a field. In contrast, a direct proof such as Richman's [8] refers only to objects mentioned in the statement itself and explicitly tells us how

$x^0 y^7 v_1$	$x^1 y^7 v_1$	$x^2 y^7 v_1$	$x^3 y^7 v_1$	$x^4 y^7 v_1$	$x^5 y^7 v_1$	$x^6 y^7 v_1$	$x^7 y^7 v_1$
$x^0 y^6 v_1$	$x^1 y^6 v_1$	$x^2 y^6 v_1$	$x^3 y^6 v_1$	$x^4 y^6 v_1$	$x^5 y^6 v_1$	$x^6 y^6 v_1$	$x^7 y^6 v_1$
$x^0 y^5 v_1$	$x^1 y^5 v_1$	$x^2 y^5 v_1$	$x^3 y^5 v_1$	$x^4 y^5 v_1$	$x^5 y^5 v_1$	$x^6 y^5 v_1$	$x^7 y^5 v_1$
$x^0 y^4 v_1$	$x^1 y^4 v_1$	$x^2 y^4 v_1$	$x^3 y^4 v_1$	$x^4 y^4 v_1$	$x^5 y^4 v_1$	$x^6 y^4 v_1$	$x^7 y^4 v_1$
$x^0 y^3 v_1$	$x^1 y^3 v_1$	$x^2 y^3 v_1$	$x^3 y^3 v_1$	$x^4 y^3 v_1$	$x^5 y^3 v_1$	$x^6 y^3 v_1$	$x^7 y^3 v_1$
$x^0 y^2 v_1$	$x^1 y^2 v_1$	$x^2 y^2 v_1$	$x^3 y^2 v_1$	$x^4 y^2 v_1$	$x^5 y^2 v_1$	$x^6 y^2 v_1$	$x^7 y^2 v_1$
$x^0 y^1 v_1$	$x^1 y^1 v_1$	$x^2 y^1 v_1$	$x^3 y^1 v_1$	$x^4 y^1 v_1$	$x^5 y^1 v_1$	$x^6 y^1 v_1$	$x^7 y^1 v_1$
$x^0 y^0 v_1$	$x^1 y^0 v_1$	$x^2 y^0 v_1$	$x^3 y^0 v_1$	$x^4 y^0 v_1$	$x^5 y^0 v_1$	$x^6 y^0 v_1$	$x^7 y^0 v_1$

FIGURE 1. A graphical depiction of a good generating family (the non-hatched cells) in the special case $n = 2, m = 1$, writing “ x ” and “ y ” for x_1 and x_2 . The hatched cells indicate vectors which have already been removed from the family. The small black squares indicate *corners*. If the vector in the red cell will be found to be expressible as a linear combination of vectors with smaller index (blue cells), it will be removed, along with the vectors in all cells to the top and to the right of the red cell.

to deduce the equation $1 = 0$ from the m equations which express that each basis vector of A^m has a preimage.

In a similar fashion, the new proof of Grothendieck’s generic freeness lemma explicitly tells us how to deduce $1 = 0$ from the given conditional equations expressing that $f = 0$ is the only element with properties (1), (2) and (3). The history of Grothendieck’s generic freeness lemma goes back more than fifty years; we are slightly surprised that a direct proof was discovered only now.

Direct proofs sometimes generalize to new situations where the reduction techniques employed in more abstract proofs cannot be applied. This is the case for Grothendieck’s generic freeness lemma, which allows for the following generalization:

Theorem 4. *Let (X, \mathcal{O}_X) be a ringed space (or ringed locale, or ringed topos), such that for every local section s of \mathcal{O}_X , if the only open on which s is invertible is the empty one, then $s = 0$. Let \mathcal{B} be a sheaf of \mathcal{O}_X -algebras of finite type. Let \mathcal{E} be a sheaf of \mathcal{B} -modules of finite type. Then there is a dense open U such that over U ,*

- (a) \mathcal{B} and \mathcal{E} are locally free as sheaves of \mathcal{O}_X -modules,
- (b) \mathcal{B} is of finite presentation as a sheaf of \mathcal{O}_X -algebras and
- (c) \mathcal{E} is finitely presented as a sheaf of \mathcal{B} -modules.

Proof. The proof of Theorem 1 can be easily adapted to this more general setting. Where that proof concludes $a_J = 0$ for ring elements a_J by considering the localized situation $A[a_J^{-1}]$, we now conclude $a_J = 0$ for local sections a_J of \mathcal{O}_X by considering the situation over the restriction to $D(a_J)$. It is then the assumption on X instead

of the reducedness assumption on A which allows us to conclude $a_J = 0$. We omit further details. \square

The spectrum of a ring A is a space of the kind required by Theorem 4 if and only if A is reduced, thus Theorem 4 indeed generalizes Theorem 2. Further examples for admissible spaces are given by any topological, smooth or complex manifold; a corollary of Theorem 4 for these examples is that quotients of vector bundles, computed in the category of sheaves of modules, are again vector bundles after restricting to suitable dense opens.

It is hard to say with certainty that a given proof does not generalize to a new situation; but we do not see how this could be the case with the proofs cited in the introduction.

REFERENCES

- [1] I. Blechschmidt. “Using the internal language of toposes in algebraic geometry”. PhD thesis. University of Augsburg, 2017. URL: <https://rawgit.com/iblech/internal-methods/master/notes.pdf>.
- [2] I. Blechschmidt. “Without loss of generality, any reduced ring is a field”. 2018, in preparation.
- [3] M. Brandenburg. “Operations on categories of modules are given by Schur functors”. 2016. URL: <https://arxiv.org/abs/1610.02180>.
- [4] MathOverflow contributors. *Constructive proof that a kernel consists of nilpotent elements (thread started by HeinrichD)*. 2016. URL: <https://mathoverflow.net/questions/250040>.
- [5] J. Dieudonné and A. Grothendieck. “Éléments de géométrie algébrique: IV. Étude locale des schémas et des morphismes de schémas, Seconde partie”. In: *Publ. Math. Inst. Hautes Études Sci.* 24 (1965).
- [6] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Vol. 150. Grad. Texts in Math. Springer, 1995.
- [7] H. Matsumura. *Commutative ring theory*. Vol. 8. Cambridge Stud. Adv. Math. Cambridge University Press, 1987.
- [8] F. Richman. “Nontrivial uses of trivial rings”. In: *Proc. Amer. Math. Soc.* 103 (1988), pp. 1012–1014.
- [9] C. Staats. *Elementary proof of generic freeness*. 2011. URL: https://math.uchicago.edu/~cstaats/Charles_Staats_III/Notes_and_papers_files/generic_freeness.pdf.
- [10] The Stacks Project Authors. *Stacks Project*. URL: <https://stacks.math.columbia.edu/>.
- [11] W. Veldman. “An intuitionistic proof of Kruskal’s theorem”. In: *Arch. Math. Logic* 43.2 (2004), pp. 215–264.

MAX PLANCK INSTITUTE FOR MATHEMATICS IN THE SCIENCES, INSELSTRASSE 22, 04103 LEIPZIG, GERMANY

E-mail address: ingo.blechschmidt@mis.mpg.de