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 doesn't proceed in a series of reduction steps and is fully constructive, not involving 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 for rings and modules in the following form.

Theorem 1. *Let A be a reduced ring. 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 proceed in a series of intermediate steps, reducing to the case that A is a Noetherian integral domain where one can argue by *dévissage*; but in fact, a direct proof is possible and shorter.

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* $\operatorname{Spec}(A)$ *contains a dense open U such that over U,*

(a) *$B^\sim$ and $M^\sim$ are 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 the basic opens $D(f)$ such that (1), (2), and (3) hold. It's 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 $h \in A$ 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-theoretical 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 an accompanying note [?].

XXX: Acknowledgments, especially Martin Brandenburg

XXX: References to prior proofs: EGA, Stacks Project, Charles Staats. Check this MO question

1. The proof of the general case

Lemma 3. *Let A be a ring. Let M be an A-module with generating family $(x_i)_{i\in I}$ where I is a totally ordered set. Assume that the only element $g \in A$ such that one of the x_i is an $A[g^{-1}]$-linear combination in $M[g^{-1}]$ of other generators with smaller index is $g = 0$. Then M is free with $(x_i)_{i\in I}$ as a basis.*

Proof. Let $\sum_i a_i x_i = 0$. Starting with the greatest index i which appears in that sum, we see that in $M[a_i^{-1}]$, the element x_i is an $A[g^{-1}]$-linear combination of other generators with smaller index. Thus $a_i = 0$ by assumption. □

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

$$I := \{(i_1, \ldots, i_n) \mid i_1, \ldots, i_n \in \{0, 1, \ldots\}\} \quad \text{and}$$
$$J := \{(\ell, i_1, \ldots, i_n) \mid \ell \in \{1, \ldots, m\}, i_1, \ldots, i_n \in \{0, 1, \ldots\}\}$$

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

Similarly, we define when a subfamily of the canonical generating family $(x_1^{i_1} \cdots x_n^{i_n})_{(i_1,\ldots,i_n)\in I}$ 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 $(w_j)_{j\in J'}$ for M and a given good generating family $(s_i)_{i\in I'}$ for B, starting with the canonical ones.

We show that $(w_j)_{j\in J'}$ is a basis of M by verifying the assumptions of Lemma 3. Thus let $g \in A$ be given such that one of the w_j is an $A[g^{-1}]$-linear combination of generators with smaller index in $M[g^{-1}]$. 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 $k_1 \geq i_1, \ldots, k_n \geq i_n$, we obtain a subfamily which is still good for the $A[g^{-1}]$-module $M[g^{-1}]$. By induction, applied to $A[g^{-1}]$ and its module $M[g^{-1}]$, it therefore follows that $A[g^{-1}] = 0$. This implies that $g = 0$ since A is reduced.

Similarly, we show that the given good generating family $(s_i)_{i\in I'}$ is a basis. Thus M and B are free over A. We fix for any corner $j = (\ell, i_1, \ldots, i_n) \in J$, as indicated in Figure 1, a way of expressing $x^{i_1} \cdots x^{i_n} v_\ell = \sum_{(p,k_1,\ldots,k_n)} a_{j;p,k_1,\ldots,k_n} x^{k_1} \cdots x^{k_n} v_p$ as a linear combination of generators with strictly smaller index. Then M is isomorphic to the B-module

$$B\langle V_1, \ldots, V_m\rangle / (x^{i_1} \cdots x^{i_n} V_\ell - \textstyle\sum_{(p,k_1,\ldots,k_n)} a_{j;p,k_1,\ldots,k_n} x_{k_1} \cdots x_{k_n} V_p)_j,$$

where the index j ranges over all corners of J, and therefore finitely presented. In a similar vain, a quotient algebra of $A[X_1, \ldots, X_n]$, where we mod out a suitable ideal with as many generators as corners of I, is isomorphic to B.

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

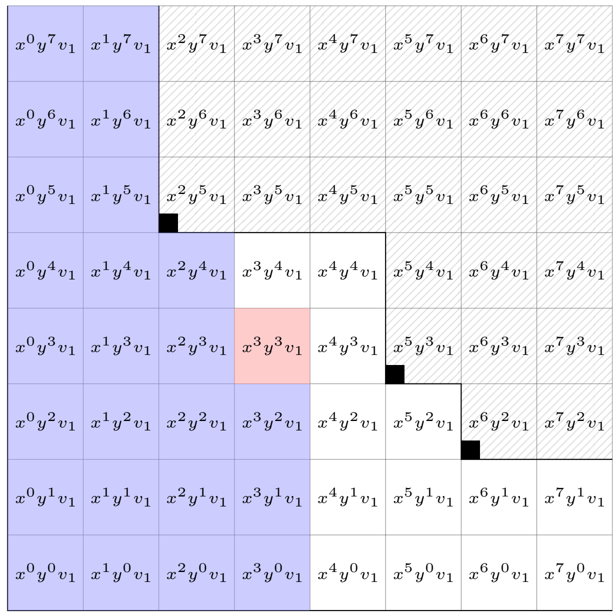

FIGURE 1. A graphical depiction of a good generating family in the special case $n = 2, m = 1$. The hatched cells indicate vectors which have already been removed from the family. If the vector in the red cell will be found to be expressible as a linear combination of vectors with smaller index (blue cells), it will be removed, along with the vectors in all cells to the top and to the right of the red cell. Corners are indicated by the small black squares.

2. THE PROOF OF THE FINITELY-GENERATED CASE

The following proposition is just an instance of Grothendieck's generic freeness lemma. We prove it here because it admits an easier proof.

Proposition 4. *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 $f = 1$. □