JOURNAL OF COMMUTATIVE ALGEBRA
Volume 5, Number 2, Summer 2013

A UNIVERSAL COEFFICIENT THEOREM FOR GAUSS'S LEMMA

WILLIAM MESSING AND VICTOR REINER

To Jürgen Herzog on his 70th birthday

ABSTRACT. We shall prove a version of Gauß's lemma. It works in $\mathbf{Z}[\mathbf{a}, \mathbf{A}, \mathbf{b}, \mathbf{B}]$ where $\mathbf{a} = \{a_i\}_{i=0}^m$, $\mathbf{A} = \{A_i\}_{i=0}^m$, $\mathbf{b} = \{b_i\}_{j=0}^n$, $\mathbf{B} = \{B_j\}_{j=0}^n$, and constructs polynomials $\{c_k\}_{k=0,\dots,m+n}$ of degree at most $\binom{m+n}{n}$ in each variable set $\mathbf{a}, \mathbf{A}, \mathbf{b}, \mathbf{B}$, with this property: setting

$$\sum_k C_k X^k = \sum_i A_i X^i \cdot \sum_j B_j X^j;$$

for elements a_i, A_i, b_j, B_j in any commutative ring R satisfying

$$1 = \sum_i a_i A_i = \sum_j b_j B_j,$$

the elements $c_k = c_k(a_i, A_i, b_j, B_j)$ satisfy $1 = \sum_k c_k C_k$.

1. The statement. Let R be a commutative ring. Consider two elements $A(X) = \sum_{i=0}^m A_i X^i$ and $B(X) = \sum_{j=0}^n B_j X^j$ in $R[X]$, with the product $C(X) = A(X)B(X) = \sum_{k=0}^{m+n} C_k X^k$, so that one has $C_k = \sum_{i+j=k} A_i B_j$. A version of Gauß's lemma, called *Gauß-Joyal de pauvre* in [**6**, Section II, Lemma 2.6], asserts the following.

Proposition 1. *If both $A(X), B(X)$ have the property that their coefficient sequences generate the unit ideal R, then the same is true of their product $C(X)$, that is, $(A_0, \dots, A_m) = R = (B_0, \dots, B_n)$ implies $(C_0, \dots, C_{m+n}) = R$.*

2010 AMS *Mathematics subject classification.* Primary 13P05, 14Q20, 12Y05.
Keywords and phrases. Gauss lemma, constructive.
The second author was partially supported by NSF grant DMS-1001933.
Received by the editors on September 26, 2012, and in revised form on October 23, 2012.
DOI:10.1216/JCA-2013-5-2-299

Standard proofs of this appeal to Zorn's lemma or some weaker version, to show that if the ideal $(C_0, \dots, C_{m+n})$ is not R, then it is contained in some maximal ideal $\mathfrak{m}$ of R. This leads to the contradiction in the integral domain $R/\mathfrak{m}[X]$, that $A(X), B(X)$ represent nonzero elements but their product represents zero. Gauß's lemma has several proofs avoiding any version of Zorn's lemma; we discuss some of these in Section 4 below.

Our goal here, however, is a construction of "universal" coefficients $c_0, \dots, c_{m+n}$ satisfying $1 = \sum_{k=0}^{m+n} c_k C_k$, expressed in terms of any a_i, b_j in R that satisfy

$$1 = \sum_{i=0}^{m} a_i A_i = \sum_{j=0}^{n} b_j B_j. \tag{1.1}$$

To do this, we work in a polynomial algebra,

$$S = \mathbf{Z}[\mathbf{a}, \mathbf{b}, \mathbf{A}, \mathbf{B}] = \mathbf{Z}[a_0, \dots, a_m, b_0, \dots, b_n, A_0, \dots, A_m, B_0, \dots, B_n]$$

and consider the elements

$$a := 1 - \sum_{i=0}^{m} a_i A_i, \qquad b := 1 - \sum_{j=0}^{n} b_j B_j, \qquad C_k := \sum_{i+j=k} A_i B_j, \tag{1.2}$$

for $k = 0, 1, \dots, m+n$. We shall prove the following equivalent of Gauß's lemma.

Proposition 2. *There exist in S polynomials $\alpha, \beta, c_0, c_1, \dots, c_{m+n}$ expressing*

$$1 = \alpha a + \beta b + \sum_{k=0}^{m+n} c_k C_k. \tag{1.3}$$

Consequently, for any commutative ring R and elements satisfying (1.1), the elements $c_k = c_k(\mathbf{a}, \mathbf{b}, \mathbf{A}, \mathbf{B})$ will satisfy $1 = \sum_{k=0}^{m+n} c_k C_k$ in R.

2. A proof which is not explicit. We first give a proof of the existence of polynomials α, β, c_k as in Proposition 2, via induction on $m+n$. In Section 3 below, we will reinterpret it to give explicit recursive formulas for α, β, c_k. These formulas also lead to a simple bound (Proposition 4 below) on the degrees of α, β, c_k when considered as polynomials in each of the variable sets $\mathbf{a}, \mathbf{b}, \mathbf{A}, \mathbf{B}$.

For the base case of the induction, let $m = n = 0$. One then checks directly that $\alpha = 1$, $\beta = a_0 A_0$ and $c_0 = a_0 b_0$ suffice:

$$1 = 1 \cdot (1 - a_0 A_0) + a_0 A_0 \cdot (1 - b_0 B_0) + a_0 b_0 \cdot A_0 B_0.$$

In the induction on $m+n$, it will be important to emphasize the dependence of various objects on m, n. Changing notation, denote by $S^{(m,n)}$ the polynomial ring S, and denote by $a^{(m)}, b^{(n)}, C_k^{(m,n)}$ the elements a, b, C_k appearing in (1.2). Let $Q^{(m,n)}$ denote the quotient ring of $S^{(m,n)}$ by the ideal generated by these elements. Proposition 2 then asserts $1 = 0$ in $Q^{(m,n)}$, that is, $Q^{(m,n)}$ is the zero ring.

One easily checks the following comparisons for $m, n \geq 1$

$$\begin{aligned} a^{(m-1)} &= a^{(m)} + a_m A_m, \\ b^{(n-1)} &= b^{(n)} + b_n B_n, \\ C_k^{(m-1,n)} &= \begin{cases} C_k^{(m,n)} & \text{if } k < m, \\ C_k^{(m,n)} - A_m B_{k-m} & \text{if } k \geq m, \end{cases} \\ C_k^{(m,n-1)} &= \begin{cases} C_k^{(m,n)} & \text{if } k < n, \\ C_k^{(m,n)} - A_{k-n} B_n & \text{if } k \geq n, \end{cases} \end{aligned} \tag{2.1}$$

which show that the principal ideals $(A_m), (B_n)$ satisfy[1]

$$\begin{aligned} Q^{(m,n)}/(A_m) &\cong Q^{(m-1,n)} \quad \text{for } m \geq 1, \\ Q^{(m,n)}/(B_n) &\cong Q^{(m,n-1)} \quad \text{for } n \geq 1. \end{aligned} \tag{2.2}$$

Now, assuming that $m+n \geq 1$, one has $Q^{(m,n)}/(B_n) \cong Q^{(m,n-1)} = 0$ using (2.2) and induction. Hence, it suffices to show that the ideal $(B_n) = 0$. Note that multiplication by B_n gives rise to a surjection $Q^{(m,n)} \twoheadrightarrow (B_n)$ that factors through $Q^{(m,n)}/(A_m)$, since A_m annihilates B_n. As $Q^{(m,n)}/(A_m) \cong Q^{(m-1,n)} = 0$, by (2.2) and induction, this shows $(B_n) = 0$, completing the proof.

3. The explicit recursions. Here we recursively produce, for $m, n \geq 0$, polynomials $\alpha^{(m,n)}, \beta^{(m,n)}, c_k^{(m,n)}$ in the ring $S = S^{(m,n)}$ with the property that

$$1 = \alpha^{(m,n)} a^{(m)} + \beta^{(m,n)} b^{(n)} + \sum_{k=0}^{m+n} c_k^{(m,n)} C_k^{(m,n)}. \tag{3.1}$$

One easily checks that, when $m = 0$, one can choose:

$$\alpha^{(0,n)} = 1, \qquad \beta^{(0,n)} = a_0 A_0, \qquad c_k^{(0,n)} = a_0 b_k. \tag{3.2}$$

By symmetry, when $n = 0$ one can choose:

$$\alpha^{(m,0)} = b_0 B_0, \qquad \beta^{(m,0)} = 1, \qquad c_k^{(m,0)} = a_k b_0. \tag{3.3}$$

For definiteness, when $m = n = 0$, we choose to use (3.2) instead of (3.3).

Now assume that $m, n > 0$. By induction on $m+n$, assume that one has constructed $\alpha^{(m,n-1)}, \beta^{(m,n-1)}, c_k^{(m,n-1)}, \alpha^{(m-1,n)}, \beta^{(m-1,n)}, c_k^{(m-1,n)}$ satisfying:

$$1 = \alpha^{(m,n-1)} a^{(m)} + \beta^{(m,n-1)} b^{(n-1)} + \sum_{k=0}^{m+n-1} c_k^{(m,n-1)} C_k^{(m,n-1)},$$

$$1 = \alpha^{(m-1,n)} a^{(m-1)} + \beta^{(m-1,n)} b^{(n)} + \sum_{k=0}^{m+n-1} c_k^{(m-1,n)} C_k^{(m-1,n)}.$$

Using (2.1), these become

$$1 = \alpha^{(m,n-1)} a^{(m)} + \beta^{(m,n-1)} b^{(n)} + \sum_{k=0}^{m+n-1} c_k^{(m,n-1)} C_k^{(m,n)} + B_n d \tag{3.4}$$

$$1 = \alpha^{(m-1,n)} a^{(m)} + \beta^{(m-1,n)} b^{(n)} + \sum_{k=0}^{m+n-1} c_k^{(m-1,n)} C_k^{(m,n)} + A_m e, \tag{3.5}$$

where we have used two auxiliary polynomials

$$
\begin{aligned}
d &= b_n\beta^{(m,n-1)} - \sum_{k=n}^{m+n-1} c_k^{(m,n-1)} A_{k-n}, \\
e &= a_m\alpha^{(m-1,n)} - \sum_{k=m}^{m+n-1} c_k^{(m-1,n)} B_{k-m}.
\end{aligned} \tag{3.6}
$$

Now one can use (3.5) to replace d in (3.4) by

$$
d = d\cdot 1 = d\Big(\alpha^{(m-1,n)}a^{(m)} + \beta^{(m-1,n)}b^{(n)} + \sum_{k=0}^{m+n-1} c_k^{(m-1,n)}C_k^{(m,n)} + A_m e\Big).
$$

This yields the following expression:

$$
\begin{aligned}
1 = &\left(\alpha^{(m,n-1)} + B_n d\alpha^{(m-1,n)}\right) a^{(m)} \\
&+ \left(\beta^{(m,n-1)} \quad + B_n d\beta^{(m-1,n)}\right) b^{(n)} \\
&\quad + \sum_{k=0}^{m+n-1} \left(c_k^{(m,n-1)} + B_n d c_k^{(m-1,n)}\right) C_k^{(m,n)} + de\cdot A_m B_n.
\end{aligned}
$$

Thus, if one recursively defines

$$
\begin{aligned}
\alpha^{(m,n)} &= \alpha^{(m,n-1)} + B_n d\alpha^{(m-1,n)}, \\
\beta^{(m,n)} &= \beta^{(m,n-1)} + B_n d\beta^{(m-1,n)}, \\
c_k^{(m,n)} &= c_k^{(m,n-1)} + B_n d c_k^{(m-1,n)} \text{ for } k = 0, 1, \dots, m+n-1 \\
c_{m+n}^{(m,n)} &= de \quad (\text{since } C_{m+n}^{(m,n)} = A_m B_n),
\end{aligned} \tag{3.7}
$$

then one obtains coefficients satisfying (3.1). We have thus proved the following.

Proposition 3. *The polynomials* $\alpha^{(m,n)}, \beta^{(m,n)}, c_k^{(m,n)}$ *defined by recursions* (3.7) *and* (3.6)*, with initial conditions given by* (3.2) *and* (3.3)*, satisfy* (3.1) (*and* (1.3)).

TABLE 1.

upper bound on total degree	in $\mathbf{a}$	in $\mathbf{b}$	in $\mathbf{A}$	in $\mathbf{B}$
for $\alpha^{(m,n)}$	$N-1$	$N-1$	$N-1$	$N-1$
for $\beta^{(m,n)}$	N	$N-1$	N	$N-1$
for $c_k^{(m,n)}$	N	N	$N-1$	$N-1$
for d	N'	N'	N'	$N'-1$
for e	N''	N''	$N''-1$	N

Proposition 4. *The polynomials $\alpha^{(m,n)}, \beta^{(m,n)}, c_k^{(m,n)}$ in Proposition 3 have degree bounded by $\binom{m+n}{m}$ in each variable set $\mathbf{a}, \mathbf{b}, \mathbf{A}, \mathbf{B}$.*

To establish this, we use induction on $m+n$ to prove a slightly more precise statement. Let $N := \binom{m+n}{m}$, $N' := \binom{m+n-1}{m}$, $N'' := \binom{m+n-1}{m-1}$ so that $N = N' + N''$. It is straightforward to check that the bounds on the total degree in Table 1 are valid in each variable set for the elements defined via the above recursions.

Question 5. Is there a good *lower* bound on the degree of α, β, c_k in Proposition 2?

4. Historical remarks.

4.1. Trivial rings. The idea from the proof in Section 2 to show that the ring $Q^{(m,n)}$ is trivial is not at all new. See Richman [**12**] for four examples of this idea, applied in a constructive manner, to prove results in commutative algebra.

4.2. Lemmas of Artin, Dedekind-Mertens, Gauss-Joyal, Kronecker and McCoy. Gauß's lemma is closely related to various results due to Artin, Dedekind-Mertens, Gauß-Joyal, Kronecker and McCoy. Proofs of these results avoiding any variants of Zorn's lemma, as well as the relations between them and their history, are beautifully discussed by Coquand, Ducos, Lombardi and Quitté [**2**], and in the book by Lombardi and Quitté [**6**, Section II Lemma 2.6, Section III.2, Section III.3, Exercise III-6 and Problem IX-3].

4.3. Zorn's lemma versus existence of maximal ideals. As mentioned in Section 1, standard proofs of Gauß's lemma appeal not to Zorn's lemma itself, but to the existence for a proper ideal in a commutative ring, of a maximal ideal containing it. As shown by Hodges [**5**], already the existence of maximal ideals in unique factorization domains implies the axiom of choice. However, for traditional proofs of Gauß's lemma, it suffices to know that any proper ideal is contained in a prime ideal. To explain this, recall that a *Boolean ring* is a ring, necessarily commutative, in which every element is idempotent. The fact that non-trivial Boolean rings contain prime (and hence maximal) ideals was proven by Stone [**15**] and is called the prime ideal theorem for Boolean rings. It was announced by Scott [**14**] that this implies that any non-trivial commutative ring has a prime ideal. Proofs of this result are given in Banaschewski [**1**] and Rav [**11**]. Perhaps the simplest proof, which the first author learned from Gabber, is based upon the fact, proven in Olivier [**9**], that any commutative ring, R, has an homomorphism $R \to T(R)$ to a *von-Neumann regular* commutative ring, also called an *absolutely flat ring*, which is universal for homomorphisms to absolutely flat rings. The set of idempotents $E(R)$ of $T(R)$ form a Boolean ring where the sum of idempotents, e and e' is given by $e + e' - 2ee'$. The proof concludes by showing (see Popescu and Vraciu [**10**]) that the map $\mathfrak{p} \mapsto \mathfrak{p} \cap E(R)$ gives a bijection $\operatorname{Spec}(T(R)) \to \operatorname{Spec}(E(R))$. Halpern and Lévy [**3**] proved that the prime ideal theorem is strictly weaker than the axiom of choice. Finally note that, for non-trivial finitely generated $\mathbf{Z}$-algebras, the existence of maximal ideals does not require Zorn's lemma, and is proven in Hodges [**4**].

4.4. The McCoy-Nagata lemma instead of Zorn's. We mention here an alternate proof of Proposition 2, avoiding Zorn's lemma, which can be deduced from a lemma of McCoy [**7**], reproven by Nagata[2] in [**8**, Section 6, pages 17, 18].

There, Nagata introduces, for a commutative ring R, the set $\mathcal{S}$ of all polynomials $A(X) = \sum_{i=0}^{m} A_i X^i$ in $R[X]$ whose coefficients $\{A_i\}_{i=0}^{m}$ generate the unit ideal R. He constructs the ring of rational functions $R(X) = \mathcal{S}^{-1}R[X]$, containing $R[X]$ as a subring. To do this, he first notes that:

(i) $\mathcal{S}$ is multiplicatively closed, that is, Proposition 1 above, and

(ii) $\mathcal{S}$ contains no zero-divisors.

He offers no proof for assertion (i) but notes that (ii) is immediate from the following lemma, which he proves without recourse to Zorn.

Lemma 6 [**7**, Theorem 2], [**8**, (6.13)]. *For Q a commutative ring, a nonzero element $A(X)$ in $Q[X]$ is a zero divisor if and only if there exists $q \neq 0$ in Q such that $qA(X) = 0$.*

Lemma 6 also leads to a proof without Zorn's lemma of Proposition 2 (and hence of Gauß's lemma), as we now explain.

Choose $Q = Q^{(m,n)}$ to be the quotient of $S = \mathbf{Z}[\mathbf{a}, \mathbf{b}, \mathbf{A}, \mathbf{B}]$ by the ideal generated by $a, b, C_0, \ldots, C_{m+n}$, as in Section 2, so that Proposition 2 asserts that Q is the zero ring. Assume for the sake of contradiction that Q is *not* the zero ring. Then $A(X)$ and $B(X)$ both have nonzero images in $Q[X]$, because their coefficients generate the unit ideal of Q. However, their product $C(X)$ has zero image in $Q[X]$. Hence the image of $A(X)$ in $Q[X]$ is a zero divisor. By Lemma 6, there exists a $q \neq 0$ in Q such that $qA(X) = 0$, leading to the contradiction $q = q \cdot 1 = \sum_i a_i q A_i = 0$.

4.5. Other constructive proofs. As Richman's [**13**, Theorem 4] is proved constructively, it immediately gives an algorithmic proof of Gauß's lemma. It is likely that the same is true for the proof of [**6**, Section II, Lemma 2.6], and the McCoy-Nagata proof, discussed above, at least in the case of "discrete" rings[3].

Acknowledgments. The authors thank Kris Fowler, Nick Katz, Henri Lombardi, Ezra Miller, Fred Richman, Dennis Stanton, Volkmar Welker and the anonymous referee for helpful comments and references.

ENDNOTES

1. These isomorphisms hold even when $m = 0$ or $n = 0$, provided one adopts the convention that $Q^{(-1,n)} = Q^{(m,-1)} = 0$: the vanishing of $a^{(0)} = 1 - a_0 A_0$ in $Q^{(0,n)}$ makes A_0 a unit, and hence $Q^{(0,n)}/(A_0) = 0$.

2. We thank the referee for pointing out to us McCoy's paper. Interestingly, Nagata states [**8**, page 213] that "The writer does not know any existing literature which contains (6.13)." It is unfortunately

too late to point out this error either to Nagata, who is deceased, or to his publisher Interscience, which no longer exists.

3. A ring is said to be *discrete* provided that one can constructively decide whether an element of the ring equals zero.

REFERENCES

1. B. Banaschewski, *The power of the ultrafilter theorem*, J. Lond. Math. Soc. **27** (1983), 193–202.

2. T. Coquand, L. Ducos, H. Lombardi and C. Quitté, *L'idéal des coefficients du produit de deux polynômes*, Rev. Math. Enseign. Sup. **113** (2003), 25–39.

3. J.D. Halpern and A. Levy, *The Boolean prime ideal theorem does not imply the axiom of choice*, *Axiomatic set theory*, Proc. Symp. Pure Math. **13**, 83–134, American Mathematical Society, 1971.

4. W. Hodges, *Six impossible rings*, J. Algebra **31** (1974), 218–244.

5. ———, *Krull implies Zorn*, J. Lond. Math. Soc. **19** (1979), 285–287.

6. H. Lombardi and C. Quitté, *Algèbre commutative*: *Méthodes constructives, Modules projectifs de type fini*, Calvage and Mounet, 2011.

7. N.H. McCoy, *Remarks on divisors of zero*, Amer. Math. Month. **49** (1942), 286–295.

8. M. Nagata, *Local rings*, Inter. Tracts Pure Appl. Math. **13**, Interscience Publishers, a division of John Wiley & Sons, New York, 1962.

9. J.-P. Olivier, *Anneaux absolument universel et epimorphismes à but reduit*, Exposé VI in *Séminaire d'Algèbre Commutative dirigé par Pierre Samuel*: 1967/1968. *Les épimorphismes d'anneaux*, Secr. math., Paris, 1968 (MR # 0245561).

10. N. Popescu and C. Vraciu, *Sur la structure des anneaux absoluments plats commutatifs*, J. Algebra **40** (1976), 364–383.

11. Y. Rav, *Variants of Rado's selection lemma and their applications*, Math. Nachr. **79** (1977), 145–165.

12. F. Richman, *Nontrivial uses of trivial rings*, Proc. Amer. Math. Soc. **103** (1988), 1012–1014.

13. ———, *A division algorithm*, J. Alg. Appl. **4** (2005), 441–449.

14. D. Scott, *Prime ideal theorems for rings, lattices, and Boolean algebras*, Bull. Amer. Math. Soc. **60** (1954), 390.

15. M.H. Stone, *The theory of representations of Boolean algebras*, Trans. Amer. Math. Soc. **40** (1936), 37–111.

School of Mathematics, University of Minnesota, Minneapolis, MN 55455
Email address: messing@math.umn.edu

School of Mathematics, University of Minnesota, Minneapolis, MN 55455
Email address: reiner@math.umn.edu