

Pacific Journal of Mathematics

A REMARK ON THE LEMMA OF GAUSS

FRED KRAKOWSKI

A REMARK ON THE LEMMA OF GAUSS

FRED KRAKOWSKI

Let R be the ring of integers of some algebraic number field K and $\mathfrak{B} = R[x_0, \dots, x_r, y_0, \dots, y_s]$, where the x_i 's and y_j 's are indeterminates. Call two ideals of \mathfrak{B} equivalent, if after substitution of the indeterminates by arbitrary elements of R they always yield identical ideals in R . For example, consider the ideal I generated by the coefficients of the product of the two polynomials $f(t) = \sum_{i=0}^r x_i t^i$ and $g(t) = \sum_{j=0}^s y_j t^j$. According to the so-called Lemma of Gauss, I is equivalent to the product J of the ideals (x_0, \dots, x_r) and (y_0, \dots, y_s) .

The object of this note is to show that the ideal I has the following minimal property: It has the smallest number of generators, namely $r + s + 1$, among all ideals in \mathfrak{B} which are equivalent to J in the above sense.

LEMMA 1. *For every nonconstant polynomial $f \in R[t]$, t an indeterminate, there exist infinitely many prime ideals $P \subset R$, such that the congruence $f(x) \equiv 0 \pmod{P}$ has a solution $x \in R$.*

Proof. Denote by f_1, \dots, f_m the polynomials conjugate to f over the rationals and let $f = f_1$. Consider their product $F = f_1 \cdots f_m$. The coefficients of F are rational integers and thus there is an infinite sequence of rational primes p_1, p_2, \dots and corresponding rational integers x_1, x_2, \dots , such that $F(x_i) \equiv 0 \pmod{p_i}$, $i = 1, 2, \dots$ (see e.g. [1], p. 33).

Let now L be a normal extension of the rationals containing K . For each p_i choose a prime ideal $P_i \subset L$ containing p_i . Then $F(x_i) \equiv 0 \pmod{P_i}$. Since $(p_i, p_j) = (1)$ for $i \neq j$, we also have $P_i \neq P_j$. Thus there exist infinitely many prime ideals of L which divide numbers of the sequence $F(x_i)$, $i = 1, 2, \dots$.

Assume now there exist only finitely many prime ideals in R , say Q_1, \dots, Q_k , such that the congruence $f(x) \equiv 0 \pmod{Q_j}$ has a solution in R for $j = 1, \dots, k$. Denote by Q'_1, \dots, Q'_k the ideals in L generated by Q_1, \dots, Q_k . A prime ideal of L containing $F(x_i)$ would then have to be also a divisor of some Q'_j or of an ideal conjugate to Q'_j , because $F(x_i)$ is the product of the conjugate elements $f_1(x_i), \dots, f_m(x_i)$. It would follow that there are only finitely many prime ideals of L containing numbers of the sequence $F(x_1), F(x_2), \dots$, which is a contradiction. This proves the lemma.

The next lemma gives a necessary condition which is satisfied by

Received June 2, 1964. The author is grateful to Professor Ernst Specker for many helpful conversations.

equivalent ideals of a polynomial ring over R . Denote by R^n the set of n -tuples of elements of R . If t_1, \dots, t_n are indeterminates and

$I = (f_1, \dots, f_r) \subset R[t_1, \dots, t_n]$, $a \in R^n$, let $I_a = (f_1(a), \dots, f_r(a))$. Further let C stand for the field of complex algebraic numbers, C^n for the n -dimensional affine space over C and V_I for the algebraic variety in C^n defined by the ideal I .

LEMMA 2. *Let I and J be ideals of $R[t_1, \dots, t_n]$ and suppose that for all $a \in R^n$ we have $I_a = J_a$. Then $V_I = V_J$.*

Proof. Let f_1, \dots, f_r be a basis of I and g_1, \dots, g_s a basis of J . Suppose $V_I \neq V_J$ and assume there is a point $\alpha = \langle \alpha_1, \dots, \alpha_n \rangle$ of V_I not contained in V_J . We must show that there exists a n -tuple $a \in R^n$, such that $I_a \neq J_a$.

Now $f_i(\alpha) = 0$, $i = 1, \dots, r$ but, say, $g_1(\alpha) \neq 0$. $K(\alpha_1, \dots, \alpha_n)$ is a separable algebraic extension of K , and let θ be a primitive element. We then have $\alpha_i = h_i(\theta)$, $i = 1, \dots, n$, where h_i is a polynomial whose coefficients may be assumed, without loss of generality, to be integers of R . Also let $p(t)$ be a polynomial in $R[t]$, of which θ is a root and which is irreducible in $K[t]$.

Put $F_i(t) = f_i(h_1(t), \dots, h_n(t))$, $i = 1, \dots, r$ and $G_1(t) = g_1(h_1(t), \dots, h_n(t))$. Since $f_i(\alpha) = 0$, $i = 1, \dots, r$ and $g_1(\alpha) \neq 0$, we have $F_i(\theta) = 0$, $i = 1, \dots, r$ and $G_1(\theta) \neq 0$. Hence there are polynomials $q_i(t) \in R[t]$ and elements $s_i \in R$, $i = 1, \dots, r$, with $s_i F_i(t) = p(t)q_i(t)$, $i = 1, \dots, r$. On the other hand, since $p(t)$ is irreducible and $G_1(\theta) \neq 0$, $p(t)$ and $G_1(t)$ are relatively prime in $K[t]$, and there are polynomials $A(t), B(t) \in R[t]$, such that

$$A(t)p(t) + B(t)G_1(t) = c,$$

where $c \in R$ and $c \neq 0$.

By Lemma 1 there are infinitely many prime ideals P in R , such that the congruence $p(x) \equiv 0 \pmod{P}$ has a solution in R . Each one of the numbers s_1, \dots, s_r and c is contained in only a finite number of prime ideals. Hence there is a prime ideal $P \subset R$ and an element $x \in R$, such that $p(x) \equiv 0 \pmod{P}$, but $s_i \not\equiv 0 \pmod{P}$, $i = 1, \dots, r$ and $c \not\equiv 0 \pmod{P}$. Therefore $B(x)G_1(x) \not\equiv 0 \pmod{P}$. If we now let $a = \langle h_1(x), \dots, h_n(x) \rangle$, then $a \in R^n$ and we get $g_1(a) = G_1(x) \not\equiv 0 \pmod{P}$ and thus also $J_a \not\equiv 0 \pmod{P}$. On the other hand, since $s_i \notin P$, it follows that $F_i(x) \equiv 0 \pmod{P}$, hence $f_i(a) \equiv 0 \pmod{P}$, $i = 1, \dots, r$ and thus $I_a \equiv 0 \pmod{P}$. Therefore $I_a \neq J_a$, which was to be shown.

COROLLARY. *If for all $a \in R^n$ we have $I_a = (1)$, then $V_I = \phi$.*

LEMMA 3. Consider polynomials $f_1, \dots, f_k \in R[t]$. Assume that for all nonzero elements $r \in R$ the k numbers $f_1(r), \dots, f_k(r)$ generate the same ideal $I \subset R$. Then we also have $I = (f_1(0), \dots, f_k(0))$.

Proof. If D is an ideal in $R, D \supset (f_1(0), \dots, f_k(0))$ and r is an arbitrary nonzero element of D , then $f_i(r) \in D$ for $i = 1, \dots, k$. Since $I = (f_1(r), \dots, f_k(r))$, we have $I \subset D$.

Conversely, if $D \supset I$ and $r \in D, r \neq 0$, then $f_i(r) \equiv f_i(0) \pmod{D}$. Since $f_i(r) \in D$, also $f_i(0) \in D$ for all i and hence $(f_1(0), \dots, f_k(0)) \subset D$. This proves the lemma.

LEMMA 4. Let f_1, \dots, f_k be arbitrary and g_1, \dots, g_m homogeneous linear polynomials in $R[t_1, \dots, t_n]$. Assume that for all $a \in R^n$ we have

$$(f_1(a), \dots, f_k(a)) = (g_1(a), \dots, g_m(a)) .$$

Also denote by h_1, \dots, h_k the subpolynomials of f_1, \dots, f_k formed by their linear terms. Then $(h_1(a), \dots, h_k(a)) = (g_1(a), \dots, g_m(a))$ for all $a \in R^n$.

Proof. Since $(g_1(0), \dots, g_m(0)) = (f_1(0), \dots, f_k(0)) = (0)$, we have $f_1(0) = \dots = f_k(0) = 0$. Thus $f_i = h_i +$ terms of degree $\geq 2, i = 1, \dots, k$. Take a fixed n -tuple $a \in R^n$ and let $r \in R$ be arbitrary but $\neq 0$. Then

$$\begin{aligned} (f_1(ra), \dots, f_k(ra)) &= (rh_1(a) + r^2(\dots), \dots, rh_k(a) + r^2(\dots)) \\ &= (r)(h_1(a) + r(\dots), \dots, h_k(a) + r(\dots)) \\ &= (g_1(ra), \dots, g_m(ra)) = (r)(g_1(a), \dots, g_m(a)) . \end{aligned}$$

R being an integral domain, we get

$$(h_1(a) + r(\dots), \dots, h_k(a) + r(\dots)) = (g_1(a), \dots, g_m(a))$$

for all nonzero $r \in R$. By Lemma 2 therefore

$$(h_1(a), \dots, h_k(a)) = (g_1(a), \dots, g_m(a)) ,$$

which was to be proved.

THEOREM. Consider in $R[x_0, \dots, x_r, y_0, \dots, y_s]$ the ideal $J = (x_0, \dots, x_r)(y_0, \dots, y_s)$ and suppose I is an ideal such that for all $a \in R^{r+s+2}$ we have $I_a = J_a$. Then the number of elements in a basis of I is at least $r + s + 1$.

Proof. Let f_1, \dots, f_n be a basis of I and let I' be the ideal generated by the subpolynomials b_1, \dots, b_n of f_1, \dots, f_n , which are linear with respect to x_0, \dots, x_r and with respect to y_0, \dots, y_s . Since also the generators of J are bilinear and for all $a \in R^{r+s+2}$ we have $I_a = J_a$, by Lemma 3, we also have $I'_a = J_a$ for all a .

Now the ideal J has only trivial zeroes in C^{r+s+2} , either all $x_i = 0$ or all $y_j = 0$. On the other hand, if $n \leq r + s$, it follows from a theorem of Macaulay (see [2], p. 54) that I' has a nontrivial zero in C^{r+s+2} . By Lemma 2 this cannot happen. Hence $n \geq r + s + 1$.

REFERENCES

1. A. Scholz, *Einführung in die Zahlentheorie*, Sammlung Götschen Band 1131, Berlin 1939.
2. F. S. Macaulay, *Algebraic Theory of Modular Systems*, Cambridge Tracts in Math. 19, Cambridge 1916.

UNIVERSITY OF CALIFORNIA, DAVIS

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

H. SAMELSON

Stanford University
Stanford, California

R. M. BLUMENTHAL

University of Washington
Seattle, Washington 98105

J. DUGUNDJI

University of Southern California
Los Angeles, California 90007

*RICHARD ARENS

University of California
Los Angeles, California 90024

ASSOCIATE EDITORS

E. F. BECKENBACH

B. H. NEUMANN

F. WOLF

K. YOSIDA

SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA
NEW MEXICO STATE UNIVERSITY
OREGON STATE UNIVERSITY
UNIVERSITY OF OREGON
OSAKA UNIVERSITY
UNIVERSITY OF SOUTHERN CALIFORNIA

STANFORD UNIVERSITY
UNIVERSITY OF TOKYO
UNIVERSITY OF UTAH
WASHINGTON STATE UNIVERSITY
UNIVERSITY OF WASHINGTON
* * *
AMERICAN MATHEMATICAL SOCIETY
CALIFORNIA RESEARCH CORPORATION
SPACE TECHNOLOGY LABORATORIES
NAVAL ORDNANCE TEST STATION

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced). The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. It should not contain references to the bibliography. No separate author's resumé is required. Manuscripts may be sent to any one of the four editors. All other communications to the editors should be addressed to the managing editor, Richard Arens, at the University of California, Los Angeles, California 90024.

50 reprints per author of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published quarterly, in March, June, September, and December. Effective with Volume 13 the price per volume (4 numbers) is \$18.00; single issues, \$5.00. Special price for current issues to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: \$8.00 per volume; single issues \$2.50. Back numbers are available.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley 8, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), No. 6, 2-chome, Fujimi-cho, Chiyoda-ku, Tokyo, Japan.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

* Basil Gordon, Acting Managing Editor until February 1, 1966.

David R. Arterburn and Robert James Whitley, <i>Projections in the space of bounded linear operators</i>	739
Robert McCallum Blumenthal, Joram Lindenstrauss and Robert Ralph Phelps, <i>Extreme operators into $C(K)$</i>	747
L. Carlitz, <i>A note on multiple exponential sums</i>	757
Joseph A. Cima, <i>A nonnormal Blaschke-quotient</i>	767
Paul Civin and Bertram Yood, <i>Lie and Jordan structures in Banach algebras</i>	775
Luther Elic Claborn, <i>Dedekind domains: Overrings and semi-prime elements</i>	799
Luther Elic Claborn, <i>Note generalizing a result of Samuel's</i>	805
George Bernard Dantzig, E. Eisenberg and Richard Warren Cottle, <i>Symmetric dual nonlinear programs</i>	809
Philip J. Davis, <i>Simple quadratures in the complex plane</i>	813
Edward Richard Fadell, <i>On a coincidence theorem of F. B. Fuller</i>	825
Delbert Ray Fulkerson and Oliver Gross, <i>Incidence matrices and interval graphs</i>	835
Larry Charles Grove, <i>Tensor products over H^*-algebras</i>	857
Deborah Tepper Haimo, <i>L^2 expansions in terms of generalized heat polynomials and of their Appell transforms</i>	865
I. Martin (Irving) Isaacs and Donald Steven Passman, <i>A characterization of groups in terms of the degrees of their characters</i>	877
Donald Gordon James, <i>Integral invariants for vectors over local fields</i>	905
Fred Krakowski, <i>A remark on the lemma of Gauss</i>	917
Marvin David Marcus and H. Minc, <i>A subdeterminant inequality</i>	921
Kevin Mor McCrimmon, <i>Norms and noncommutative Jordan algebras</i>	925
Donald Earl Myers, <i>Topologies for Laplace transform spaces</i>	957
Olav Njstad, <i>On some classes of nearly open sets</i>	961
Milton Philip Olson, <i>A characterization of conditional probability</i>	971
Barbara Osofsky, <i>A counter-example to a lemma of Skornjakov</i>	985
Sidney Charles Port, <i>Ratio limit theorems for Markov chains</i>	989
George A. Reid, <i>A generalisation of W^*-algebras</i>	1019
Robert Wells Ritchie, <i>Classes of recursive functions based on Ackermann's function</i>	1027
Thomas Lawrence Sherman, <i>Properties of solutions of nth order linear differential equations</i>	1045
Ernst Snapper, <i>Inflation and deflation for all dimensions</i>	1061
Kondagunta Sundaresan, <i>On the strict and uniform convexity of certain Banach spaces</i>	1083
Frank J. Wagner, <i>Maximal convex filters in a locally convex space</i>	1087
Joseph Albert Wolf, <i>Translation-invariant function algebras on compact groups</i>	1093