Briefwechsel

H.Hasse – A.A.Albert

Version von Dienstag, 17.Feb.2004

Hasse an Albert 10.8.33 und 2.2.35
Albert an Hasse 6.2.31 – 6.2.34
Referate Zentr.Bl.Math.

Hasse–Albert vollständig (soweit photokopiert)

Für PDFLaTeX/hyperref und LaTeX2e/hyperref

Inhaltsverzeichnis

Kapitel 1

Korrespondenz Hasse–Albert

1.1 06.02.1931, Albert an Hasse

Columbia University
in the City of New York
DEPARTMENT OF MATHEMATICS

45 Thayer Street,
New York, N.Y., U.S.A.
February 6, 1931.

Dear Professor Hasse:

I was very interested to receive your letter from Professor Dickson describing your work. I am very pleased at your interest in my work and am sending you a set of my reprints under separate cover. I have also five new papers being published soon and shall send you the reprints as soon as I obtain them.

I live at the above Thayer St. address and shall be there until August 15, 1931. After that my address will be:

Department of Mathematics, University of
Chicago, Chicago, Illinois, U.S.A.

I have been appointed assistant professor of mathematics at the University of Chicago beginning next Autumn and shall give a course in the Galois Theory of Equations and one in Linear Associative Algebras there next year.

With my best regards to you and to Professor Archibald whom you may see, I am

Very sincerely yours,

A. Adrian Albert

1.2 23.03.1931, Albert an Hasse

Columbia University
in the City of New York
DEPARTMENT OF MATHEMATICS

45 Thayer Street,
New York, N.Y.,
March 23, 1931.

Dear Professor Hasse:

I received your letter a short while ago but waited until I completed some new results before answering you. My new paper „On direct products, cyclic division algebras, and pure Riemann matrices" has appeared in the January Transactions and I will send you a reprint when I get them. I am sure you will be interested in the results I obtained there.

I considered your question on the existence of non–cyclic division algebras of order sixteen in my April 1930 Transactions paper of which you have a copy. The question seems to be a number–theoretic one and I see no way to get an algebraic hold on it. It seems to be a hopeless problem to me after more than a year's work on it.

The other question is much easier to answer in the light of the work I have just completed. I have shown that the direct product $A \times A$ is a total (vollständige) matrix algebra if A is

(a) any cyclic algebra over F.
(b) any normal division algebra of order n^2 over F where n has no square factor.

Here F is *any* non–modular field. So in particular since there exist *cyclic* division algebras of order 16 over algebraic number fields of finite degree which are not the direct product of two generalized quaternion algebras (shown to exist over the field R of all rational numbers in my April 1930 Transaction paper) the direct product of such an algebra with itself is a total matric algebra.

I have recently obtained a new result which will interest you, I believe. Using the definition of algebras of type R_2 in thirty–six units of my American Journal paper, I have extended the work of that paper and have proved that every normal division algebra of type R_2 in thirty–six units over any non–modular field F is a cyclic algebra. This mild assumption of type R_2 is the same as saying that for some quantity x in the algebra, the minimum equation of x has degree 2 or 3 instead of 6.

The above results are very new and will probably not appear until next year.

With my best regards, I am

Very sincerely yours,

A. Adrian Albert

1.3 27.03.1931, Albert an Hasse

Columbia University
in the City of New York
DEPARTMENT OF MATHEMATICS

45 Thayer St.,
New York, N.Y.,
March 27, 1931.

Dear Professor Hasse:

I have at last received reprints of my four latest papers and will send them shortly to you.

I am writing to you principally to correct the statements of my last letter. Recent work of mine yielded the result that if A is any normal division algebra of order sixteen over a non–modular field F, and if A is not the direct product of two generalized quaternion algebras, then the direct product $A \times A$ is expressible as the direct product of an eight–rowed total matric algebra and a generalized quaternion division algebra. Also the direct product $A \times B$ where B is the algebra *reciprocal* to A is a total matric algebra.

This leads to a contradiction of the results I communicated to you in my last letter. I studied the proofs and have found my error. I believe, however, that the theorems on direct products are correct if you replace $A \times A$ by $A \times B$ where B is reciprocal to A.

I am not quite sure of these results, but am certain that the theorems on direct products $A \times A$ are false. In particular my theorem on the direct product with itself of a cyclic algebra of order p^2, p a prime, (published in the new Trans. paper) is false but is correct when we replace $A \times A$ by $A \times B$ where B is reciprocal to A.

I shall have to wait a while before feeling certain that the revised theorems and proofs are correct, as this work is very complicated and tricky, and one is likely to make mistakes. I *think* the results I have given here are now correct, in fact I have a feeling that it should be the reciprocal algebra which is associated with an algebra A in the relation $A \times B$ is a total matric algebra, instead of A itself. Of course any algebra which is a direct product of generalized quaternion algebras is self–reciprocal.

If you are interested in knowing of the correctness of my results after I have had an opportunity for them to become settled, I shall be glad to communicate them to you.

With my best regards, I am
Very sincerely yours,

A. Adrian Albert

1.4 11.05.1931, Albert an Hasse

Columbia University
in the City of New York
DEPARTMENT OF MATHEMATICS

45 Thayer St.,
New York, N.Y.,
May 11, 1931.

Dear Professor Hasse:

I received your most interesting letter and have read it with a great deal of pleasure. I too have felt that the problems of the theory of normal division algebras are in a great measure number–theoretic as well as algebraic.

Some time ago I completed a paper for the Transactions in which I obtained independently most of Brauer's results by means of certain new simple considerations which in themselves are rather powerful new tools for research in division algebras. I was fortunate, however, to discover Brauer's paper before it was too late, and have revised my paper so as to give Brauer priority for the theorems first secured by him. But my own proof uses none of the theory of "factorsystems", is self contained, and is rather short. Brauer's work, on the other hand, depends on two previous memoirs, and two papers of I. Schur. Professor Wedderburn thinks my method a great advance and so I am publishing my new proof. It will probably appear about November.

Your work on quadratic forms is not new to me. In fact I have been reading your Crelle and Jahresbericht work ever since your first letter to me. In this period I have also been able to apply your most fundamental result on quadratic forms in $n \geq 5$ variables, together with my above mentioned new methods to prove the following results on algebras over a field F (always F is here an algebraic field of finite degree over the field of all rational numbers):

1. A direct product $A \times B$ of two generalized quaternion algebras is never

a division algebra. (in fact $A \times B$ of any orders 2^{2e}, 2^{2f})

2. Every normal division algebra of order 16 over such an F is a cylic (Dickson) algebra.

3. Every normal division algebra of order 64 over F contains a maximal sub–field $F(x)$ which is a direct product of a quadratic field and a cyclic quartic field (and hence is generated by a $(4,2)$ group.)

4. Every normal division algebra of order 2^{2m} has exponent 2^m.

   In fact 4) implies a more powerful result. We say that an equation with coefficients in F belongs to a normal division algebra A over F if A contains a quantity x which has the given equation as its minimum equation (Hauptgleichung). Then we have

5. Let A be a normal division algebra of order 2^{2m} over an algebraic field F and let $0 \leq t < m,\ \sigma = 2^{m-t}$. Then

$$A^{\sigma} = M_{\sigma} \times A_{\sigma}$$

   where M_{σ} is a total matric algebra over F and A_{σ} is a normal division algebra of order 2^{2t} over F such that every equation of degree $2^r \leq 2^t$ which belongs to A_{σ} belongs to A, and conversely.

This last result is probably true when we replace 2 by any prime p. In fact I can prove it if and only if the theorem analogous to 1) is true, namely

> "A direct product of two cyclic algebras of the same order p^2 (p a prime) is never a division algebra."

By your Annalen paper (letter to L.E.Dickson) the above theorem is true over every p–adic extension of F. Hence the form $N(x)$, the norm or determinant of the general quantity of the direct product, is a null form over any p–adic extension of F. Also certainly over $F(p_{\infty})$. By the general principle which you proved for quadratic forms this ought to imply that the form $N(x)$ is a null form in F and hence my general result. Have you been able to prove this result in your newly completed work?

In my work on normal disivion algebras over any non–modular field F (no more just an algebraic field) I in fact proved that, with the notation of my April 1930 Transactions paper, if A is a normal division algebra of order sixteen over F then $A^2 = M \times Q$ where M is an eight rowed total matric algebra and

$$Q = (1, u, y, uy)\,,\ yu = -uy\,,\ u^2 = \rho\,,\ y^2 = \gamma_3^2 - \gamma_4^2\sigma$$

$(\rho, \sigma, \gamma_1, \ldots, \gamma_6$ of my paper such that

$$\gamma_5^2 - \gamma_6^2\sigma\rho = (\gamma_1^2 - \gamma_2^2\rho)(\gamma_3^2 - \gamma_4^2\sigma)$$

the associativity condition

A necessary and sufficient condition that Q be a division algebra is that

$$\gamma_3^2 - \gamma_4^2\sigma \neq \xi_1^2 - \xi_2^2\rho$$

for any ξ_1 and ξ_2 of F. It follows immediately that a necessary and sufficient condition that A be not a direct product of two generalized quaternion algebras is that Q is a division algebra, that is that A have exponent 4. I believe this answers your question.

I am very interested in your new results and will be very anxious to know the details. Will all the results be in the Transactions paper, or just what you communicated in your first letter to me? If the latter, where will your new work appear?

The work of the German mathematicians on algebras is very interesting to me and should like to know all of it if possible. In particular I have been unable to obtain Artin's Hamburg papers. Can you tell me in a few words what subjects he studied in these papers on linear algebras, and whether or not he has published anything in more accessible journals? I certainly do not wish to repeat known results, even if they are unknown in America, and am very pleased and thankful for the opportunity to communicate with you and know of your results.

With my very best regards, I am

Very sincerely yours,

A. Adrian Albert

1.5 30.06.1931, Albert an Hasse

Columbia University
in the City of New York
DEPARTMENT OF MATHEMATICS

45 Thayer St.,
New York, N.Y.,
June 30, 1931.

Dear Professor Hasse:

I am very sorry that I gave you the impression that I had completed a proof that the exponent of any normal division algebra of degree n over an algebraic field has exponent n. I still have to prove the fundamental result that a normal division algebra A which is a crossed product of degree p^2, p a prime, has exponent p^2 when it is not a direct product of two algebras of degree p. I have proved that $A^p \sim B$ where B is a cyclic algebra of degree p whose constants are readily expressible in terms of those of A. (This is the ease of an abelian (p, q) group.)
For $p = 2$ the work of my April 1930 Transactions paper proved that when B was not a division algebra algebra A is the direct product of two generalized quaternion algebras; but I cannot seem to obtain the analogous result for p an odd prime. I want to remark that in this connection I have proved that your results imply that the direct product of any two normal division algebras is a division algebra if and only if the degrees of the two algebras are relatively prime (for an algebraic reference field.)

I want to thank you for your very kind letter and for the reprints you sent me. My theorem on normal division algebras of degree four will be offered to the Transactions for publication in a few days. I have already published a report of this work in the June Proceedings of the National Academy of Sciences. I should be pleased to have you refer to my result in your Transactions paper.

I hope to hear from you again, and I shall also write to you at the end of this summer when I may perhaps have more things of interest to you. I have some new results now but wish to wait until they are more complete before making any communication of them to you.

With very best regards, I am
Very sincerely yours,

A. A. Albert

P.S. Your English is very clear and understandable. I only wish I could write German half so well! I hope that in perhaps two years I may visit Germany and there see you and discuss our beautiful subject, linear algebras.

1.6 06.11.1931, Albert an Hasse

The University of Chicago

Department of Mathematics November 6, 1931.

Dear Professor Hasse:

I received your very interesting communication this morning and was very glad to read of such an important result. I consider it as certainly the most important theorem yet obtained for the problem of determining all normal division algebras over an algebraic number field Ω. In particular it furnishes a new proof that all normal division algebras of degree four over Ω are cyclic.

The results I had partially obtained at the time I wrote my last letter were not really theorems but a new method of proving my above theorem on algebras of degree four. It seemed that this would generalize to algebras of degree 2^e but I needed some sort of a result which I hoped would come out of your work on p–adic adjunctions. But now your result just communicated gives me almost immediately the following theorems.

I. *All normal division algebras of degree* 2^e *are cyclic algebras.* For just as I was able to prove that every n.d.a. of degree 8 had an abelian $(2,4)$ generation and hence now cyclic, so it follows, by an induction on e, that every n.d. algebra of degree 2^e has an abelian $(2,2^{e-1})$ generation, where the cyclic sub–field of order 2^{e-1} is a splitting field of A^2.

It is easily shown that if A is a n.d.alg. of degree p^2, p a prime then it is possible to extend the centrum so that A', the algebra over the extended field, has a abelian (p,p) generation and is still a normal division algebra over the extended field Ω' (whose order with respect to Ω is relatively prime to the prime p.) But A' is then cyclic by your theorem, hence has exponent p^2. Hence A has exponent p^2. From this it is easy to prove

II. The exponent of any normal division algebra of degree n over an algebraic number field Ω is n.

but also then it follows that we have

III. Let A be a normal division algebra of degree p^e, p a prime, over an algebraic number field Ω. Then there exists an algebraic field Ω' over Ω (of degree r prime to p over Ω), such that $A' = A \times \Omega'$ is a cyclic normal division algebra of degree p^e over Ω'.

This above result says that while we don't know if A is cyclic we at least have this property *extensionally obtainable* while A' remains a division algebra. This may prove sufficient for some purposes.

Finally I obtained several months ago some new results on cyclic algebras. These results will be published in the American Journal of Math. I am sending you a copy of my proof sheets together with a reprint of my paper in which I give a new proof of Brauer's theorems.

You asked for references to my own and Dickson's papers. In addition to the references you gave in your paper on cyclic algebras there is Dickson's recent "Construction of division algebras" Trans. of the Amer. Math. Soc. vol.32 (1930), pp.319–334. Here Dickson gives a better proof of the material of his Chapter III which you quote in your letter. As for his other papers there are none which give material not in his "Algebren" except the paper "New Division Algebras" (Bull. of the A.M.S.) which you quote.

In my paper "Normal division algebras in $4p^2$ units, p an odd prime", (Annals of Math., vol.30(1929), pp.583–590) I proved that the algebras considered in the above Dickson paper were actually crossed products and hence not "new". If you gave Dickson's paper as a reference I think you should certainly give my proof that his algebras are not new.

I have sent you all of my reprints except the most recent ones. I shall make up a separate list of all my papers on algebras (including the ones to be published soon) with a brief summary of results and shall send this to you in a few days.

I would have written to you sooner but I was waiting to get the proof sheets of your Trans. paper to see whether I could complete the new theorems I,II,III which are now complete in view of your new theorem.

When and where do you intend to publish your new result ? Of course my own theorem is not proved unless I can refer to your paper ? Can we not perhaps make some arrangement to publish in the same place (or even in the same paper !) ? Of course it may even be that by the time you wish to publish your new results that you can prove all normal division algebras cyclic and hence make my I,II,III of no value.
Please tell me what you think of these results and also about publishing them.

Professor Dickson was much interested in your new work. He sends you his kindest regards.

I have been accustomed to communicate all my work and what you have written to me to Professor Wedderburn (whom I worked with when I was in Princeton). Unfortunately he is very ill now and is in a hospital in Baltimore. We all hope here that he recovers from his illness very soon. The doctor who takes care of him says that his trouble should yield to proper treatment and that he will be well in a short time.

I was fortunate to be able to read your paper for the editor's of the Transactions. I have not, as yet, received the proof sheets, however.

With my best regards, and hoping to hear from you soon, I am

Very sincerely yours,

A. Adrian Albert

A. Adrian Albert.

1.7 26.11.1931, Albert an Hasse

The University of Chicago

Department of Mathematics

Eckhart Hall,

November 26, 1931.

Dear Professor Hasse:

I received your most welcome letter yesterday and I heartily congratulate you on the remarkable theorem you have proved.

Your proof of the main theorem is very interesting to me. Of greatest interest is your reduction to Theorem I. I cannot even yet see how this reduction is an immediate consequence of your Satz 2 but perhaps the existence of a cyclic field such that A splits everywhere will be made clear when you publish your proof.

In all my work on division algebras the principal difficulty has been to somehow find a cyclic splitting field. This your p–adic method accomplishes.

The part of the proof of Theorem I which you attribute to Brauer and Noether is however already in print. Your Theorem I has the following almost trivial proof. We require to prove the equivalent

I. *Let D be a normal division algebra of degree m over its centrum F, an algebraic number field. Then if D splits everywhere $m = 1$.*

For let $m > 1$. By the Brauer structure theorem it is obviously sufficient to consider the case where $m = p^e, p$ a prime, so that $e > 0$. By Theorems 13,10,9 of my Bulletin paper there exists an algebraic field K over F such that $D' = D \times K = M \times B$ where M is a total matric algebra and B is a cyclic normal division algebra of prime degree p over its centrum K. But D splits everywhere so also D' and hence B split everywhere. By your 3.13 algebra B is not a division algebra, a contradiction. Hence

$m = 1$.

The above quoted Theorems 9,10,13 are from my paper in the Bulletin of the American Mathematical Society, vol.37, October 1931, pp.777–784. I have not as yet received reprints but will send you a reprint when they arrive. The theorems are about a normal division algebra D of degree m over any non–modular field F. They read

Theorem 9. *Let y in D have grade s for F so that $m = st$. Then if η is any scalar root of the minimum equation of y for F*

$$D \times F(\eta) = M \times B,$$

where M is a total matric algebra of degree s and B is a normal division algebra of degree t over its centrum $F(\eta)$.

Theorem 10. *The algebra B of Theorem 9 is simply isomorphic with the algebra of all quantities of D commutative with y, under a correspondence where y corresponds to η. Hence this latter algebra is a normal division algebra of degree t over its centrum $F(y)$.*

I also used Theorem 2? of my Trans. paper "On direct products" which I stated as

Theorem 12. *Let $m = p^e$, p a prime, and let x in D have grade m for F. Then there exists an algebraic field Z of order n over F such that n is prime to p, $D \times Z$ is a normal division algebra of degree m over its centrum Z, and $Z(x)$ is a cyclic field of order p over a sub–field $Z(y)$ of order p^{e-1} over Z.*

I then had, without further proof,

Theorem 13. *Let $D' = D \times Z$ and x be as in Theorem 12. Then the algebra B_0 of all quantities of D' commutative with y is a cyclic algebra of degree p over its centrum $Z(y)$.*

This Theorem 13 combined with the two supplementary Theorems 9 and 10 are precisely what I used on page 1 of this letter. As my theorems have already been printed I believe that I may perhaps deserve some priority on that part of your proof. I may say, however, that the remarkable part of your proof for me is the obtaining of the cyclic field C. I of course knew of your 3.13.

In your letter of November 11 you said that the results of my paper "On direct products" were almost all not new. From my examination of both the Brauer–Noether paper and of your Transactions paper I cannot see where any of you have considered what I believe to be the new point of my paper. Neither you, Brauer, nor Noether considered anything but *splitting* fields. I on the other hand, in my section 3, considered all types of algebraic field extensions of the field F. I believe my Theorems 14,15 etc. of section 3 to be all new results, of which N's are special cases. Also my Theorem 23 is precisely what E.Noether is using in her reduction of II (where already I reduces to II either by the Brauer structure theorem, or, as I have stated your I, by my Theorem 21) instead of the better Theorem 22 as in my statement above. Note also that my paper was received by the editors of the Transactions on April 17, 1931, yours presented April 2?.

It is possible that Emmy Noether did make the above considerations as you suggest. It is of course impossible for people working in the same field not to frequently obtain overlapping results. I have the highest respect for Fr.Noether and certainly appreciate her great mathematical powers. Please carry to her my most sincere best wishes and appreciation for her accomplishments in our beloved field of ALGEBRA.

I cannot quite see what you mean about the theory of crossed products. Did not Dickson really first consider them? As to the general associativity conditions I obtained them in 1929 from my matrix representation of any "normal division algebra of type R" in my paper "The structure of pure Riemann matrices with non–commutative multiplication algebras". The matrix representation (of any crossed product) is on page 31 (section 7) of the Rendiconti del Circolo Matematico di Palermo (vol.55,1931) reprint which I sent you. I never published the associativity conditions but they are immediate consequences of the matrix representations. I showed them to Professor Dickson in July 1929 when the above paper was completed but he did not think them important enough to be published.

As to Brauer's "obscure" conception of factorsystems, I do not believe them so obscure. In my paper "The structure of matrices with any normal division algebra of multiplications", Annals of Math. vol.32(1931) pp.131–148 I obtained a sort of a generalization of some of I.Schur's work which led both for Brauer (very early) and myself later and independently to the theory of factor systems. I still believe this important. Suppose that x is any quantity of a normal simple algebra. It is desirable to find a multiplication table of the algebra relative to the quantity x. I have shown that the algebra has a basis $x^i y x^j$ $(i, j = 0, 1, \ldots, n-1)$ where n is the degree of the algebra, and that from the factorsystem (which I had no idea had been considered before) we can get immediately the multiplication table of the algebra. It is desirable to know this even for an algebra known to be cyclic. I never published this but still think it worth while. What do you think of this material? It was all communicated to Wedderburn at the time I obtained the results and he still has my letters to verify this. He was quite interested at the time.

Professor Dickson sends you his sincere regards. I have not heard from Archibald for some time. I thought you knew that he did not come from Chicago but is at Columbia University in New York.

I hope you will pardon a slight criticism of your envelopes. You have addressed your letters recently to THE UNIVERSITY,CHICAGO. There are, of course, more than one university in Chicago. It is only by guesswork that the postal authorities delivered them here. The correct address is THE UNIVERSITY OF CHICAGO, Chicago, Illinois.

Let me express my thanks for communicating your wonderful theorem to me. I deeply appreciate it. With best regards, I am

Very sincerely yours,

A.Adrian Albert

P.S. I am very glad that you are interested in the possibility of my visiting you. I hope that I will be able to leave Chicago on Sept. 1,1933 to return here not later than Dec. 31,1933. I do not believe I can make the trip before that time.

A.A.Albert

1.8 09.12.1931, Albert an Hasse

The University of Chicago

Department of Mathematics

Eckhart Hall,
December 9, 1931

Dear Professor Hasse:

I am writing to you in great haste as I must attend a meeting in a short time (in fact 20 minutes!)

I was very glad to get your letter as well as the proof sheets of your new result. I have read them and am returning them to you in the present letter. (I shall mail it *now*!).

You will have received my last letter at the time I am writing this. I feel even more strongly now than before that in E.Noether's and R.Brauer's part of your paper there was a good deal of unnecessary complication due to the fact that the following reduction was not made. You all tried to prove that if a normal simple algebra A over F splits every where then $A \sim F$. But this is merely to prove that the index of A is one and reduces to the theorem that if A is a normal division algebra of degree m and splits everywhere then $m = 1$. As in the proof I gave you this avoids the induction of your paper which is really completely non–essential. Also I think it better to use Brauer's structure theorem than the additional adjunction to reduce to the case $m = p^e$.

I have not had time to write out the resume I promised you. This will be accomplished later. Also I am certain that the delay in publishing your paper is due to its length. The editors of the Transactions generally make up their numbers according to the long papers, filling in the extra space with short papers even though they (the short papers) may have been presented much *later* than some long papers.

I hope to have more time to write to you later

With the best regards, I am very sincerely

Yours

A.A.Albert

1.9 25.01.1932, Albert an Hasse

The University of Chicago
——
Department of Mathematics

January 25, 1932.

Dear Professor Hasse:

I have finally found time to write up the article by both of us "A Determination of all Normal Division Algebras over an Algebraic Number Field" for the Transactions. I gave a historical sketch of the proof, my short proof, and a slight revision (to make it more suitable for American readers) of your proof. I believe the presentation will be approved by you and with a footnote to the effect that I undertook the writing of the article at your suggestion, I have presented the paper to the American Mathematical Society and will send it soon to the editors of the Trans.

I have recently been able to throw more light on the meaning of the so–called index reduction factor in the direct product $D \times Z$ of a normal division algebra D over F and an algebraic field Z of finite degree r over F. In fact I have defined

Definition. Let Q be a total matric algebra of degree q, D a normal division algebra of degree (index) m, and Z be an algebraic field of degree r over F. Then the quotient index

$$q \equiv q(Z, D)$$

of Z with respect to D is defined to be the least integer q such that $Q \times D$ has a sub–field equivalent to Z.

I have then proved the following

Theorem. The quotient index $q(Z, D)$ is a divisor of the degree r of Z, $r = qs$. Every normal simple algebra A of degree n and which is similar to D has complementary index $\frac{n}{m}$ divisible by q if and only if A has a sub–field Z_0 equivalent to Z. In this case $A = H \times Q \times D$ where Z_0 is in $Q \ +++ \ Z$, and H is a total matric algebra. If Z' is equivalent to Z the index of $D \times Z' \sim D'$, a normal division algebra over Z' is $m' = \frac{m}{s}$ so that $s = \frac{r}{q}$ is the index reduction factor of D with respect to Z. Moreover the algebra D_0 of all the quantities of $Q \times D$ commutative with all the quantities of Z_0 is a normal division algebra over Z_0 equivalent to D' as over Z'.

In the above I have defined the complementary index of a normal simple algebra to be the quotient of its degree and its index. Moreover I call the algebra $Q \times D$ a least normal simple representation of Z by D. As you see above I have shown that any normal simple representation of Z by D is the direct product of a total matric algebra and a *least* representation. Moreover a normal simple algebra A gives a least representation of Z if and only if the algebra of all quantities of A commutative with $Z_0 \cong Z$ is a division algebra.
In particular we notice that $m = sm'$, $n = qm$ for a least representation, so that, since $r = sq$, we have $n = (qs)m' = rm'$. Hence the index of A is divisible by $\frac{n}{r}$.

The above criterion has enabled me to give a very simple proof of a conjecture by L.E.Dickson as to criteria that a normal simple algebra be a division algebra. For the case $p = 3$ you may see this in his Algebren pg.66, otherwise in his Transactions paper vol.28, 1926, pp.207–234, p.227. Dickson considered a normal simple algebra of order t^2p^2, p a prime which contained a normal division algebra B over a cyclic p–ic field Z. Algebra A has a B–Basis $1, j, j^2, \ldots, j^{p-1}$ where $jb = b'j$ for every b in B. That is there is a self correspondence in B which is preserved under addition, multiplication, and scalar multiplication such that if S is the generator of the Galois group of Z then $u^S = u'$ for every u in Z. The algebra B is evidently the algebra of all quantities of A commutative with Z. Since B is a division algebra it follows from my theory that either the index of A is t or is $n = pt$. In fact a necessary and sufficient condition that A have index n is that there exist no X in B such that

$$j^p = X^{(p-1)}X^{(p-2)} \cdots X''X'X \qquad \left(X^{(r)} = \left((X)^{(r-1)}\right)'\right)$$

This was the Dickson conjecture. He proved this true for $p = 2, 3$ by computation. I have gone much deeper. By the way the conditions above apply, of course to the case of crossed product with solvable group but also to the algebras of degree p^e (not crossed products) of my "On direct products" Theorem 23. There seems to be a slight difficulty in the present crossed product theory. Suppose that D is a normal division algebra of degree p^e, p a prime. If we consider the crossed product A similar to D then the subalgebra B of A, whose degree is the same as that of D and which is in fact $D \times Z$, where Z is a field, is in general not a division algebra. On the other hand if we extend F by a field whose $\left\{ \begin{matrix} \text{degree} \\ \text{order} \end{matrix} \right\}$ is prime to p the new algebra is a division algebra but is not a crossed product. I have tried to prove the existence of the latter type of extension and in fact have tried to prove

Let D be a normal division algebra of degree p^e over F. Then there exists an extension Z of F of degree prime to p such that $D' = D \times Z$ over Z is a crossed product with abelian $(p, p, \ldots, p)$ group, that is D' contains a sub–field of degree p^e which is a direct product of e cyclic p–ic fields.

However I have been unable to prove this theorem except for $e = 2$ (and of course $e = 1$). The case $e = 2$ is very much like the case $p = e = 2$ in my Transactions paper of vol.32 (1930) pg.184.

In your recent letter you had the attitude of reducing problems on normal simple algebras to problems on sub–fields of splitting fields. In my above considerations on $q(Z, D)$ I have tried to bring out the converse point of view. That is I have tried to bring out the properties of extensions of F in terms of sub–fields of normal simple algebras. Both points of view are, I believe, well taken, and both must be used if we are to have a complete theory. I also think that it has now been brought out that there is more to the theory of normal simple algebras than just the theory of normal division algebras.

I wish to accept your kind offer to send me a copy of your little 2 volume book "Hohere Algebra". I have been using it (library copy) in my course on Group Theory as a supplement to the chapters in Dicksons Modern Algebraic Theories, and I will be very pleased if you send me a copy.

You seem to have twisted my theorem on the norms in cyclic fields. I proved that if a power of α is the norm in a cyclic field then α is the norm in a sub–field. Perhaps your statement that interchanged sub–field with larger field was due to haste not to an error in thought.

Some time ago it was arranged, through Professor C.C. MacDuffee, that I was to write a tract on Algebras for the Zentralblatt. Now Dr. Neugebauer has discovered that he had arranged with Dr. A. Deuring to write on "Hypercomplex Systems" and just now discovers that the subjects are the same. Who is Deuring and what has he done that he should be the person to write on Algebras. I have, of course, dropped the whole matter now as I have intention of writing merely on the relation between algebras and matrices (Dr.Neugebauer's present desire). This latter will probably be done by MacDuffee.

I now come to a list of people who would like reprints of your Transactions paper. This will be on the enclosed sheet.

With my best regards to Brauer, Noether and yourself, I am

Very sincerely yours,

A. Adrian Albert

P.S. It seemed rather silly for Dr.Neugebauer to make the discovery after *several months* and made me rather angry.

Permit me to say I did not believe it possible for mere correspondence to arouse such deep feelings of friendship and comradeship as I now feel for you. I hope that you reciprocate

With best wishes.

A. A. Albert

P.S. again! Your criticism of my $F(\eta)$ is well founded. Blame my training! The Galois Theory of "Equations" is Dickson's. Wedderburn has written a paper (of an expository nature) on the Galois Theory of *Fields*. He would have sent it to me but for his illness. I shall correct my fault in future papers. I thank you.

A. A. A.

1.10 01.04.1932, Albert an Hasse

The University of Chicago

Department of Mathematics

April 1, 1932.

Dear Professor Hasse:

I have at last found time to answer your very interesting and enjoyable letter of March 6. We too have had an end of our term here but that meant a great deal of work as our new term (or rather *quarter*) began a week later. We have the four quarter system here of which all students and professors attend some certain three. The quarters are between 11 and 12 weeks each and, as a result, we teach only 2 courses at one time instead of the three in other universities although the number of hours of teaching is the same as elsewhere.

I went to answer your letter in the order in which it was written so we first go to your

1) I did not have, in the manuscript of our joint paper, the errors you wrote to me about except the serious one which I corrected very briefly by an application of lemma 1.[1] We don't have to worry about the order of the splitting field for the algebra of degree p^e. Just take a new splitting field by applying lemma 1, and then make a new extension of the reference field such that the splitting field has as galois group a p–group. That is, we repeat the process of your original proof with the algebra of degree p^e which you applied only to the algebra of degree m. This required only a change of two lines.

[1] Handschriftliche Bemerkung auf dem Rand des Blattes, offenbar von H. Hasse: "I should like to have a look at the proofs before their going to print"

2) My paper on normal simple algebras is already in the possession of the editors of the Transactions. I agree with you that I should publish it. For I obtained the results independently and by other methods than those used by Emmy Noether, her results have not been published (except for the van der Waerden book in which they are very obscurely presented), the introduction of ideal theory is certainly extraneous for proofs in the pure linear algebra theory of normal simple algebras,[2] and, finally, my proof is such a very simple consequence of Th. 14, 18 of my paper "On direct products". Th. 14 is the lemma at the basis of our joint paper and both it and Th. 18 come almost immediately from the uniqueness in the Wedderburn structure theorem on simple algebras.

3) I cannot understand why you still insist on working with cyclic algebras of degree n instead of degree p^e, p a prime.[3] You must certainly lose in simplicity of your theorems, and can gain nothing in generality in view of section 4, Th.5 of the American Journal paper I sent you. In view of that theorem I cannot see how your result (of your letter) is at all a generalization of my theorem 4.[4] Also your Transactions result that an algebra is cyclic if and only if it is cyclically representable could have been reduced, by the Brauer theorem, to the case of algebras of degree p^e, and then your theorem would read more precisely that A of degree p^e is cyclic if and only if A is similar to a cyclic algebra of degree p^f. For if A is similar to B of degree $p^f q$, and B is cyclic then $B = C \times D$ where C has degree p^f, is similar to A, and is cyclic.

I really believe that your whole Transactions paper could be simplified considerably if this reduction had been made to begin with.[5] Of course this is a matter of personal taste and you may not even yet agree.[6]

Now comes a more serious criticism. Your letter states that

---

[2] Handschriftliche Bemerkung auf dem Rand des Blattes, offenbar von H. Hasse: "no! invariant sub–algebras are ideals"

[3] Handschriftliche Anmerkung auf dem Rand des Blattes, augenscheinlich von H. Hasse: "for example class–field theory is as simple +++ now!"

[4] Handschriftliche Bemerkung auf dem Rand des Blattes, augenscheinlich von H. Hasse: "Only formally, not essentially"

[5] Handschriftliche Anmerkung auf dem Rand des Blattes, offenbar von H. Hasse: "no! class field theory!"

[6] Handschriftliche Bemerkung auf dem Rand des Blattes, augenscheinlich von H. Hasse: "yes!"

if Z is a cyclic field of degree n, $Z^{(r)}$ a cyclic field containing Z and of relative degree r over Z then (really by my theorem 4)

$$\left(\alpha^r, Z^{(r)}, S^{(r)}\right) = (\alpha, Z, S)_r\,.$$

You then conclude that immediately every algebra similar to a cyclic division algebra is cyclic.[7] But how do you know that if A is a cyclic algebra of degree n that *any* cyclic sub–field Z of A is contained in a $Z^{(r)}$? This is in fact false. For if $(-1, Z, S)$ is the algebra of ordinary quaternions no sub–field of this algebra is contained in a cyclic quartic field. In fact

$$(-1, Z, S)_2 = (\beta, \overline{Z}, \overline{S})$$

where evidently $\beta \neq \alpha^2 = 1$.

I do not believe that your theorem is even true, not merely that it does not follow from the above result. Of course it is true (since every normal simple algebra is then cyclic) when the reference field is an algebraic number field of finite degree. But not by any such argument as you gave in your letter to me. Also I think I have an example of an algebra over a function field which is similar to a cyclic algebra and is not cyclic, but I have not yet been able to complete the proof that the algebra is not cyclic.

4) I thank you for your photograph and books. I was very pleased to receive them both and will try to send you at least a snapshot of myself as soon as the weather is nice enough so one can be taken.

5) I am very pleased to have been asked to write a report on linear algebras for the Jahresbericht. I shall certainly accept this kind proposition. As to the translation into German I shall be compelled to accept your very good offer. I still hope to go to Germany at some not too distant time but have no idea as to whether or not this will be possible. I shall study your report and try to understand better precisely what type of report you wish me to write.

6) The report by MacDuffee is in the Bulletin of the Mathematical Society, December 1931, pg. 841. MacDuffee seems completely

[7] Handschriftliche Anmerkung auf dem Rand des Blattes, offenbar von H. Hasse: "yes! error of me!"

ignorant of the work of Artin and Brandt, and in fact of all development of ideal theory in Germany. He doesn't even know, apparently of Emmy Noether's papers on the abstract theory of ideals. Speiser's paper isn't given perhaps as much space as it deserves but he shouldn't worry about that as so much else is completely omitted. By the way, MacDuffee's report for the Zentralblatt ought to be looked at by Dr. Deuring before publication. Please don't let this spread but neither Wedderburn nor myself think very much of MacDuffee's work. I have never met him personally but Wedderburn has met him and, in fact MacDuffee was at Princeton one year.

7) Now as to some new results. I have written a paper and it is now being considered by a referee for the Bulletin on algebras $A = B \times C$ where B and C are generalized quaternion algebras over a field $K = F(u, v)$ with u and v independent indeterminates, F any *real* field. These algebras were first considered by R. Brauer (Math. Zeits. vol. 31, 1929, pp. 733–747) and Brauer took

$$B = (1, i, j, ij), \quad ji = -ij, \quad i^2 = u, \quad j^2 = b \text{ in } K,$$
$$C = (1, x, y, xy), \quad yx = -xy, \quad x^2 = v, \quad y^2 = a \text{ in } K.$$

Brauer stated that if the fields $K(\sqrt{a})$, $K(\sqrt{b})$ are distinct quadratic fields that $A = B \times C$ is a division algebra and he gave a false proof. The theorem is not true since we can take $a = -v$, $b = -u$ and have $(i + j)^2 = u + ij + ji - u = 0$.
On page 747 he made a serious error. He took

$$\xi_1 = x_1 + x_2\sqrt{a} + x_3\sqrt{b} + x_4\sqrt{a}\sqrt{b} \qquad (x_i \text{ in } K),$$

etc. and put $v = 0$ obtaining

$$(\xi_1\xi_2 - u\eta_1\eta_2)(\xi_3\xi_4 - u\eta_3\eta_4) = 0$$

He said that it followed that one ξ_ν and hence all the ξ_ν are divisible by u.* But this is false since we can have $\xi_1 = u + \sqrt{-u}$, $\xi_2 = u - \sqrt{-u}$ and yet $\xi_1\xi_2 = u^2 + u$ div. by u, not by u^2.

Brauer did not notice that he had *irrationalities* in the ξ_ν and that the

* Of course in the sense that x_1, x_2, x_3, x_4 all divisible by u as otherwise this would not have meaning.

behaviour of these irrationalities had not been restricted.[†] His proof is false and his work at that place valuable only in that he began the study of this interesting type of algebras. Brauer in fact actually was trying to prove a certain quartic form in sixteen variables (in K) was not a null form. I have shown that necessary and sufficient conditions that the algebras of Brauer be division algebras in that the quadratic form

$$u\lambda_1^2 + b\lambda_2^2 - ub\lambda_3^2 - (v\lambda_4^2 + a\lambda_5^2 - va\lambda_6^2)$$

in six variables $\lambda_1, \ldots, \lambda_6$ in K be not a null form.
I have used this theorem to now prove, for the first time in the literature, that there exist non–cyclic normal division algebras (of order 16 and the Brauer type). I now have reason to believe that I may soon be able to show that there exist non–cyclic algebras of exponent 4 (the present algebras have exponent 2). However this latter result has not yet been obtained. But we now know that non–cyclic algebras exist, that the theory of algebras over any non–modular field F is not as simple as the theory when F is an algebraic number field.

I think the above result is a very significant one for further research in division algebras, in spite of the fact that the algebras are rather simple. By the way I merely needed to take b of even degree in v, a of odd degree in v, such that each of these two polynomials in v has leading coefficient a polynomial in u of odd degree and with positive leading coefficient.

Hoping to hear from you soon, I am
Very sincerely yours,

A. Adrian Albert

P.S. I have introduced the notation $A \simeq B$ (A is *associated* with B) to mean that A is the direct product by a total matric algebra. This is more precise than merely $A \sim B$. *A.A.Albert*

[†] i.e. we might have $a = b = 0$ at $v = 0$ and know nothing about the coeff of $\sqrt{a}$, $\sqrt{b}$.

1.11 22.06.1932, Albert an Hasse

The University of Chicago

Department of Mathematics

June 22, 1932

Dear Professor Hasse:

I have been very well pleased at receiving your several letters. You are, may I say it, a very pleasing friend to write to me so often without receiving any answer. However I shall make this present letter long enough to answer *all* your communications.

I am very interested in your generalizations of my theorem on the square of an algebra of degree four. However, as you have stated, there does not appear to be any immediate application of your results. What would be to my mind the finest application is a proof of what I suspect is a true theorem. It is really a burning question with me as to whether the theorem is true. If it is true I suspect that many important results on normal division algebras over a general field will follow. We may state my conjecture as follows.

Let A be a normal division algebra. Then we say that A is *prime* if A is not expressible as a direct product of two normal division algebras no one of degree unity. It follows from the Brauer theorem that every normal division algebra of degree a prime is a prime algebra, no normal division algebra of degree de, $(d, e) = 1$, d and e not unity, is prime.
Also there exist normal division algebras of not–prime degree which are prime algebras. The conjecture is then as to the necessity of the theorem: *A necessary and sufficient condition that a normal division algebra of prime power degree p^e be a prime algebra is that it have equal degree and exponent p^e.*

I proved the above result for $p = e = 2$ in my most recent Transactions paper but have been unable to extend my proof even to the case $p = 3,\ e = 2$.

Your proof sheets of our joint Transactions paper reached me and I was very pleased with essentially all of your revisions. However I took the liberty of making one small change. First of all the theorem "there exist splitting fields of finite degree for any normal division algebra" is so well known as to be a text–book theorem (cf. Dickson, Algebren p.137) and needs no other reference. Secondly, in view of the great number of necessary changes in the proof, I think it desirable to omit as far as possible any *insertions*. So I omitted the statement you made as to what had been my previous deeper lying theorem (that is, every normal division algebra of degree n has a splitting field of degree n). Since you have found the much smoother, better proof without this more complicated theorem I think the older proof best forgotten. I certainly think your new argument the simplest possible. I sent your proof sheets to Dr. Seeley in New York long ago and, since she has not replied to my letter regarding the changes, I believe that they will be made without question.

Now as to a new result. I have finally proved that there exist non–cyclic normal division algebras of degree and exponent four and have, of course, constructed such algebras. These algebras (over a function field $F(x, y, z)$ where F is any real field) have an essentially different structure from cyclic algebras. The older non–cyclic algebras which I constructed were, after all, direct products of cyclic algebras of degree two and hence not so very different from the cyclic type. But the new algebras are not so expressible and are then essentially non–cyclic. Moreover I have shown now the complicated associativity condition

$$(\gamma_1^2 - \gamma_2^2\rho)(\gamma_3^2 - \gamma_4^2\sigma) = (\gamma_5^2 - \gamma_6^2\rho\sigma) \tag{1}$$

may be satisfied. Here we are dealing of course with a quartic field $K(u, v)$, $u^2 = \rho,\ v^2 = \sigma$ in $K = F(x, y, z)$, and a transformer j_1 such that j_1 is commutative with u, transforms v into $-v$, j_2 commutative with v and transforms u into $-u$, $j_3 = j_1j_2,\ j_1^2 = \gamma_1+\gamma_2u,\ j_2^2 = \gamma_3+\gamma_4v,\ j_3^2 = \gamma_5+\gamma_6uv$. Then the only essential associativity condition is (1) above. In my work I merely use this equation to determine ρ which occurs linearly therein. In all previous work the field $K(u, v)$ was given as defining the algebra, thus

ρ and σ were given and the problem was then to determine the γ_i so as to satisfy the associativity condition (1). This is, of course, a much more complicated problem as (1) is a quadratic equation in the γ_i.

It is interesting to note that if A is any normal division algebra of degree and exponent four then $A^2 = C^2$ where C is a cyclic normal division algebra. Also C may be easily determined by my Theorem 7 (Normal division algebras of degree four over an algebraic field) which holds for any non–modular field as reference field.

I am very sorry that your name was ommitted from the list "*Hasse*, Brauer, and Noether succeeded in completing a proof." I assure you that this ommission was not made in my original manuscript, but only in a revised copy by a very regrettable oversight. I most humbly apologize.

I have been very busy here but hope to begin work this week on my preparations for the writing of a report on linear algebras. I am of course correct in assuming that you only want the modern theory so I shall not have to refer to papers written before 1900 unless they have direct influence on modern work (as for example the remarkable work of Frobenius on matrices). I don't even want to have to mention work like that of Hawkes and Pierce which was absolutely worthless, to my mind.

Have you seen a report on normal division algebras by O.L. Davies in the Proceedings of the London Mathematical Society vol.33 (April 1932), p.537. It is very silly. He first states that it has been proved that all normal division algebras of order less than or equal to sixteen are cyclic, quoting Wedderburn's paper on order nine. They are not all cyclic as I have shown. Secondly he considers algebras of degree m, a product of distinct primes. He states that since all normal division algebras of type R *) (i.e. containing a maximal sub–field of degree equal to the degree of the algebra) and order p^2 (i.e. degree a prime) are necessarily cyclic, every normal division algebra of degree m (as above) and type R is cyclic. This does not at all follow from just theorems already known. For if A has degree m and type R it does not at all follow that the direct factors of A also have type R just as it does not follow that every regular group of degree a product of distinct primes is a direct product of cyclic groups of prime order. His paper is perfectly silly.

*) Called of type R by me very early. They are the algebras of Dickson the crossed products of E.Noether.

I forgot to mention that now my proofs of the existence of non–cyclic algebras of degree four have shown that my determination of all normal division algebras of order sixteen over a non–modular field in the 1929 Transactions gave the best possible result. It was not, however, the best possible proof. I have prepared a much shorter and smoother proof and hope to publish it in the Bulletin of the American Mathematical Society.

My American Journal paper, a copy of which is on its way to you now, appeared in vol.54 (January 1932). I am also sending you other reprints, those you already have mentioned in a recent letter.

I was interested to know that you had had conversation with someone who had met me. I do not remember Professor Maier. I am surprised that he remembers me as our meeting must have been a brief one. I met very many people in the East, unfortunately rememember but few.

I have no photograph to send you but am sending you a Kodak picture of my son Alan and myself.

With my very best regards, I am
Very sincerely yours,

A. Adrian Albert

1.12 09.02.1933, Albert an Hasse

The University of Chicago

——

Department of Mathematics

February 9, 1933.

Dear Professor Hasse:

I was very pleased to receive your letter today and most interested in its contents. I am also pleased to be able to give you what I hope is the best possible answer to the question you have asked of me.

A necessary and sufficient condition that $(c,d)\times(e,f)\sim(a,b)$, that is, a direct product of two normal simple algebras of degree two shall have exponent not more than two, is that the two algebras shall have a quadratic sub–field in common. Hence your assumption **A** is equivalent to the condition that there shall always exist (for every non–zero c,d,e,f) quantities $x_1,\dots,x_6$ not all zero and in F such that

$$[cx_1^2+dx_2^2-cdx_3^2]-[ex_3^2+fx_4^2-efx_5^2] \;=\; 0\,. \tag{1}$$

Suppose that then $x_1,\dots,x_6$ is *any one* such solution.
(Up to now my proof is not rational. But neither is your condition **A**. The following is rational, however.)

I have proved (p.537 of my Bulletin A.M.S. paper "on the equivalence of g.q.alg.") that then $(c,d)=(a,g)$ $(e,f)=(a,h)$ so that $(c,d)(e,f)=(a,b)$ with $b=gh$, where

$$a \;=\; cx_1^2+dx_2^2-cdx_3^2 \;=\; ex_4^2+fx_5^2-efx_6^2$$

and

$$g \;=\; -cd(x_2^2-cx_3^2)\,,\quad h \;=\; -ef(x_5^2-ex_6^2)$$

if not both of x_2 and x_3 are zero and not both of x_5 and x_6 are zero. If $x_2 = x_3 = 0$ then we may take $a = c$, $g = d$ in the above. In case $x_5 = x_6 = 0$ we take $e = a$, $h = f$.

It is of course obvious that a completely rational solution of your problem would require the finding of a *general* solution of the equation (1) which we know has a solution for all values of c, d, e, f in F. I don't believe such a solution can be found (or at least has been found.)

Now for my own work. I have written a rational classification of all cyclic fields of degree eight over any non–modular field F. I have given just as explicit formulae for the construction of all such fields as are well known for cyclic cubics and quartics. My formulae are even better than those of F.Mertens even for his case where F is the field of rational numbers. He used ideal theory and certainly did not obtain rational results.

Next I call a normal division algebra primary if it is not expressible as a direct product of two normal division algebras neither of degree unity. The problem I wrote to you about last June is then the following. A sufficient condition that A of degree p^e, p a prime, be primary is that A have exponent=degree. Is this condition necessary? I have now proved, using the above construction of cyclic fields of degree eight, that there exist cyclic primary normal division algebras of degree eight and exponent four. For I have proved the existence of cyclic algebras of degree eight over the function field $R(z)$ of all rational functions with rational coefficients of z, such that A^2 has index four but exponent two. If A were not primary then A^2 would have index two. Also A has exponent four if A^2 has exponent two. Hence A is primary of exponent < degree.

Suppose also that we could prove the existence of a cyclic algebra A of degree eight over $R(z)$ such that A^2 is similar to Q of degree two such that Q is not similar to the square of any cyclic division algebra of degree four. It seems almost certain that such algebras A exist. Then A would be primary and again of exponent four (but of a new type). For if A were not primary so that $A = C \times D$ where C has degree two and D has degree four then obviously $A^2 \sim D^2$. But I have proved that $D^2 \sim E^2$ where E is cyclic. I have not completed the proof of the existence of such algebras A as yet, but hope to do so in the near future.

The above first case is also the first proof of the theorem that the field $R(z)$ of a single indeterminate z does not have your property **A**. Brauer proved the same theorem for $R(y,z)$ where y and z are independent indeterminates and I have proved the same theorem for fields $F(y,z)$ where F is any real number field. But I can also easily prove that the field $F(z)$ does not satisfy property **A** for any real number field F (of course of characteristic zero.)

I have recently written a brief note on the conditions for the equivalence of any two generalized quaternion algebras over a general field F. In fact for any normal simple algebras (a,b), $ab \neq 0$ we have

Theorem. *A necessary condition that* (a,b) *and* (c,d) *be equivalent is that there exist* ξ_1, ξ_2, ξ_3 *in* F *for which*

$$c = \xi_1^2 a + \xi_2^2 b - \xi_3^2 ab\,. \tag{2}$$

For any ξ_1, ξ_2, ξ_3 *satisfying (2) algebras* (a,b) *and* (c,d) *are equivalent if and only if*

$$d = (\xi_4^2 - \xi_5^2 c) b_0 \tag{3}$$

for ξ_4, ξ_5 *in* F *where*

$$b_0 = b\,, \quad or \quad b_0 = -ab(\xi_2^2 - \xi_3^2 a)$$

according as ξ_2 *and* ξ_3 *are or are not both zero.*

I have also done some work on the problem of obtaining explicit conditions (algebraic conditions for the case of a general F) for the equivalence of any crossed products. In view of R. Brauer's recent "Uber die algebraische Struktur von Schiefkorpern" I have delayed publishing my results until I compare with his. In this same paper of Brauer (presented Nov.11, 1931) in his footnote on page 243 Brauer gives a result which we (he and I) probably obtained about the same time but which was given in my paper "On algebras of degree 2^e and pure Riemann matrices" of the Annals of Mathematics April 1932 which was received by the editors in October 24, 1931 and is a paper a summary of which was given in May 1931 by me a published in the Proceedings of the National Academy of Sciences of June, 1931. The particular theorem did not appear in this earlier paper (P.N.A.

paper) because of the character of the paper (just a report) and because the theorem is not very important. However I don't think Brauer ought to claim it as his, especially in view of the fact that he gives no proof. The result of Brauer is of course equivalent to my theorem that if A is a normal division algebra of degree p^e, p a prime, so that $A^p \sim A_p$, a normal division algebra of index (degree) t_p, then t_p divides p^{e-1}.

I have been doing a great deal of research lately on the integers represented by sets of positive ternary (classical) forms. In particular I say that a is represented by a set S of a finite number of forms (in the sense of equivalence) if some form of S represents a. Let then $S(d)$ be the set of all positive ternaries of determinant d. Write $d = e^2 f$ where f has no square factor. Then an integer $a = b^2 c$, c with no square factor is represented by $S(d)$ if and only if a has not the form

$$a = b^2 c\,, \quad c = fg\,, \quad g \equiv 7 \pmod{8}$$

such that g is prime to d and, for every odd prime divisor p of d, $(p|g) = 1$. (this, of course, the Jacobi symbol).

The above result is certainly an elegant one. I have also proved that if $S(n, d)$ is the set of all positive n–aries of determinant d, $n \geq 4$, then $S(n, d)$ represents all positive integers. However every $S(3, d)$ represents no integers $f(8nd - 1)$ and hence no positive ternary represents all positive integers.

What then is to be a theory of universal ternaries? I believe this will be a theory of chains of forms $S = (f_1, \dots, f_r)$ such that S represents all positive integers but $S - f_i$ does not have this property, $i = 1, \dots, r$. I have been unable to solve the problems suggested by this, as yet, and hope to be able to use your p–adic number theory. But I have investigated the theory of chains of sets of forms $S(d)$ and have shown that for such chains $r = 2$. Moreover I have determined all such chains. (Such a chain is a set $S(d_1, \dots, d_n)$ of all the positive ternaries of determinants $d_1, \dots, d_n$ such that the omission of one d_i makes the universal set S not universal.)

I believe the above problems very beautiful and hope they are worthy of work by other mathematicians besides myself.

Now finally as to my future plans. My trip to Germany is now indefinitely postponed as next year I have a leave of absence here and go to the Institute of Advanced Study in Princeton, on a one year appointment. I don't have any plans for the period after that.

With best regards, I am
Very sincerely yours,

A.Adrian Albert

1.13 08.08.1933, Albert an Hasse

The University of Chicago
——
Department of Mathematics

August 8, 1933.

Dear Professor Hasse:

I am very sorry not to have been able to write the letter you requested but many things prevented it. We have been terribly busy all summer with the Fair, the Society meeting, a very large group of National Research Fellows, and a large number of students trying to finish their theses. Professor Dickson has been out of town all summer so I have not been able to ask him to write also. I don't know just where he is or when he will return. My most humble apologies for the delay.

After a very long period during which I hoped to learn enough of your existence theorems to be able to answer a very important question, I have decided to ask your help. Consider a division algebra D over the field R of all rational numbers. Let the order of D be $2tn^2$ such that the centrum K of D is an algebraic field of order $2t$ over R. Let S be a correspondence of the quantities of D such that rational numbers are self corresponding $(a+b)^S = a^S + b^S$, $(ab)^S = b^S a^S$. Then D is self–reciprocal. But the quantities of its centrum are not self–corresponding. In fact the assumption is that $K = R(s,q)$, where $q^S = -q$, q^2 is in $R(s)$, $s^S = s$. The quantities of $R(s)$ are self–corresponding and are called symmetric, the quantity q is skew–symmetric.

It is known that D contains tn^2 linearly independent symmetric quantities, tn^2 linearly independent skew–symmetric quantities. The question I wish to raise is whether D contains a maximal sub–field over K which is in fact cyclic over $R(s)$ not merely over K. For the question I am studying (the theory of the multiplication algebras of pure Riemann matrices of the second kind) it is of no use to know that D is cyclic as long as it is not known that the cyclic field is composed of symmetric quantities *

It is well known that the property that a field be composed of symmetric quantities is that it be equivalent to a total real field. A skew–symmetric quantity, on the other hand, generates a field which is equivalent to a pure imaginary field over a total real field.

Thanking you for any answer you may be able to give me, I am with best regards,

Very sincerely yours,
A.Adrian Albert

* I thus wish that it be shown that $D = (Z, S, \gamma)$ where Y is cyclic of degree n over $R(s)$, $Z = Y_K$, $K = R(s, q)$, γ is in K.

1.14 10.09.1933, Hasse an Albert

10.9.33

Brief an Albert in Antwort auf Brief vom 8.8.33

I.) *Widerspruch in Alberts Forderungen.*
1.Forderung. Max. Teilkp. Z über K, zyklisch über $R(s)$
2.Forderung. Z aus symm. Größen bestehend
Wie ist das möglich, wenn Z doch den unsymm. Teilkörper K hat?
In Fußnote 2.Ford. anders interpretiert: $Z = Y_K$, wo Y zykl. über $R(s)$. Auch das scheint unmöglich, wenn z.B. der gegeb. Grad n eine Potenz von 2 ist, denn dann ist $Z = Y_K$ sicher nicht zyklisch vom Grad $2n$ über $R(s)$.

II.) *Behandlung der 1.Forderung.*
Ergänzung zu Grunwalds Existenztheorem I (Crelle 169) unter der Einschränkung: $\mathfrak{G}$ zykl. von Primzahlpotenzgrad ℓ^s.
Behauptung: Man kann dann zu Grunwalds Bedingungen 1.–4. die weitere Bedingung hinzufügen, daß K einen gegebenen zykl. Körper K_0 über k mit Gruppe $\mathfrak{G}_0 = \mathfrak{G}/\mathfrak{U}$ enthalte, wenn nur

(a) unter den gegeb. $\mathfrak{p}_k$ jeder Teiler des Führers f_0 von K_0/k vorkommt.

(b) die gegeb. Char. $\chi_k(\alpha)$ eine Fortsetzung der N.R.S. $\left(\frac{\alpha, K_0}{\mathfrak{p}_k}\right)$ bilden, d.h.

$$\chi_k(\alpha) \equiv \left(\frac{\alpha, K_0}{\mathfrak{p}_k}\right) \mod \mathfrak{U}.$$

Beweis. Wahl von Hilfsprimideal $\mathfrak{q}$. Anstatt (1) hier

$$\mathfrak{N}_{\mathfrak{q}} \equiv 1 \mod \ell^u, \quad \text{wo} \quad \ell^u \quad \text{Ordnung von} \quad \mathfrak{U}.$$

(2) ungeändert. $\chi_{\mathfrak{q}}$ homom.Abb. der pr.Restklfn. mod $\mathfrak{q}$ auf $\mathfrak{U}$. Definition von f wie l.c. dann etwas allgemeiner:

$$\chi(\mathfrak{a}) \;=\; \prod_j S_j^{a_j} \cdot \prod_k \chi_k(\alpha) \cdot \chi_{\mathfrak{q}}(\alpha)\,, \quad \text{wenn} \quad \mathfrak{a} \sim_\ell \prod_j \mathfrak{r}_j^{a_j} \alpha\,,$$

die $\mathfrak{r}_j$ wie l.c., (2') unverändert, die S_j Elemente aus $\mathfrak{G}$, die Fortsetzungen der Artin–Symbole $\left(\frac{K_0}{\mathfrak{r}_j}\right)$ sind, d.h.

$$S_j \equiv \left(\frac{K_0}{\mathfrak{r}_j}\right) \ \text{ mod. } \mathfrak{U}\,.$$

Dann

$$\chi(\mathfrak{a}) \equiv \prod_j \left(\frac{K_0}{\mathfrak{r}_j}\right)^{a_j} \prod_k \left(\frac{\alpha, K_0}{\mathfrak{p}_k}\right) \ \text{ mod. } \mathfrak{U}\,.$$

Wenn $\mathfrak{a}$ prim zu den $\mathfrak{p}_k$,

$$\prod_k \left(\frac{\alpha, K_0}{\mathfrak{p}_k}\right) \;=\; \prod_{\mathfrak{p} \neq \mathfrak{p}_k} \left(\frac{\alpha, K_0}{\mathfrak{p}}\right)^{-1} \;=\; \left(\frac{K_0}{\alpha}\right).$$

Daher

$$\chi(\mathfrak{a}) \equiv \prod_j \left(\frac{K_0}{\mathfrak{r}_j}\right)^{a_j} \cdot \left(\frac{K_0}{\alpha}\right) \;=\; \left(\frac{K_0}{\mathfrak{a}}\right) \ \text{ mod } \mathfrak{U}\,.$$

Somit enthält Klassenkörper K zu Idealgr. H definiert durch $\chi(\mathfrak{a}) = 1$ den Körper K_0.

$\mathfrak{q}$ hier analog zu (3.) l.c. so zu wählen, daß $\chi(\mathfrak{a}) = 1$ wirklich Idealgr. H definiert, also so, daß (1.) $\chi(\mathfrak{a})$ *Ideal*funktion ist:

$$\prod_k \chi_k(\varepsilon_i) \cdot \chi_{\mathfrak{q}}(\varepsilon_i) \;=\; 1 \quad \text{für Grundeinheiten } \varepsilon_i \text{ von } k\,,$$

und (2.) $\chi(\mathfrak{a})$ nicht von Normierung der Expon. a_j in ihren Restkl. mod. ℓ^{h_j} abhängt:

$$S_j^{\ell^{h_j}} \cdot \prod_k \chi_k(\zeta_j) \cdot \chi_{\mathfrak{q}}(\zeta_j) \;=\; 1\,, \quad \text{wenn} \quad \mathfrak{r}_j^{\ell^{h_j}} \zeta_j \;=\; 1\,.$$

Schließlich analog zu (4.) l.c.

$$\prod_j S_j^{p f_j} \cdot \chi_f(\pi_k) \cdot \prod_{k' \neq k} \chi_{k'}(\pi_k) \cdot \chi_{\mathfrak{q}}(\pi_k) \;=\; 1\,.$$

In allen drei Bedingungsserien gehört Aggregat der Faktoren von $\chi_{\mathfrak{q}}$ zu $\mathfrak{U}$. Daher $\mathfrak{q}$ nach Schluß aus Grundwald's Dissertation so wählbar, daß alle Bedingungen erfüllt.

Klassenkörper K zu H leistet das Verlangte.

III.) *Alberts Frage.* (K_0/k vom Grad 2, in Alberts Bezeichnung $K/R(s)$).

Triviale Reduktion auf Fall $n = 2^u$ durch Abspaltung des Körpers von ungeradem Grade, der direkt durch Grunwald's Existenztheorem III über k garantiert wird.

Notwendige Bedingung für Existenz zyklischen Körpers K vom Grad 2^u über K_0, der zyklisch (vom Grad 2^{u+1}) über k ist:

1.) Zu 2 prime Führerteiler $\mathfrak{p}$ von K_0/k müssen in K voll verzweigt sein, also $\mathfrak{N}_{\mathfrak{p}} \equiv 1 \mod 2^{u+1}$.

2.) In 2 aufgehende Führerteiler $\mathfrak{p}$ von K_0/k: Die Gruppe $\left(\frac{\alpha, K_0}{\mathfrak{p}}\right) = 1$ darf nicht durch Basiselemente endlicher 2–Potenz Ordnung $< 2^u$ erzeugt sein. Es gibt nur ein Basiselement endlicher 2–Potenz Ordnung, die höchste in $k_{\mathfrak{p}}$ enthaltene 2^ν–te Einheitswurzel. K_0 darf nicht an der Stelle $\mathfrak{p}$ mit dem lokalen Klassenkörper identisch sein, der diesem Basiselement entspricht, wenn $\nu \leq u$ ist. Speziell für $k = R$ folgt, daß quadratfreie Zahl a mit $K_0 = R(\sqrt{a})$ nicht $\equiv -1 \mod 8^3$ sein darf.

3) Reell unendliche Führerteiler $\mathfrak{p}$ von K_0/k dürfen nicht existieren.

Sind diese Bedingungen erfüllt, so gestattet $\left(\frac{\alpha_0, K}{\mathfrak{p}}\right)$ wirklich stets Fortsetzung $\chi_k(\alpha)$ in $\mathfrak{G}$, d.h. obige Bedingungen (a),(b) sind realisierbar (für die Nicht-Führerteiler trivialerweise), und zwar auch so, daß die $\mathfrak{P}_k$–Grade von K (für die Primteiler $\mathfrak{P}_k$ der $\mathfrak{p}_k$ in K_0) gleich 2^u (bzw., bei unendl. $\mathfrak{p}_k$, gleich 2) werden, also Zerfällungskörperbedingung garantiert ist.

1.15 o.D.,1934, Albert an Hasse

Fine Hall,
Princeton University,
Princeton, N.J.

Dear Professor Hasse:

I have spent the last week studying your letter and connected published work but have been unable as yet to get my desired theorem. However I still believe the result is correct and hope you can help me finish the theorem.

Consider a total real algebraic number field Ω of finite degree, a number $\mu < 0$ in Ω and with all its conjugates also negative, the relative quadratic field $K_0 = \Omega(u)$, $u^2 = \mu$. Then I believe it is clear that if $\underline{P}$ is any *infinite* prime spot of K_0 the field $K_{0\underline{P}}$ is the field of all complex numbers? If this is true then in the considerations of algebras over K_0 we need not consider the infinite prime spots.

Consider now a normal division algebra D of degree n over K_0. Then D has order $2n^2$ over Ω and I assume that D is self reciprocal under a correspondence carrying u into $-u$. In fact I assume a star operation in D such that

$$u^* = -u\,, \quad (ab)^* = b^*a^*, \quad \lambda^* = \lambda\,, \quad (a^*)^* = a$$

for every $\underline{a}$ and $\underline{b}$ of D and λ of Ω. Then D has a basis

$$v_1, \ldots, v_m\,, \quad v_0 = 1\,, \quad m = n^2$$

of quantities $v_i = v_i^*$. But

$$v_i v_j = \sum \gamma_{ijk} v_k\,, \quad v_j v_j = \sum \gamma_{ijk}^* v_k\,,$$

with γ_{ijk} in K_0 not in Ω. In particular it is evident that the minimum equation of any quantity $\underline{a} = \underline{a}^*$ has actually coefficients in Ω. What I really want is to prove the existence of an $\underline{a}$ in D such that $\underline{a}^* = \underline{a}$, the field $\Omega(a)$ has the cyclic group with respect to Ω and degree n. It will then follow immediately that, since K_0 is not equivalent to any sub–field of $\Omega(a)$, the field $K_0(a)$ is cyclic of degree n over K_0. Moreover $K_0(a)$ is a maximal sub–field of D.

It is evident that D cannot have a splitting field which is cyclic of degree $2n$ over K_0 as you discussed in your letter. For my purposes it is sufficient to prove the

Conjectural Theorem *There exists a field K cyclic of degree n over Ω such that the composite $Z = (K, K_0)$ is a splitting field of D.*

I have, however, only been able to prove

Theorem There exists a field K, cyclic of degree $2n$ over Ω such that $Z = (K, K_0)$ splits D (when n is even).

In fact let $n = \overline{n}2^e$ where $\overline{n}$ is odd. Then let P_k range over the prime spots of K_0 for which D has P_k–index $\neq 1$ and p_k the corresponding prime spots (P_k/p_k) of Ω. By Grünwalds Theorem 3 with $e_k = 1$ there exists a cyclic field $\overline{K}$ of degree $\overline{n}$ over Ω with p_k as an invariant ideal (that is with the group of $\overline{K}$ as decomposition group). Since $\overline{K}$ has degree $\overline{n}$ prime to 2 the ideal P_k is also an invariant ideal of $\overline{Z} = \overline{K} \times K_0 = \overline{K}_{K_0}$ a cyclic field of degree $\overline{n}$ over K_0 and $\overline{Z}$ has P_k–index $\overline{n}$. Thus $\overline{Z}$ is a splitting field for $D^{(1)}$ where $D = D^{(1)} \times D^{(2)}$, $D^{(1)}$ of degree $\overline{n}$, $D^{(2)}$ of degree 2^e.

The conjectural theorem has then been proved for n odd.

But now I tried to obtain the same result for degree 2^e. Again we chose K of degree 2^e over Ω and cyclic over Ω and I wish to make $Z = (K, K_0)$ a splitting field of $D^{(2)}$ of degree 2^e over K_0. I can again make the p_k invariant ideals of K but then if $\mathrm{p}_k = \Pi_k^\mu$, Π_k an invariant prime ideal of K and $\mu = 2^e$ it will not necessarily follow that P_k is an invariant ideal of Z.

For if $\mathrm{p}_k = P_k$ then it is true that P_k is invariant. If $\mathrm{p}_k = P_k^2$, that is p_k is a Führer divisor of K_0, then also P_K is invariant. But if

$\mathrm{p}_k = P_k\overline{P}_k$ then it may happen that $\Pi_k = \wp_k\overline{\wp}_k$ where $\wp_k^S = \overline{\wp}_k$, $\wp_k^{S^2} = \wp_k$ so that $\wp_k$ has $\frac{1}{2}n$ as the order of its decomposition group. Thus Z does not split $D^{(2)}$. But if we take K and hence Z of *degree* $2n$ then Z splits $D^{(2)}$.

It seems to me that something like the proof you outlined ought to give my desired result, that is a cyclic field K of degree n over Ω such that not K but (K, K_0) [1] splits the algebra D. One ought to be able to use Grunwalds Theorem 1 with group the direct product of a cyclic group of order 2^e and one of order 2 and with a given K_0 as having the group of order 2.

I should be very glad if you could provide me with a detailed proof for joint publication in a paper by both of us. The result is certainly of the greatest importance in several parts of algebraic geometry.

As you see from the address I have given you I am now in Princeton. I am with the Institute for advanced study and have been doing a large amount of research.

1) I have written a paper on algebras over modular (infinite) fields and have proved that if D is a normal division algebra of degree n over a perfect (vollkommen) field F of charakteristik p then n is not divisible by p. As the only reason for assuming that F is perfect is in case n is divisible by p the assumption that F is perfect (made by you and Brauer repeatedly) is too strong.
I have also given a brief discussion of the validity of the principal results on normal division algebras for the case where F is not perfect. In particular E.Noether and G. Koethe have given proofs that D has maximal sub–fields of the first kind and with non–zero trace (Spur). But my proof for the non–modular case (short Bulletin note) holds with no change.

I finally give the (trivial) determination of all normal division algebras of degree 2 over F of characteristic 2 and algebras of degree 3 over F of characteristic 3. Several changes in Wedderburn's proof had to be made. (TRANSACTIONS 1934).

[1] Fußnote auf dem unteren Rand des Blattes: "This is the case that seemed to you to be the difficult one. That is why I hope you can finish this proof without much difficulty."

2) I have used Artin–Schreiers paper on cyclic fields of degree p^2 over F of characteristic p and have studied all the types of fields

$$F(x) > F(u) > F$$

where $F(x)$ is not cyclic over F but $F(x)$ is cyclic of degree p over $F(u)$ which is cyclic of degree p over F

(Annals of Math. 1934)

3) I have determined all normal division algebras D of degree 4 over F of characteristic 2. Many results are different from the case of characteristic $p \neq 2$. In particular D is cyclic if and only if D has a quadratic subfield of the second kind (i.e. inseparable). In particular every D which is a direct product of two algebras of degree 2 is cyclic.

(American Journal 1934)

4) In the Bulletin 1933 pp 146–149 I have proved that every normal division algebra of degree n over any algebraic field F (of infinite degree) is cyclic and has exponent n. But normal simple algebras need not be cyclic (for there need not be any algebraic extensions of a given degree of F). In fact I have the following

Theorem Let D be a normal division algebra over an infinite field F with P as prime sub–field.
Then there exists a sub–field $\Lambda = P(\lambda_1, \ldots, \lambda_r)$ of F obtained by finite algebraic and transcendental extension of P and a normal division algebra B over Λ such that

$$D = B_F .$$

In the particular case where F is an algebraic number field the field Λ is algebraic of finite degree, B is cyclic and $D = B_F$ is cyclic.
Moreover the above theorem is trivial for we may take

$$u_1, \ldots, u_m \quad \text{as a basis of } D,$$
$$u_i u_j = \sum \gamma_{ijk} u_k ,$$

$$\Lambda = P(\gamma_{111}, \ldots, \gamma_{mmm}), \quad B = (u_1, \ldots, u_m) \quad \text{over } \Lambda .$$

5) I have proved for p an odd prime

Theorem Let the minimum equation of a primitive $p^{\underline{\text{th}}}$ root of unity ε with respect to a non–modular field F have the roots

$$\varepsilon_k = \varepsilon^{t_k}, \quad t_k \equiv t^{k-1} \pmod{p}, \quad 0 < t_k < p \quad (k = 1, 2, \ldots, n)$$

and let $g = g(\varepsilon)$ range over all the quantities of $F(\varepsilon)$ such that

$$a = \prod_{k=1}^{n} g(\varepsilon_k)^{r_k}, \quad r_k \equiv t_{p-k+1} \equiv t^{p-k} \pmod{p}$$

is not the $p^{\underline{\text{th}}}$ power of any quantity of $F(\varepsilon)$. Then if

$$\mathfrak{z}^p = a$$

the field $F(\mathfrak{z})$ is cyclic of degree np over F and

$$F(\mathfrak{z}) = F(x) \times F(\varepsilon)$$

where $F(x)$ is cyclic of degree p over F. Conversely every cylic field Z of degree p over F is generated as the uniquely determined sub–field $F(x)$ of such an $F(\mathfrak{z})$.

I have thus given a formal construction of all cyclic fields of odd prime degree over any non–modular field F. I hope to be able to use this in proving the existence of non–cyclic algebras of degree 5. I have also proved for p a prime, F non–modular,

Theorem A normal division algebra D of degree p over F is cyclic if and only if D contains a sub–field $F(y)$, $y^p = \gamma$ in F.
(Annals 1934 or Am. Journal!)

6) I have been studying certain commutative non–associative algebras of quantum mechanics. They were discussed by P. Jordan in the Göttinger Nachrichten. More recently Jordan, Neumann and Wigner have proved that all algebras satisfying

1) Commutative

2) Distributive

3) $(xy)x^2 = x(yx^2)$

4) Finite basis over field of real numbers

5) Artin real, ie. $x_1^2 + \ldots + x_n^2 = 0$ implies $x_i = 0$;

which are irreducible, are obtained by quasimultiplication

$$ab = \frac{1}{2}(a \cdot b + b \cdot a) \qquad (a \cdot b \text{ ordinary matrix product})$$

of either real matrices or all 3–rowed Hermitian matrices with elements in the real Cayley algebra of order 8. I have completed this work by proving that the last algebra $\mathfrak{M}_3^8$ is not equivalent to one of the former.

(Annals Jan 1934).

As you can see I have been quite busy. I hope you will pardon my delay in answering your letter and also my writing it instead of typewriting.

I have seen R.Brauer and E.Noether. They passed through here and stayed a short while.

I hope you can answer my letter soon and that you obtain the desired result.

Anxiously awaiting your reply, and with best regards,

I am
Very sincerely yours

A. Adrian Albert.

1.16 06.02.1934, Albert an Hasse

Fine Hall,
Feb.6, 1934.

Dear Professor Hasse:

I am happy to be able to write to you of my success in generalizing the Artin–Schreier results. Let F be a field of characteristic p. Then it is easy to prove

Lemma 1 Every cyclic field of degree p^n over F is generated by a quantity x_n such that

(1) $\quad x_i^p = x_i + a_i\,,\quad a_i$ in $Z_{i-1} = F(x_{i-1})\,,\quad x_0 = 1 \quad (i = 1, 2, \ldots, n)\,,$

and $x_1^p = x_1 + a_1$ irreducible in F. If S is the generating automorphism of Z_n then

(2) $\quad x_i^S = x_i + b_i\,, T_{Z_i|F}(b_{i+1}) = h_i \quad (h_i = 1, 2, \ldots, p-1\,;\ i = 1, \ldots, n)$

(3) $$a_i^S - a_i = b_i^p - b_i$$

Conversely if $x_1^p = x_1 + a_1$ is irreducible in F then the field $F(x_n)$ defined by (1),(2),(3) is cyclic of degree p^n over F with generating automorphism S given by (2).

Here I mean $T_{Z_i|F}(b_{i+1})$ to represent the trace (spur) of b_{i+1} in Z_i. We may write

$$c_i = \sum_{j_k = 1, \ldots, p-1} \lambda_{j_1 \ldots j_i} x_1^{j_1} \cdots x_i^{j_i}$$

for any c_i of Z_i. We call c_i non–maximal if the first coefficient $\lambda_{p-1,\ldots,p-1} = 0$. Then I have proved

Lemma 2 If $b_i = (x_1 x_2 \cdots x_{i-1})^{p-1}$ the polynomials

$$(4) \quad c_{i-1} = b_i^p - b_i = \Big[(x_1 + a_1) \cdots (x_{i-1} + a_{i-1})\Big]^{p-1} - b_i \quad (i = 2, \ldots, n)$$

are non–maximal. Then (3) have solutions a_i (unique up to an additive constant) and define cyclic fields Z_n of degree p^n over F. In fact if c_i is any non–maximal quantity of Z_i there exist solutions d_i in Z_i of

$$(5) \qquad d_i^S - d_i = c_i$$

A simple application of the above finally gives

Theorem Every cyclic field Z_1 of degree p over F of characteristic p is a subfield of cyclic overfields Z_n of degree p^n. If $Z_1 = F(x_1)$ where

$$(6) \qquad x_1^p = x_1 + a_1$$

is irreducible in F then all such fields Z_n are given by

$$(7) \qquad Z_i = F(x_i), \quad x_i^p = x_i + a_i \quad (a_i \text{ in } Z_{i-1}, \ i = 2, \ldots, n)$$

where a_i is determined uniquely up to an arbitrary additive constant in F as a solution of

$$\left\{ \begin{array}{c} a_i(x_1 + b_1, \ldots, x_{i-1} + b_{i-1}) - a_i(x_1, \ldots, x_{i-1}) = \\ = \big[(x_1 + a_1) \cdots (x_{i-1} + a_{i-1})\big]^{p-1} - b_i \\ b_i = (x_1 x_2 \ldots x_{i-1})^{p-1} \end{array} \right\}$$

Conversely every Z_n defined above for irreducible $x_1^p = x_1 + a_1$ is cyclic of degree p^n over F with generating automorphism S given by

$$x_i^S = x_i + (x_0 x_1 \cdots x_{i-1})^{p-1}, \quad x_0 = 1, \quad (i = 1, \ldots, n).$$

This is a complete solution of the question and I am sending the resulting paper to the Bulletin of the American Mathematical Society.

I have also proved the conjecture I discussed with you recently is a true one. In fact I have shown that the following theorem is true.

Let R be the field of all rational numbers, F a total real algebraic extension of R, K a total pure imaginary quadratic extension of F. Let Z be cyclic of degree n over F and total real so that $W = (Z, K)$ is cyclic of degree n over K. Let the generating automorphism of Z be given by $Z = F(x)$,

$$x \longleftrightarrow x^S$$

and define a cyclic algebra D by

$$y^i x = x^{S^i} y^i \,, \quad y^n = \gamma \text{ in } K$$

such that $\gamma = \gamma_1 + \gamma_2 q$, $K = F(q)$, $q^2 = \mu$ in F, γ_1, γ_2 in F,

$$\gamma_1^2 - \gamma_2^2 \mu = N_{Z|F}(d) \,,$$

where d is a *total positive* quantity of Z.
Then there exist Riemann matrices with D as multiplication algebra.

Conversely let D be the multiplication algebra of a pure Riemann matrix and with K as centrum. Then D is a cyclic algebra of the above type (and a division algebra).

The special conditions imposed on D are

1) D is self reciprocal but moreover such that $d^{**} = d$ for every d of D.

2) If $F(x)$ is any total real sub–field of D then there exists a self–reciprocal correspondence of D with x self corresponding.

3) Any algebra similar to D has the above two properties.

I was unable to prove the above theorem on the structure of D without using the existence part. It is easy to prove the theorem when D has odd degree. Hence let D have degree 2^ν.

Then $A = D \times M_2$ (M_2 total matric of degree 2) is cyclic of the above type and I can prove that $\gamma_1^2 - \gamma_2^2\mu = N(d)$, d total positive. But then $A^{2^{\nu-1}} \sim Q$ where $M_2 \times Q$ is also cyclic as above and hence is the algebra of a Riemann matrix. Moreover we use (3) to show that (1) holds for algebra Q. It is then easy to show that (1) holds for algebra Q. It is then easy to show that $Q = Q_1 \times K$ where Q_1 has degree 2 over F.

Now $D^{2^{\nu-1}} \sim (Q_1 \times K)$ and if we use Grunwalds theorem to obtain the existence of a field Z of degree n whose quadratic sub–field Z_2 splits Q_1 then Z will split D.

I hope the above outline of my proof is clear. I will publish the paper in the Annals of Mathematics.

I knew about your work and that of Hilbert on Kummer fields. But isn't my formula as given in the following theorems new?

Theorem 1 Let $F(x)$ have degree p over F and $F(x,\varepsilon) \equiv Z$ be normal over F. Then Z has group

(8) $$S^iT^j \qquad (i = 0,1,\ldots,p-1;\ j = 0,1,\ldots,??)$$

such that $S^p = T^n = I$, the identity automorphism,

(9) $$TS = S^eT \qquad (0 < e < p)$$

moreover $Z = F(y,\varepsilon)$ where $y^p = \mu$ in $F(\varepsilon)$,

(10) $$\varepsilon^T = \varepsilon^t,\ \ y^{(T)} = \lambda y^r,\ \ \varepsilon^{(S)} = \varepsilon,\ \ y^{(S)} = \varepsilon y,$$

$$\mu^T =_{(p)} \mu^r$$

and $r \equiv et \pmod{p}$.

The above is the Hilbert result generalized to $F(\varepsilon)$ of degree n over F, ε a primitive $p^{\underline{\text{th}}}$ root of unity, T the generating automorphism of $F(\varepsilon)$ given by $\varepsilon \leftrightarrow \varepsilon^t$. Now my result is

Theorem 2 Let λ range over all quantities of $F(\varepsilon)$ such that

(11) $$y^p = \mu = \Pi\, \lambda(\varepsilon_k)^{\rho_k} \neq 1$$

Then $F(y,\varepsilon)$ is a normal field of Theorem 1.
Conversely every normal field of Theorem 1 is generated by a μ defined as above.

Here $\rho r \equiv 1 \pmod{p}$, $\rho_k \equiv \rho^{k-1} \pmod{p}$, $1 \leq \rho_k < \rho$.

I have not found any such formula as (8) in the literature although it probably exists in the *arithmetic* work on Kummer fields.

I have borrowed your work on Klassenkörpertheorie from the University of Chicago library. It is certainly a beautiful piece of exposition and I should like to buy a copy but they are out of print.

Is it true that an English translation is being made and when will it appear?

My Institute position is neither a promotion nor permanent. The Institute for Advanced Study has only 5 members on its permanent faculty (Weyl, Einstein, Neumann, Veblen and Alexander). All the other appointments are for one year and merely to give young men an opportunity to do research unhampered by teaching duties. I have been giving a seminar on Algebra all year however.

I leave Princeton to return to Chicago on May 1st. My address will again be the University of Chicago.

I hope you will excuse my handwriting. I have been very ill (have had a bad cold and dizziness ever since) and do not want to go to work to typewrite this.

Hoping you are well and with best regards I am

Very sincerely yours,

A Adrian Albert.

P.S. Fr. E.N. speaks here tomorrow on Hypercomplex numbers and Number Theory.

1.17 02.02.1935, Hasse an Albert

Mathematisches Institut der Universität

Göttingen, den 22. 1. – 2. 2. **19** 35
Bunsenstraße 3/5

Dear Prof. Albert,

I suppose it will interest you to hear about some improvements and new results recently found by our best man here, Dr. E. Witt, in Linear Algebras and other subjects.

I. Witt has found independently of you the construction of all cyclic*) fields of degree p^h over a field R of characteristic p. When I showed him your letter about this subject, he stated that his theory was materially identical with yours. There are however some formal improvements in his method, which are in a way characteristic for Witt's outstanding ability in dealing with a formal algebraic subject. Also his method leads up to some very

*) P. T. O.
"Cylic" here and subsequently means "*separable* cyclic", i.e., the order of the cyclic Galois group is equal to (no proper divisor of) the degree of the normal field in question. Similarly later on "normal" means "separable normal". For an inseparable normal field K/k there exists an uniquely determined maximal separable subfield K_0/k such that K/K_0 may be generated by adjunction of p^{th} roots of elements of K_0, and the Galois group of K/k is the same as of K_0/k, because K/K_0 has no automorphisms different from unity.

interesting generalisations.

Let	R	be an arbitrary field of characteristic p
	R_0	its Primkörper, consisting of $0, 1, \dots, p-1$
		(elements small Greek letters)
	k	a cyclic field of degree $q = p^{h-1}$ $(h \geq 2)$ over R
		(" " Latin letters)
	K	a cyclic field of degree $qp = p^h$ $(h \geq 2)$ over R
		(" capital " ")
	σ	a generating automorphism of K/R
hence	σ	also a generating automorphism of K/R
		when applied to k only
and	σ^q	also a generating automorphism of K/k

We have to consider the following operators:

$$\begin{array}{rcll} & & \sigma - 1 & \\ & & \sigma^q - 1 & \\ Sp & = & \frac{\sigma^q - 1}{\sigma - 1} & \text{(Spur for } k/R) \\ sp & = & \frac{\sigma^{q^p} - 1}{\sigma^q - 1} & \text{(Spur for } K/k) \\ Sp\ sp & = & \frac{\sigma^{q^p} - 1}{\sigma - 1} & \text{(Spur for } K/R) \\ \pi & & \text{defined by} & \pi X = X^p - X\,. \end{array}$$

All these operators are linear and commutative with each other. The solutions of $\pi X = 0$ are the elements of R_0.

Theorem 1. *K/k may be generated by an irreducible Artin–Schreier equation*

(1.) $\quad \pi W = a\,, \quad a \neq \pi x$ *for any x in k*

as

$$K = k(W)\,.$$

For each such generation one has simultaneously:

(2.) $\quad (\sigma^q - 1)W = \zeta \neq 0$ *(in R_0)*

(3.) $\quad (\sigma - 1)W = e$ *(in k)*

(4.) $\quad Sp\ e = \zeta$

(5.) $\quad (\sigma - 1)a = \pi e\,.$

Proof. I need not reproduce the proof for the existence of a generation (1.)

for K/k. For each such generation one has (2.) with a certain $\zeta \neq 0$, as is also well–known. By applying $\sigma - 1$ to (2.) one gets:

$$(\sigma^q - 1)(\sigma - 1)W \;=\; 0\,,$$

hence (3.) with a certain e. By applying Sp to (3.) one gets (4.), and by applying $\sigma - 1$ to (1.) one gets (5.).

Corollary. *All generations of the type (1.) arise from one of them by the substitutions*

$$W' \;=\; \nu W + x\,, \quad \nu \neq 0 \;\; (\textit{in } R_0)\,, \quad x \;\; (\textit{in } k) \;\; \textit{arbitrary.}$$

(1.)–(5.) transform into

$$\begin{array}{lrclcrcl}
(1'.) & \pi W' & = & a' & \textit{with} & a' & = & \nu a + \pi x \\
(2'.) & (\sigma^q - 1)W' & = & \zeta' & \shortparallel & \zeta' & = & \nu\zeta \\
(3'.) & (\sigma - 1)W' & = & e' & \shortparallel & e' & = & \nu e \\
(4'.) & Sp\; e' & = & \zeta' & & & & \\
(5'.) & (\sigma - 1)a' & = & \pi e'. & & & &
\end{array}$$

Proof. This is also well–known, and (1'.) – (5'.) are easily deduced from (1.) – (5.) by the elementary properties of the operators. —

Now let R, k be given as before. For the moment σ signifies only a generating automorphism of k/R.

Theorem 2. *To every solution e, a of (4.),(5.) in k (with a given $\zeta \neq 0$ in R_0) equation (1.) defines a field $K = k(W)$, which is cyclic over R of degree $qp = p^h$, and has properties (2.),(3.) for a certain generating automorphism σ of K/R which continues the given σ of k/K.*

Proof. *(i) The element a generates k/R:*

$$k \;=\; R(a)\,.$$

It suffices to prove

$$(\sigma^r - 1)a \neq 0 \qquad \text{where} \quad r \;=\; p^{h-2} \;=\; \frac{q}{p}\,.$$

Suppose

$$(\sigma^r - 1)a \;=\; 0\,,$$

then by (5.)

$$\pi\,\frac{\sigma^r - 1}{\sigma - 1}\,e \;=\; 0\,,$$

hence

$$\frac{\sigma^r - 1}{\sigma - 1}\,e \;=\; \mu \quad (\text{in } R_0)$$

$$Sp\ e \;=\; \frac{\sigma^q - 1}{\sigma^r - 1}\,\frac{\sigma^r - 1}{\sigma - 1}\,e \;=\; \frac{\sigma^q - 1}{\sigma^r - 1}\,\mu \;=\; 0\,,$$

which is a contradiction to (4.).

(ii) The element a is not of the form πx .
Suppose

$$a \;=\; \pi x\,,$$

then by (5.)

$$\pi e \;=\; \pi(\sigma - 1)x\,,$$

hence

$$e \;=\; (\sigma - 1)x + \mu \qquad (\mu \text{ in } R_0)$$

$$Sp\ e \;=\; (\sigma^q - 1)x + Sp\ \mu \;=\; 0 + 0 \;=\; 0\,,$$

which is again a contradiction to (4.).

(iii) $K = R(W)$, where W is defined as a root of (1.), contains k and has degree $qp = p^h$ over R .
Since $\pi W = a$, $K = R(W)$ contains $k = R(a)$ (according to (i)).
K is of degree p over k , according to (ii).

(iv) $\overline{\sigma} W = W + e$ defines an automorphism $\overline{\sigma}$ of K/R .
We consider the polynomial

$$f(x) \;=\; \prod_{i \text{ mod. } q} (\pi x - \sigma^i a)\,.$$

$f(x)$ has coefficients in R, because $f(x)$ is invariant under σ . $f(W) = 0$ from the factor with $i = 0$.
Since $f(x)$ has degree $qp = p^h$ equal to the degree of K/R , $f(x)$ is *the*

irreducible polynomial in R with root W.
$f(W+e)=0$ from the factor with $i=1$. For $\pi(W+e) = \pi W + \pi e = a+(\sigma-1)a = a$, according to (1.),(5.). Hence $\overline{\sigma}$ is an automorphism of K/R.

(v) $\overline{\sigma}$ *continues* σ*; hence we may write* $\overline{\sigma}=\sigma$ *without misunderstanding.*
From the definition of $\overline{\sigma}$ follows:

$$(\overline{\sigma}-1)W = e,$$

any by applying π:

$$(\overline{\sigma}-1)a = \pi e = (\sigma-1)a,$$

hence

$$\overline{\sigma}a = \sigma a.$$

Since a generates k/R, $\overline{\sigma}$ continues σ.

(vi) (2.) and (3.) hold for the automorphism σ *of* K/R *as defined in (v).*
(3.) is the definition of σ; (2.) follows from (3.) by applying $\frac{\sigma^q-1}{\sigma-1}$.

(vii) The automorphism σ *of* K/R *has order* $qp=p^h$*.*
$\sigma^{qp}=1$, whereas $\sigma^q\neq 1$, for K/R, both by (2.).

(viii) K/R *is cyclic.*
The powers of σ give qp different automorphisms of K/R. Since K/R has degree qp, K/R is Galoisien, and cyclic. —

Theorem 3. *For each solution* e *(4.) in* k *(with a given* $\zeta\neq 0$ *in* R_0*) equation (5.) is soluble by an element* a^* *in* k*. The general solution* a *of (5.) arises from a fixed solution* a^* *in the form*

$$a = a^*+r, \quad r \textit{ in } R \textit{ arbitrary}.$$

Proof. The second part is immediately obvious. In order to prove the first part, notice that

$$Sp\,\pi e = \pi\zeta = 0 \quad \text{for a solution } e \text{ of (4.).}$$

Hence the proof follows immediately from the following general

Lemma. *Let K by a cyclic field of degree n over an arbitrary field k, σ a generating automorphism of K/k and Sp the Spur for K/k.*
An element A of K has $Sp\ \mathsf{A} = 0$ if and only if it is expressible as $\mathsf{A} = (\sigma - 1)\mathsf{B}$ with B in K.

Proof. We consider the following four Mengen of elements of K:

$(\sigma-1)\mathsf{A}$,	where A runs through K
$Sp\ \mathsf{A}$,	" " " " "
$\mathsf{A}_{\sigma-1}$,	all elements with $(\sigma-1)\mathsf{A}_{\sigma-1} = 0$
A_{Sp},	" " " $Sp\ \mathsf{A}_{Sp} = 0$.

$\sigma-1$ and Sp are linear operations in the n–dimensional space K/k represented by the coordinates $a_1, \ldots, a_n$ of the general element

$$\mathsf{A} = a_1\mathsf{E}_1 + \cdots + a_n\mathsf{E}_n$$

of K ($\mathsf{E}_1, \ldots, \mathsf{E}_n$ a basis for K/k). The above four Mengen are linear sub–spaces of K/k. By a well–known theorem about linear equations the sub–spaces

$$\begin{array}{rcl} (\sigma-1)\mathsf{A} & \text{and} & \mathsf{A}_{\sigma-1} \\ Sp\ \mathsf{A} & \text{and} & \mathsf{A}_{Sp} \end{array}$$

are complementary, i.e., their dimensions have sum n.

Now $\mathsf{A}_{\sigma-1} = k$ by the fundamental theorem of Galois theory. Hence $\dim \mathsf{A}_{\sigma-1} = 1$. Therefore $\dim(\sigma-1)\mathsf{A} = n-1$.

Further $Sp\,\mathsf{A} = k$. For $Sp\,\mathsf{A} \leq k$; and since the discriminant $|Sp(\mathsf{E}_i\,\mathsf{E}_k)| \neq 0$ (Dedekind!), $Sp\ \mathsf{A} \neq 0$. As a linear sub–space therefore necessarily $Sp\ \mathsf{A} = k$. Hence $\dim Sp\ \mathsf{A} = 1$. Therefore $\dim \mathsf{A}_{Sp} = n-1$.

$\dim(\sigma-1)\mathsf{A} = n-1$	$\dim\ \mathsf{A}_{\sigma-1} = 1$
$\dim\ \mathsf{A}_{Sp} = n-1$	$\dim\ Sp\ \mathsf{A} = 1$

Now obviously

$$(\sigma - 1)\mathsf{A} \leq \mathsf{A}_{Sp}\,,$$

since $Sp = 1+\sigma+\cdots+\sigma^{n-1} = \frac{\sigma^n-1}{\sigma-1}$ and $\sigma^n - 1 = 0$. As linear spaces with the same dimension therefore necessarily

$$(\sigma - 1)\mathsf{A} = \mathsf{A}_{Sp}\,.$$

Note. The Lemma is the additive analogue to Hilbert, Zahlbericht, Satz 90. I find Witt's arrangement of the proof very nice, indeed. Another more formal proof runs thus: Let C be an element of K with $Sp\ C \neq 0$. Then

$$\mathsf{B} = -\frac{1}{Sp\ C}\sum_{\nu=0}^{n-1}\frac{\sigma^\nu - 1}{\sigma - 1}\mathsf{A}\cdot\sigma^\nu C$$

satisfies $(\sigma - 1)\mathsf{B} = \mathsf{A}$. —

Theorem 4. *Equation (4.) (with a given $\zeta \neq 0$ in R_0) is soluble by an element e^* of k. The general solution e of (4.) arises from a fixed solution e^* in the form*

$$e = e^* + (\sigma - 1)x\,, \quad x \textit{ in } k \textit{ arbitrary}.$$

Proof. The solubility follows immediately from the statement $Sp\,\mathsf{A} = k$ in the proof of the Lemma. That e is the general solution, follows immediately from the Lemma itself. —

Consequences from Theorem 1 − 4 for the construction of all cyclic fields K/R of degree p^h.

1.) *Construction of the fields K to a given sub–field k of degree $q = p^{h-1}$.*

According to Theorems 1−4, one has to take all solutions $\zeta \neq 0$, e, a of (4.),(5.) and apply Theorem 2. According to the substitutions allowed by the Corollary of Theorem 1, one may restrict oneself to a fixed $\zeta \neq 0$ (say 1) and a fixed solution e of (4.), and consider only all solutions

$$a = a^* + r\,, \quad r \text{ in } R \text{ arbitrary}$$

of (5.). To each such a corresponds a field K of the type in question, and every such field K is obtained by this process.

Two elements r, r' in R lead to the same field K if and only if

$$r' = r + \pi x\,, \quad x \text{ in } k\,.$$

Let k_1 be the uniquely determined sub–field of degree p over R and

$$k_1 = R(w_1) \quad \text{with} \quad \pi w_1 = a_0 \quad (a_0 \text{ in } R, \text{ not of the form } \pi r_0 \\ \text{with } r_0 \text{ in } R)\,.$$

Then necessarily x in k_1 and

$$x = \nu w_1 + r_0 \quad \text{with} \quad \left\{ \begin{array}{l} \nu \text{ in } R_0 \\ r_0 \text{ in } R \end{array} \right\}\,,$$

hence

$$\pi x = \nu a_0 + \pi r_0\,,$$

and

$$r' = r + \nu a_0 + \pi r_0 \quad \text{with} \quad \left\{ \begin{array}{l} \nu \text{ in } R_0 \\ r_0 \text{ in } R \end{array} \right\}\,.$$

Conversely, every such r' leads to the same field K as r.

There are the following two possibilities for R:

(i) R as an additive group is of *finite order* with respect to the sub–group πR (of all πr_0, r_0 in R). Then the factor–group $R/\pi R$ has a finite basis, say $c_1, \ldots, c_n$, such that every r in R is uniquely expressable in the form

$$r = \nu_1 c_1 + \cdots + \nu_n c_n + \pi r_0 \quad \left\{ \begin{array}{l} \nu_i \text{ in } R_0 \\ r_0 \text{ in } R \end{array} \right\}\,.$$

Hence the order of $R/\pi R$ is the p–power p^n. Since one of those c_i may be taken as a_0 above, the number of essentially different elements r is p^{n-1}. Hence:

The number of different fields K of the type in question, containing a fixed field k, is p^{n-1}, where n is dependent on R only.

(ii) $R/\pi R$ is of *infinite order. Then the number in question is infinite.*

2.) *Construction of all fields K cyclic of degree p^h over R.*
One has to apply the above construction in h single steps of relative degree p:

$$R = K_0 < K_1 < \cdots < K_h = K$$

Let the lower index i always indicate elements of K_i, further sp the relative Spur for the single steps K_i/K_{i-1}. Then one has the following scheme:

$$\begin{array}{rclrclrclrcl}
\pi w_1 & = & a_0, & (\sigma-1)w_1 & = & e_0, & e_0 & = & 1 & & & \\
\pi w_2 & = & a_1, & (\sigma-1)w_2 & = & e_1, & sp\ e_1 & = & e_0, & (\sigma-1)a_1 & = & \pi e_1 \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\
\pi w_h & = & a_{h-1}, & (\sigma-1)w_h & = & e_{h-1}, & sp\ e_{h-1} & = & e_{h-2}, & (\sigma-1)a_{h-1} & = & \pi e_{h-1}\,.
\end{array}$$

σ denotes a generating automorphism of K/R, which may be considered also as a generating automorphism of each K_i/R when applied to the elements of K_i only. $e_0 = 1,\ e_1, \ldots, e_{h-1}$ denote a fixed set of solutions of the equations in the third column. a_0 is arbitrary; $a_1, \ldots, a_{h-1}$ run through all solutions of the equations in the fourth column; such a_{i-1} that lead to the same field K_i may be left out.

For the first step K_1/R the number in question is $\frac{p^n-1}{p-1}$, according to the allowed substitutions $a_0' = \nu a_0 + \pi r_0 \quad \left\{ \begin{array}{l} \nu \neq 0 \text{ in } R_0 \\ r_0 \text{ in } R \end{array} \right\}$. Together with the above statements, it follows:

(i) *If $R/\pi R$ is of finite order p^n, the number of all fields K in question is*

$$\frac{p^n-1}{p-1}\, p^{(n-1)(h-1)}.$$

(ii) *If $R/\pi R$ is of infinite order, the number in question is infinite.*

In particular:

If there is only one cyclic field K_1 of degree p over R, there is also only one cyclic field K_h of degree p^h over R for each h.

The latter is the case in one of my Crelle papers (Crelle 172, p. 77), for instance.

II. The whole theory as represented in **I** has its multiplicative analogue.

Let R be a field which contains the p^{th} roots of unity and whose characteristic is *not* p, such that the p^{th} roots of unity are different from each other. Replace (1.) – (5.) above by

$$\begin{array}{lrcll}
(1.) & w^p & = & a\,, & a \neq x^p \\
(2.) & w^{\sigma^q - 1} & = & \zeta \neq 1 & (p^{\text{th}} \text{ root of unity}) \\
(3.) & w^{\sigma - 1} & = & e & (\text{in } k) \\
(4.) & Ne & = & \zeta & \\
(5.) & a^{1-\sigma} & = & e^p &
\end{array}$$

and (1'.) – (5'.) by

$$\begin{array}{lrclcrcl}
(1'.) & W'^p & = & a' & \text{with} & a' & = & a^\nu x^p \\
(2'.) & W'^{\sigma^q - 1} & = & \zeta' & \shortparallel & \zeta' & = & \zeta^\nu \\
(3'.) & W'^{\sigma - 1} & = & e' & \shortparallel & e' & = & e^\nu \\
(4'.) & Ne' & = & \zeta' & & & & \\
(5'.) & a'^{1-\sigma} & = & e'^p & & & &
\end{array}$$

Then Theorems $1, 2$ hold again, with formally the same proofs. Also Theorem 3 holds again, with the Lemma replaced by its multiplicative analogue (Hilbert, Zahlbericht, Satz 90; the proof there is valid for a general cyclic field K/k of degree n).

The only difference arises concerning Theorem 4. Equation (4.) is not always soluble in k, for instance not when R is the rational field, $p = 2$, and $k = R(\sqrt{d})$ with d no sum of two squares in R. One has therefore a *genuine condition* for the existence of fields K of the requested type over a given field k, *namely the expressibility (4.) of a primitive* p^{th} *root of unity as a norm from* k.

Nevertheless, the analogue indicated gives the full determination of all cyclic fields of degree p^h over any field R which is not of characteristic p and contains the p^{th} roots of unity. Even the latter condition may be removed by an easy consideration, on account of the fact that the degree of the field of the p^{th} roots of unity over any R (of characteristic $\neq p$) is a divisor of $p - 1$, hence prime to p.

III. A further generalisation gives the analogous complete determination of all fields K over R of the following type:

Given a normal field k/R, group $\mathfrak{g}$, elements $\sigma, \tau, \ldots$

K/k cyclic of degree p, group $\mathfrak{Z}$, elements z

K/R normal, group $\mathfrak{G}$ with $\mathfrak{G}/\mathfrak{Z} \cong \mathfrak{g}$ and such that:
(i.) $\mathfrak{Z}$ lies in the centre of $\mathfrak{G}$, but
(ii.) $\mathfrak{Z}$ is no direct factor of $\mathfrak{G}$.

$\mathfrak{G}$ may be considered as a crossed product arising from the cyclic sub–group $\mathfrak{Z}$ by a certain given factor set $z_{\sigma,\tau}$ (in $\mathfrak{Z}$) corresponding to all pairs σ, τ of elements of $\mathfrak{g}$, i.e., $\mathfrak{G}$ is generated by the elements z of $\mathfrak{Z}$ and elements u_σ with the relations:

$$\begin{aligned} u_\sigma z &= z u_\sigma \qquad \boxed{z^\sigma = z \text{ according to (i.)}} \\ u_\sigma u_\tau &= z_{\sigma,\tau} u_{\sigma\tau} \end{aligned}$$

According to (ii.), the factor set $z_{\sigma,\tau}$ does not split, i.e., is not of the form $\frac{z_\sigma z_\tau}{z_{\sigma\tau}}$ with elements z_σ in $\mathfrak{Z}$.

R is supposed to be either of characteristic p (additive theory), or not of characteristic p and then containing the p^{th} roots of unity (multiplicative theory). It may suffice to point out the generalisation in the case of characteristic p (additive theory).

Here one has simply to replace (1.)–(5.) in Theorem 1 by

$$\begin{array}{lrcll} (1.) & \pi W & = & a\,, & a \neq \pi x \text{ for any } x \text{ in } k \\ (2.) & (z-1)W & = & \zeta \neq 0 & (\text{in } R_0) \\ (3.) & (\sigma-1)W & = & e_\sigma & (\text{in } k) \\ (4.) & e_\sigma + \sigma e_\tau - e_{\sigma\tau} & = & \zeta_{\sigma,\tau} & \\ (5.) & (\sigma-1)a & = & \pi e_\sigma\,. & \end{array}$$

(1.) is unaltered. (2.) defines a fixed isomorphism between the abstract cyclic group $\mathfrak{Z}$ of p elements and R_0 as an additive group. In (3.) e_σ is a vector of elements e_σ in k corresponding to the elements σ of $\mathfrak{g}$. In (4.) the original Spur of e is replaced by what E. Noether calls the Transformationsgrössen arising from the vector e_σ; $\zeta_{\sigma,\tau}$ denotes the elements in R_0 corresponding to the elements $z_{\sigma,\tau}$ in $\mathfrak{Z}$ by the isomorphism (2.)
(5.) is of course again a set of conditions, one for each component of the vector e_σ.

With this generalisation Theorem 1 holds. Also the Corollary and Theorem 2 hold with the obvious generalisations after the lines indicated. I need not give the new form of (1'.) – (5'.) and Theorem 2 here, nor give the detailed proof of the generalised Theorem 2. Once one has got the knack of the generalisation, there is no difficulty in carrying through all details.

Theorem 3 also generalises. The new Lemma is

Let K/k be normal with group $\mathfrak{g}$, elements σ. A vector A_σ in K has (additive) Transformationsgrössen $\mathcal{O}$, i.e.,

$$\mathsf{A}_\sigma + \sigma\mathsf{A}_\tau - \mathsf{A}_{\sigma\tau} = \mathcal{O}$$

if and only if it is expressible as

$$\mathsf{A}_\sigma = (\sigma - 1)\mathsf{B}$$

with B in K.

Proof. Let C be an element of K with $Sp\ C \neq 0$. Then

$$\mathsf{B} = \frac{1}{Sp\ C} \sum_\tau \mathsf{A}_\tau \cdot \tau C$$

satisfies the condition.

In the multiplicative case ($\mathsf{A}_\sigma \neq 0$, $\frac{\mathsf{A}_\sigma \mathsf{A}_\tau^\sigma}{\mathsf{A}_{\sigma\tau}} = 1$, $\mathsf{A}_\sigma = \mathsf{B}^{1-\sigma}$) the Lemma is due to E. Noether who gave the following very simple proof of this so–called "Hauptgeschlechtsatz im Minimalen":

Consider the crossed product of K with its Galois group and factor set 1:

$$\mathfrak{A} = (1, K) = K(u_\sigma)$$

with

$$u_\sigma \mathsf{A} = \mathsf{A}^\sigma u_\sigma\,, \qquad \mathsf{A} \text{ in } K$$
$$u_\sigma u_\tau = u_{\sigma\tau}\,.$$

Then

$$\mathsf{A} \longrightarrow \mathsf{A}\,, \quad u_\sigma \longrightarrow \mathsf{A}_\sigma u_\sigma$$

is an automorphism of $\mathfrak{A}$ which leaves the elements of K invariant, and is therefore generated by transformation with an element $\mathsf{B} \neq 0$ in K

$$\mathsf{A}_\sigma u_\sigma = \mathsf{B}^{-1} u_\sigma \mathsf{B} = \mathsf{B}^{\sigma-1} u_\sigma\,,$$

hence

$$\mathsf{A}_\sigma \,=\, \mathsf{B}^{\sigma - 1}.$$

Again Theorem 4 generalises *for the additive case:*

Every "additive factor set" $\zeta_{\sigma,\tau}$ *— i.e., satisfying the additive associativity conditions*

$$\zeta_{\sigma,\tau\nu} + \sigma\zeta_{\tau,\nu} - \zeta_{\sigma\tau,\nu} \,=\, \zeta_{\sigma,\tau} \quad — \,,$$

splits in k *:*

$$\zeta_{\sigma,\tau} \,=\, e_\sigma + \sigma e_\tau - e_{\sigma\tau}\,.$$

Proof. The vector

$$e_\sigma \,=\, \frac{1}{Sp\ c} \sum_\tau \zeta_{\sigma,\tau} \cdot \sigma\tau c$$

where c is an element of k with $Sp\ c \neq 0$, satisfies the condition. —

For the multiplicative case the splitting of $\zeta_{\sigma,\tau}$ in k is again a *genuine condition* for the existence of fields K of the type in question.

IV. Witt considered cyclic algebras H of degree p over the field

$$K \,=\, \overline{k(\mathsf{P})}$$

of all power series

$$A \,=\, \sum_{\nu=n}^{\infty} a_\nu \mathsf{P}^\nu$$

with coefficients a_ν in an arbitrary vollkommen field k of characteristic p.

Let

$$H \,=\, (A, B)$$

denote the cyclic Algebra over K defined by

$$H \,=\, K(u, v)$$

with the relations

$$\pi u \,=\, A\,, \quad v^p \,=\, B\,, \quad v^{-1}uv \,=\, u + 1\,,$$

where A is arbitrary and $B \neq 0$ in K.

Let $\rho(XdY)$ denote the residuum of the differential XdY of K, i.e., the coefficient of P^{-1} in the power series $X\,\frac{dY}{d\mathsf{P}}$.

Theorem 1. $(A,B) = (\rho\left(A\frac{dB}{B}\right), \mathsf{P})$.

This gives explicitly the analogue to what I called "arithmetisch ausgezeichnete zyklische Erzeugung" in my $\wp$–adic paper (Annalen 104) and in my Transactions paper.

For, the field (or semi–simple algebra) $K(u_0)$ with

$$\pi u_0 = \rho(A\frac{dB}{B})$$

is unverzweigt over K, because $\rho(A\frac{dB}{B})$ belongs to k (is "constant").

The proof of Theorem 1 depends on the following easily provable properties of the symbol (A,B):

$$\begin{array}{lrcl} (1.) & (A_1+A_2,B) & \sim & (A_1,B)\times(A_2,B) \\ (2.) & (A,B_1B_2) & \sim & (A,B_1)\times(A,B_2) \\ (3.) & (A,B) & \sim & K \quad \text{if and only if} \quad B \text{ is a norm from } K(u)\,. \end{array}$$

In particular,

$$(A,1)\sim K\,, \quad (A,A)\sim K$$
$$(0,B)\sim K\,.$$

The method is decomposing A additively and B multiplicatively in simple components:

$$\begin{array}{rcll} A & = & \frac{a_m}{\mathsf{P}^m}+\cdots+\frac{a_1}{\mathsf{P}}+a_0+A_0\,, & A_0 \text{ an entire power series} \\ B & = & \mathsf{P}^n b B_1\,, & B_1 \text{ an unit power series.} \end{array}$$

I will not give the details here.

Theorem 1 may be applied to the study of the law of reciprocity (in Hilbert's product form) for the exponent p in algebraic function fields K of one indeterminate with a finite field k of characteristic p as Konstantenkörper. The latter means that k itself is already the whole of all elements of K algebraic over k.

Let $\mathfrak{p}$ be any prime divisor of K and P a corresponding prime element (element of order 1 in $\mathfrak{p}$). Then the $\mathfrak{p}$–adic extension $K_{\mathfrak{p}}$ of K is of type

$$K_{\mathfrak{p}} = \overline{k_{\mathfrak{p}}(\mathsf{P})}$$

where $k_{\mathfrak{p}}$ is uniquely determined as the whole of all elements of $K_{\mathfrak{p}}$ algebraic over k. $k_{\mathfrak{p}}$ is a finite extension of k, whose degree $f_{\mathfrak{p}}$ is usually called the degree of $\mathfrak{p}$; $k_{\mathfrak{p}}$ is what I call the Konstantenkörper for $\mathfrak{p}$.

Now let the norm residue symbol $\left(\frac{A,B}{\mathfrak{p}}\right)$ for elements A, B in K be defined analogously to my Annalen 107 paper by means of the $\mathfrak{p}$–invariant $\frac{\nu_{\mathfrak{p}}}{p}$ mod. 1 of $H = (A, B)$:

$$\left(\frac{A,B}{\mathfrak{p}}\right) = e(\nu_{\mathfrak{p}}), \qquad e(\nu) = e^{\frac{2\pi i \nu}{p}}.$$

Then Theorem 1 gives easily the explicit formula

$$(*) \qquad \left(\frac{A,B}{\mathfrak{p}}\right) = e\Big(\mathfrak{S}_{\mathfrak{p}}\,\rho_{\mathfrak{p}}\left(A\frac{dB}{B}\right)\Big),$$

where $\rho_{\mathfrak{p}}$ indicates the residuum in $K_{\mathfrak{p}} = \overline{k_{\mathfrak{p}}(\mathsf{P})}$ and $\mathfrak{S}_{\mathfrak{p}}$ denotes the Spur in $k_{\mathfrak{p}}$ with respect to the Primkörper (the absolute Spur).
For, according to Theorem 1,

$$(A, B)_{\mathfrak{p}} = (\rho_{\mathfrak{p}}\left(A\frac{dB}{B}\right), \mathsf{P}),$$

and the algebra on the right hand side has $\nu_{\mathfrak{p}} = \mathfrak{S}_{\mathfrak{p}}\,\rho_{\mathfrak{p}}\left(A\frac{dB}{B}\right)$, as is easily seen.

From the explicit formula (*) the law of reciprocity in Hilbert's product form or – what is essentially the same – the Summenformel for the $\mathfrak{p}$–invariants of $H = (A, B)$, appears as an immediate consequence of the Residuensatz:

$$(**) \qquad \sum_{\mathfrak{p}} sp\ \rho_{\mathfrak{p}}\left(A\frac{dB}{B}\right) = 0,$$

where $\mathfrak{p}$ runs through all prime divisors of K, and sp denotes the Spur in $k_{\mathfrak{p}}$ with respect to k. I proved this Residuensatz in one of my recent

Crelle papers (Crelle 172, Theorie der Differentiale in algebraischen Funktionenkörpern), following entirely the analogy to the proof of the Residuensatz in the classical theory of algebraic functions (k the field of all complex numbers).

The Residuensatz (**) gives indeed the law of reciprocity

$$\prod_{\mathfrak{p}} \left(\frac{A, B}{\mathfrak{p}}\right) = 1$$

as an immediate consequence of (*).

(*) was discovered before Witt's Theorem 1 by a pupil of mine, Hermann Schmid, in his Marburg Dissertation (will appear in the Math. Zeitschr.). Witt found the more general fact about linear algebras, lying at the bottom of (*), as expressed in Theorem 1.

I value all this as a welcome insight into the nature of the law of reciprocity: we have a case here where the law of reciprocity appears as essentially identical with the Residuensatz.
Hence we may consider the law of reciprocity in algebraic number fields as an equivalent of the Residuensatz in the theory of algebraic functions.

After this digression I take up the line of Witt's investigations.

For the case where K contains the n^{th} roots of unity and has characteristic 0 or p with $p \nmid n$, and where

$$H = (A, B) = K(u, v)$$

with

$$u^n = A \neq 0\,, \quad v^n = B \neq 0\,, \quad v^{-1}uv = \zeta u\,,$$
$$\zeta \text{ primitive } n^{\text{th}} \text{ root of unity in } k$$

the so–called Vertauschungssatz holds:

$$(A, B)(B, A) \sim K\,.$$

What analogue to this Vertauschungssatz holds in the above case ("semi–additive case")

$$K = \overline{k(\mathsf{P})}, \quad k \text{ vollkommen of characteristic } p$$

$$H = (A, B) = K(u, v)$$

with

$$\pi u = A, \quad v^p = B \neq 0, \quad v^{-1}uv = u + 1\ ?$$

Witt found that there is a partial analogue, namely an analogue to the fact

B *is norm from* $K(u)$ *if and only if* A *is norm from* $K(v)$,

which follows from $(A, B)(B, A) \sim K$ in the other case ("multiplicative case") by means of the analogue to (3.). Witt found, indeed, that in the semi–additive case there is an property analogous to (3.):

(4.) $(A, B) \sim K$ *if and only if* A *is a generalised "Spur" from* $K(v)$.

Here the generalised "Spur" of an element

$$y = Y_0 + Y_1 v + \cdots + Y_{p-1} v^{p-1}, \quad Y_\nu \text{ in } K$$

of $K(v)$ is defined as follows:

$$Sp\ y = y^p - Y_0 = (Y_0^p - Y_0) + Y_1^p B + \cdots + Y_{p-1}^p B^{p-1}.$$

The proof of (4.) depends on the following identity:

$$(\dagger) \qquad \pi(u + y) = \pi u + Sp\ y \qquad \text{for any } y \text{ in } K(v),$$

which may be proved by a simple purely calculating argument. As (3.) follows immediately from the corresponding identity

$$(vx)^p = v^p N(x) \qquad \text{for any } x \text{ in } K(u),$$

(4.) follows immediately from the first identity.

(3.) and (4.) together give at once the following partial analogue to the Vertauschungssatz:

Theorem 2. *B is a norm from $K(u)$ with $\pi u = A$ if and only if A is a generalised "Spur" from $K(v)$ with $v^p = B$.*

More than this partial analogue to the full Vertauschungssatz (A, B) $(B, A) \sim K$ in the multiplicative case cannot be expected in the semi–additive case because of the different character of both sides u, v of the symbol (A, B). –

Finally Witt proved a third analogue to Hilbert's Zahlbericht, Satz 90, namely the analogue to the fact:

$$N(x) = 1 \longleftrightarrow x = x_0^{S-1} \qquad \text{for } x \text{ in } K(u) \text{ and } S = (u \to \zeta u)\,; \quad x_0 \text{ in } K(u)$$

in the multiplicative case. This analogue is again formally different because of the different character of both sides in the semi–additive case:

Theorem 3. *The generalised "Spur" of an element y in $K(v)$ is 0:*

$$Sp\; y = 0$$

if and only if y is of the form:

$$y = v\,\frac{y_0'}{y_0} \qquad \textit{where} \quad y_0' = \frac{dy_0}{dv}\,; \quad y_0 \ \textit{in} \ K(v)\,.$$

The proof follows the same lines as E.Noether's proof for the Hauptgeschlechtssatz im Minimalen. If $Sp\; y = 0$,

$$\begin{array}{lll} u & \to & u + y \\ v & \to & v \end{array}$$

is an automorphism of $H = K(u, v)$, on account of identity (†). This automorphism must be generated by transformation with a regular element y_0 of H, and y_0 must belong to $K(v)$, since v is unaltered. Hence

$$u + y = y_0^{-1} u y_0\,.$$

Let

$$y_0 = Y_0 + Y_1 v + Y_2 v^2 + \cdots + Y_{p-1} v^{p-1}\,.$$

Then

$$uy_0 \;=\; Y_0u + Y_1uv + Y_2uv^2 + \cdots + Y_{p-1}uv^{p-1}\,.$$

Since $uv^\nu = v^\nu u + \nu v^\nu$, this becomes

$$\begin{aligned} uy_0 \;&=\; Y_0 + Y_1vu + Y_2v^2u + \cdots + Y_{p-1}v^{p-1}u \\ &\quad\; + Y_1v + 2Y_2v^2 + \cdots + (p-1)Y_{p-1}v^{p-1} \\ &=\; y_0u + vy_0'. \end{aligned}$$

Hence

$$\begin{aligned} u + y \;=\; y_0^{-1}uy_0 \;&=\; u + v\frac{y_0'}{y_0}\,, \\ y \;&=\; v\frac{y_0'}{y_0}\,. \end{aligned}$$

Notice that the common Spur in the inseparable field $K(v)$ with $v^p = B$ is identically 0, because all conjugates to y equal y. I find it interesting that the logarithmic derivatives $\frac{1}{B}\frac{dB}{d\mathsf{P}}$ and $\frac{1}{y_0}\frac{dy_0}{dv}$ play a role in this theory. This throws a new light on Kummer's logarithmic differential coefficients in his treatment of the norm–residue symbol in the cyclotomic field of exponent p for the prime divisor $\mathfrak{p}$ of p.

V. You will remember my writing you about a certain connexion between general quadratic forms and linear algebras. Two years ago Artin proved that for a quadratic form

$$f(\mathfrak{x}) \;=\; a_1x_1^2 + \cdots + a_nx_n^2\,, \quad a_i \neq 0$$

with coefficients a_i in an arbitrary field k (not of characteristic 2) the normal simple algebra of exponent 2 and order $4^{\frac{n(n+1)}{2}}$ over k:

$$H \;=\; \prod_{i \leq k} (a_i,\, a_k)$$

is an invariant. Here (a, b) denotes the generalised quaternion algebra over k generated by

$$u^2 \;=\; a\,, \quad v^2 \;=\; b\,, \quad vu \;=\; -uv\,.$$

Artin's proof depends on certain identities between minors of a general symmetric matrix $A = (a_{ik})$. Witt found a very much nicer and simpler proof, that shows moreover explicitly the close connexion between the form $f(\mathfrak{x})$ and the algebra H.

Let k be an arbitrary field, not of characteristic 2. We consider quadratic forms

$$f(\mathfrak{x}) \;=\; \sum_{i,k=1}^{n} a_{ik}x_i x_k \;=\; \mathfrak{x}' A \mathfrak{x}\,,$$

where $A = (a_{ik})$ is a non–singular n–rowed symmetric matrix over k and $\mathfrak{x}$ denotes the vector of the n variables x_i as a one–columned matrix.
We are looking for invariants of $f(\mathfrak{x})$ under rational transformations:

$$\mathfrak{x} \;=\; \mathsf{P}\mathfrak{y}\,, \quad \mathsf{P} \text{ a non–singular } n\text{–rowed matrix over } k$$

$$f(\mathfrak{x}) \;=\; f(\mathsf{P}\mathfrak{y}) \;=\; g(\mathfrak{y}) \;=\; \mathfrak{y}'\mathsf{P}'A\mathsf{P}\mathfrak{y} \;=\; \mathfrak{y}'B\mathfrak{y}\,, \quad \text{where} \quad B \;=\; \mathsf{P}'A\mathsf{P}\,.$$

One invariant is the class of the discriminant

$$d \;=\; |A|$$

with respect to the equivalence

$$a \sim b \quad \text{when} \quad \frac{a}{b} = c^2 \quad (c \text{ in } k)$$

for elements $a \neq 0\,,\ b \neq 0$ in k.

In order to construct another invariant, we define a linear algebra U_0 over k as following:

$$U_0 \;=\; k(u_1, \ldots, u_n)$$

where the u_i are associative and satisfy all relations arising from the identity

$$f(\mathfrak{x}) \;=\; \Big(\sum_{i=1}^{n} u_i x_i\Big)^2 \;=\; (\mathfrak{u}\mathfrak{x})^2,$$

where $\mathfrak{u}$ denotes the one–lined matrix of the n elements u_i. The relations implied by this identity are explicitly:

$$f(\mathfrak{x}) \;=\; \sum_i a_{ii}x_i^2 + \sum_{i<k} 2a_{ik}x_i x_k \;=\; \sum_i u_i^2 x_i^2 + \sum_{i<k}(u_i u_k + u_k u_i)x_i x_k\,,$$

hence

$$u_i^2 \;=\; a_{ii}\,, \quad u_i u_k + u_k u_i \;=\; 2a_{ik} \quad (i \neq k)\,.$$

As one sees from these formulas, U_0 is indeed of finite order over k, namely of order 2^n with basis

$$1;\ u_1, \ldots, u_n;\ u_1u_2, u_1u_3, \ldots, u_{n-1}u_n;\ \ldots\ldots\ ;\ u_1u_2\ldots u_n$$

of

$$1 \quad + \quad \binom{n}{1} \quad + \quad \binom{n}{2} \quad + \quad \cdots\cdots\cdots \quad + \quad \binom{n}{n} \quad = 2^n$$

elements.

A transformation $\mathfrak{x} = \mathsf{P}\mathfrak{y}$ is connected with the contragredient transformation $\mathfrak{u} = \mathfrak{v}\mathsf{P}^{-1}$. Since this obviously leads to a linear transformation of the above basis of U_0, and since $f(\mathfrak{x}) = (\mathfrak{u}\mathfrak{x})^2 = (\mathfrak{v}\mathfrak{y})^2$, U_0 is indeed an invariant of $f(\mathfrak{x})$.

Now by a well–known theorem $f(\mathfrak{x})$ is equivalent to a pure form (with a diagonal matrix). Hence there is no restriction in supposing from the beginning

$$f(\mathfrak{x}) = a_1x_1^2 + \cdots + a_nx_n^2, \quad a_i \neq 0 \text{ in } k$$

$$A = \begin{pmatrix} a_1 & & & & & \\ & \cdot & & & & \\ & & \cdot & & & \\ & & & \cdot & & \\ & & & & \cdot & \\ & & & & & a_n \end{pmatrix}$$

$$d \sim a_1 \cdots a_n$$

For reasons of simplicity we replace the above invariant U_0 by the corresponding invariant U of

$$f^*(\mathfrak{x}^*) = a_1x_1^2 + \cdots + a_nx_n^2 - x_{n+1}^2 - \cdots - x_{2n}^2,$$

which is, of course, also an invariant of $f(\mathfrak{x})$. Call

$$U_0 = (a_1, \ldots, a_n),$$

then

$$U = (a_1, \ldots, a_n; -1, \ldots, -1).$$

Theorem 1.
$$U \sim \prod_{i \leq k} (a_i, a_k)\,.$$

Proof. Since the u_i are regular elements of U, the elements

$$u_1, \ldots, u_{n-1}\,; u_{n+1}, \ldots, u_{2n-1} \parallel u_1 \ldots u_n u_{n+1} \ldots u_{2n-1}\,,\; u_n u_{2n}$$

also generate U:

$$\begin{aligned} U &= k(u_1, \ldots, u_n, u_{n+1}, \ldots u_{2n}) \\ &= k(u_1, \ldots, u_{n-1}; u_{n+1}, \ldots, u_{2n-1} \parallel u_1 \ldots u_n u_{n+1} \ldots u_{2n-1}\,, u_n u_{2n})\,. \end{aligned}$$

We show that the two vertical bars indicate a direct composition of U. This follows immediately from the relations

$$u_1^2 = a_1, \ldots, u_n^2 = a_n,\; u_{n+1}^2 = -1, \ldots, u_{2n}^2 = -1,\; u_i u_k = -u_k u_i \quad (i \neq k)$$

For these relations imply that the elements before the bars are commutative with the elements behind the bars. The first direct factor is $(a_1, \ldots, a_{n-1}; -1, \ldots, -1)$ in the other notation. The second direct factor is $(a_1 \ldots a_n,\, a_n)$, for with $\overline{u}, \overline{v}$ for the two elements behind the bars, the above relations imply
$$\overline{v}\,\overline{u} = -\overline{v}\,\overline{u}, \quad \overline{u}^2 = a_1 \ldots a_n\,, \quad \overline{v}^2 = a_n\,.$$

Hence

$$\begin{aligned} U &= (a_1, \ldots, a_n\,; -1, \ldots, -1) \qquad (n \text{ times } -1\,) \\ &= (a_1, \ldots, a_{n-1}\,; -1, \ldots, -1) \times (a_1 \ldots a_n\,, a_n) \qquad (n-1 \text{ times } -1\,) \end{aligned}$$

Since
$$(a_1,\, -1) \;=\; (a_1,\, a_1)\,,$$
the assertion follows by complete induction.

Witt further proved

Theorem 2. *For $n = 1, 2, 3$ the invariants d, U are a complete system of invariants, i.e., two forms are equivalent if and only if they have the same invariants d, U (d in the sense of the above equivalence $\sim$, U in the sense of similarity $\sim$).*

The same holds for any $n \geq 4$ *if* k *has the property: every quadratic form of* 5 *variables allows a non–identical representation of zero.*

One may express the necessary and sufficient condition for non–identical representability of zero and for representability of an element $a \neq 0$ by $f(\mathfrak{x})$ in terms of the invariants d, U:

a.) *Representability of* 0 *.*

$$\begin{array}{ll} n = 1 & \text{impossible} \\ n = 2 & d \sim -1 \\ n = 3 & U \sim (-1,-1) \\ n = 4 & U \sim (-1,-1) \text{ in } k(\sqrt{d}) \\ (n \geq 5 & \text{always possible under assumption in Theorem 2)} \end{array}$$

b.) *Representability of* $a \neq 0$ *.*

$$\begin{array}{ll} n = 1 & a \sim d \\ n = 2 & (-a,-d) \sim U \times (-1,-1) \\ n = 3 & U \sim (-1,-1) \text{ in } k(\sqrt{-ad}) \\ (n \geq 4 & \text{always possible under the assumption in Theorem 2).} \end{array}$$

The assumption in Theorem 2 is fulfilled for the $\mathfrak{p}$–adic extensions $k_\mathfrak{p}$ of an algebraic number field k when $\mathfrak{p}$ is finite. For the real infinite primes $\mathfrak{p}$ of k one has a further invariant, Sylvester's Trägheitsindex j for $\mathfrak{p}$. Theorem 2 holds again in these cases when one adjoins j to the invariants d, U, and in the above conditions a.), b.) one has to write:

$$\begin{array}{llll} \text{a.)} & n \geq 5 & & j \neq 0, n \\ \text{b.)} & n \geq 4 & & \left\{ \begin{array}{ll} a > 0 & \text{for } j = 0 \\ a < 0 & \text{for } j = n \end{array} \right\} . \end{array}$$

It is not difficult to prove my fundamental theorem about quadratic forms over an algebraic number field k on this basis. The proof depends on a simple application of the general theorem about arithmetic progressions in k. The theorem states:

Theorem 3. *For the equivalence of two forms in* k *the equivalence in all* $k_\mathfrak{p}$ *is necessary and sufficient.*

For the representability by a form in k the representability in all $k_{\mathfrak{p}}$ is necessary and sufficient.

The proof depends moreover on the facts:

$$
\begin{array}{rcl}
d \sim 1 \text{ in } k & \longleftrightarrow & d \sim 1 \text{ in all } k_{\mathfrak{p}} \\
U \sim k & \longleftrightarrow & U_{\mathfrak{p}} \sim k_{\mathfrak{p}} \text{ for all } \mathfrak{p} \text{ (fundamental theorem} \\
& & \text{on normal simple algebras)}
\end{array}
$$

Witt finally remarked that for $n \geq 4$ there are fields k where the invariants d, U do not suffice. His example is

$$f_1 = t_1x_1^2+t_2x_2^2+t_3x_3^2+t_4x_4^2\,; \quad f_2 = -(t_2t_3t_4x_1^2+t_1t_3t_4x_2^2+t_1t_2t_4x_3^2+t_1t_2t_3x_4^2)$$

over an arbitrary field k or rather the field $k(t_1, t_2, t_3, t_4)$ of 4 algebraically independent variables $t_1, \ldots, t_4$. Those two forms have the same invariants d, U, as one easily sees. But one can show that they are not equivalent, since t_1 is not representable by f_2. This cannot be due to a Trägheitsindex, for one can chose k as the field of all complex numbers, so that $k(t_1, \ldots, t_4)$ has no order in the sense of Artin–Schreier, hence no possibility for defining a Trägheitsindex.

We do not know what sort of further invariants is required for a complete system of invariants of a quadratic form over an arbitrary field k.

I hope I have told you something of interest for you. I should be glad to hear from you about your own work. I have read your recent papers on Riemann matrices with *greatest interest*, also Weyl's new paper on this. We are studying the matter in my Seminar.

I have just read your paper on normal Kummer fields. The last result there (Theorem 5) seems to me of a particular interest. It allows to eliminate Grunwald's complicated existence theorem in the proof that every normal division algebra D of prime degree p over an algebraic number field k is cyclic.

Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ those prime spots of k for which D has $\mathfrak{p}$–index $m_{\mathfrak{p}_i} \neq 1$, hence $m_{\mathfrak{p}_i} = p$. By the fundamental theorem a field K/k splits D if (and only if) the $\mathfrak{P}_i$–degrees $n_{\mathfrak{P}_i}$ of K are multiples of the $m_{\mathfrak{p}_i}$ for the prime divisors $\mathfrak{P}_i$ in K of the $\mathfrak{p}_i$. Let now α be an element of k such that

α	contains the exact power $\mathfrak{p}_i^1$ of each finite $\mathfrak{p}_i$
$\alpha < 0$	for each real infinite $\mathfrak{p}_i$ (effective for $p = 2$ only)

The existence of such an α in k follows quite elementarily. Then $K = k(\sqrt[p]{\alpha})$ has $\mathfrak{P}_i$–degree p for each $\mathfrak{p}_i$. Hence K splits D, and therefore K occurs as a maximal commutative sub–field of D. By your Theorem 5, D is cyclic.

We are trying to generalise your Theorem 5 to prime power degree. This would eliminate Grunwald's existence theorem also for the proof that every normal division algebra D over k of arbitrary degree is cyclic. –

Another remark will interest you in this connexion: In my paper in Math.Annalen 107 I derived theorem (6.43) (exponent $\ell =$ index m) from Grunwald's existence theorem. In point of fact this deep existence theorem is not necessary for proving $\ell = m$. For one can carry through the proof with any sort of splitting field K instead of a cyclic K.

By the fundamental theorem the exponent ℓ is the lowest common multiple of the $\mathfrak{p}_i$–indices $m_{\mathfrak{p}_i}$. Now let K be any algebraic extension of degree ℓ over k with $\mathfrak{P}_i$-degree $n_{\mathfrak{P}_i} \equiv 0 \mod. m_{\mathfrak{p}_i}$. The existence of such a field K follows elementarily by $\mathfrak{p}_i$–adic approximation; see my first existence theorem in Math.Annalen 95. Then K is splitting field, hence its degree ℓ is a multiple of the index m. On the other hand ℓ divides m. Hence $\ell = m$.

With kindest regards,
sincerely Yours,

H. Hasse

P.S. Witt has just generalised his theorems about cyclic extensions K/k, which are normal with a given group $\mathfrak{G}$ with $\mathfrak{G}/\mathfrak{Z} \cong \mathfrak{g}$, to the case where $\mathfrak{Z}$ is not necessarily in the centre of $\mathfrak{G}$. The other restriction, that $\mathfrak{G}$ is no direct factor of $\mathfrak{G}$, remains as essential for his results.

Kapitel 2

Verschiedenes zu Hasse–Albert

2.1 Referat, On direct products, 1930

Zentralblatt MATH 1931 – 2004

Zbl. Math. 56.0869.01

Albert, A. A.
On direct products, cyclic division algebras, and pure Riemann matrices.
(English)
Proceedings USA Academy 16, 313-315. (1930)

Verf. gibt in dieser kurzen Note zunächst Sätze über direkte Produkte von Divisionsalgebren über einem nicht–modularen Körper F: Ein direktes Produkt $A = B \times C$ von Divisionsalgebren B und C ist dann und nur dann Divisionsalgebra, wenn für jedes Paar b aus B, c aus C auch $F(b) \times F(c)$ Divisionsalgebra ist. $A = B \times C$ ist Divisionsalgebra, wenn die Ordnungen von B und C teilerfremd sind.
Weitere Sätze machen Aussagen über Matrixdarstellungen von Divisionsalgebren: Zu jeder normalen Divisionsalgebra (als Matrixalgebra) von der Ordnung n^2 über F kann man eine normale Divisionsalgebra B_1 der gleichen Ordnung über F angeben, so daß $A = B \times B_1$ eine vollständige Matrixalgebra über F ist; umgekehrt sind bei einer Zerlegung $M = B \times C$ einer vollständigen Matrixalgebra über F in normale Divisionsalgebren B und C diese von gleicher Ordnung. Eine Matrixdarstellung in m–reihigen Matrizen existiert für eine normale Divisionsalgebra von der Ordnung n^2 über F dann und nur dann, wenn m durch n^2 teilbar ist.
Über zyklische (*Dickson*sche) Divisionsalgebren lassen sich hieraus eine Reihe von Strukturaussagen machen, die hier aufzuführen unmöglich ist. Aus allen diesen kann man Resultate für die Theorie *Riemann*scher Matrizen entnehmen (vgl. A. A. *Albert*, Proceedings USA Academy 16, 308-312; F. d. M. $56_I, 329$):

(1) Der Multiplikationsindex h einer reinen *Riemann*schen Matrix vom Geschlechte p ist Teiler von $2p$.
(2) ω sei eine reine *Riemann*sche Matrix über einem reellen Körper F; ihre Multiplikationsalgebra sei eine normale Divisionsalgebra von der Ordnung F. Diese enthalte eine Größe a vom Grade n in bezug auf F, derart, daß n verschiedene polynomiale Ausdrücke in a die Minimalgleichung $\varphi(\xi) = 0$ von a in bezug auf F erfüllen. $\varphi(\xi)$ habe eine reelle Wurzel oder nur imaginäre Wurzeln, so daß die Substitution, die jede komplexe Wurzel in ihre konjugiert komplexe überführt, vertauschbar ist mit der *Galois*gruppe von $\varphi(\xi) = 0$. Dann ist n eine Potenz von 2.
Alle diese Aussagen werden ohne Beweis angegeben. (Data of JFM: JFM 56.0869.01;)

Specht, W.; Dr. (Königsberg i. Pr.)
Published: **1930**
Document Type: **J**

2.2 Referat, On direct products, 1931

Zentralblatt **MATH**

scanned image, vol. 1,p. 116

116

Albert, A. Adrian: On direct products, cyclic division algebras, and pure Riemann matrices. Trans. amer. math. Soc. **33**, 219–234 (1931).

Es werden hyperkomplexe Systeme $\mathfrak{o}$ über einem kommutativen Körper K der Charakteristik Null betrachtet, der ohne wesentliche Einschränkung als Unterring von $\mathfrak{o}$ angenommen werden kann. $\mathfrak{o}$ heißt normal bez. K, wenn K das Zentrum von $\mathfrak{o}$ ist. Über diese normalen hyperkomplexen Systeme wird bewiesen: 1. Stellt man ein einfaches normales hyperkomplexes System $\mathfrak{o}$ nach Maclagan – Wedderburn dar als vollständigen Matrizenring in einem (nicht notwendig kommutativen) Körper P, so wird P normal bez. K. Umgekehrt ist ein vollständiger Matrizenring in einem bez. K normalen Körper endlichen Grades ein normales hyperkomplexes System. 2. Das direkte Produkt zweier einfacher bez. K normaler hyperkomplexer Systeme ist wieder einfach und normal bez. K. Und umgekehrt: Wird das einfache bez. K normale hyperkomplexe System $\mathfrak{o}$ direktes Produkt $\mathfrak{o} = \mathfrak{o}_1 \times \mathfrak{o}_2$ zweier hyperkomplexer Systeme $\mathfrak{o}_1$ und $\mathfrak{o}_2$, so sind $\mathfrak{o}_1$ und $\mathfrak{o}_2$ einfache normale hyperkomplexe Systeme. 3. Ist das einfache normale hyperkomplexe System $\mathfrak{o}$ direktes Produkt $\mathfrak{o} = \mathfrak{o}_1 \times \mathfrak{o}_2$ und sind $\mathfrak{o}$ und $\mathfrak{o}_1$ vollständige Matrizenringe, so auch $\mathfrak{o}_2$. 4. Zu einem normalen (nicht notwendig kommutativen) Körper $\mathfrak{k}_1$ vom Grade n^2 über K existiert immer ein normaler Körper $\mathfrak{k}_2$ desselben Grades, so daß das direkte Produkt $\mathfrak{o} = \mathfrak{k}_1 \times \mathfrak{k}_2$ vollständiger Matrizenring in K wird. 5. Ist der vollständige Matrizenring $\mathfrak{o}$ direktes Produkt der beiden normalen Körper $\mathfrak{k}_1$ und $\mathfrak{k}_2$, so haben beide denselben Grad bez. K. Für die spätere Anwendung auf Riemannsche Matrizen ist vor allem von Bedeutung: 6. Dann und nur dann ist der normale Körper $\mathfrak{k}$ des Grades n^2 als ein Unterring des Ringes aller m–reihigen quadratischen Matrizen in K darstellbar, wenn m durch n^2 teilbar wird. Es gilt noch: 7. Das direkte Produkt zweier normaler Körper von den zueinander teilerfremden Graden m^2 und n^2 ist wieder normal. Alle bisher genauer untersuchten normalen Körper von endlichem Grade über K sind zyklisch. Unter einem zyklischen hyperkomplexen System $\mathfrak{o}$ versteht man ein solches vom Grade n^2 über K mit den Basiselementen $\alpha^r\beta^s$ $(r,s=0,1,\ldots,n-1)$, wo α und β den folgenden Bedingungen unterworfen sind: a) $\beta^n=\kappa\neq 0$, κ aus K. b) α ist Nullstelle eines Galoisschen Polynoms $f(x)=(x-\alpha)(x-\alpha^s)\ldots(x-\alpha^{s^{n-1}})$ mit zyklischer Gruppe, deren erzeugende Substitution S ist. c) $\beta\alpha\beta^{-1}=\alpha^s$. Für die allgemeinen zyklischen Körper vom Grade n^2 wird die Untersuchung ihrer

117

Struktur zurückgeführt auf solche von Primzahlpotenzgrad p^{2e} mittels 8. Ist $n=p_1^{e_1}\ldots p_t^{e_t}$ die Zerlegung von n in paarweise teilerfremde Primzahlpotenzen und $\mathfrak{k}$ ein zyklischer Körper vom Grade n^2 über K, so wird $\mathfrak{k}$ das direkte Produkt von t zyklischen Körpern $\mathfrak{k}_i$ vom Grade $p_i^{2e_i}$. Umgekehrt sind alle solchen direkten Produkte wieder zyklische Körper. W e d d e r b u r n bewies: Das zyklische hyperkomplexe System $\mathfrak{o}$ ist Körper, wenn keine Potenz κ^r $(r<n)$ Norm (=Produkt der konjugierten) eines Elementes aus $K[\alpha]$ ist; für $n=2$ oder $n=3$ genügt es sogar schon, daß κ selbst nicht Norm eines Elementes aus $K[\alpha]$ wird. Hiervon gilt folgende Ausdehnung und Umkehrung: 9. Ist p Primzahl und $\mathfrak{o}$ ein zyklisches hyperkomplexes System vom Grade p^2 über K, so ist $\mathfrak{o}$ dann und nur dann Körper, wenn κ niemals Norm eines Elementes aus $K[\alpha]$ ist. Ist $\mathfrak{k}$ zyklischer Körper vom Grade n^2 mit $n=p_1^{e_1}\ldots p_t^{e_t}$ und κ^s Norm eines Elementes aus $K[\alpha]$, so wird s teilbar durch $p_1\ldots p_t$. Diese Resultate erlauben, 4. zu verschärfen in einem Spezialfall: Sei $\mathfrak{k}_1$ ein zyklischer Körper vom Grade p^2, $\mathfrak{k}_2$ ein normaler Körper desselben Grades (p Primzahl). Dann und nur dann ist das direkte Produkt $\mathfrak{o}=\mathfrak{k}_1\times\mathfrak{k}_2$ vollständiger Matrizenring, wenn $\mathfrak{k}_2$ zu $\mathfrak{k}_1$ isomorph ist. Die vorstehenden Ergebnisse werden angewandt auf die Theorie der reinen Riemannschen Matrizen, (s. K r a z e r – W i r t i n g e r , Abelsche Funkt. u. allg. Thetafunkt.; Enzyklop. d. math. Wiss. II B **7**, 114; ferner G . S c o r z a , intorno alla teoria gen. delle matrici di Riemann e ad alc. sue applic.; Rendiconti Palermo **41** [1916], 263–380). Es wird vor

allem gezeigt: 10. Der Multiplikabilitätsindex h einer reinen Riemannschen Matrix vom Geschlecht p in einem reellen Körper ist ein Teiler von $2p$. Zuletzt werden noch normale Körper vom Typus R_n betrachtet. Man versteht darunter einen normalen Körper $\mathfrak{k}$ vom Grade n^2, der ein Element α enthält, das Nullstelle eines Galoisschen Polynoms $f(x)$ mit Koeffizienten aus K vom Minimalgrade n ist. Bedeuten $S, T, \ldots$ die n Automorphismen der Galois–Gruppe von $K(\alpha)$ bez. K, so zeigt man, daß $\mathfrak{k}$ eine Basis der Form $\alpha^{j-1}\beta_s$ hat $(j = 1, \ldots, n)$, wo die $\beta_s, \beta_r, \ldots$ gerade n den Automorphismen entsprechende Elemente aus $\mathfrak{k}$ sind, für die gilt: a) $\beta_E = 1$ (E die Gruppeneinheit), b) $\beta_s \alpha \beta_s^{-1} = \alpha^s$, c) $\beta_r \beta_s = g_{r,s} \beta_{sr}$ mit Elementen $g_{s,r}$ aus $K[\alpha]$. Hierüber wird schließlich gezeigt: 11. Eine reine Riemannsche Matrix über einem reellen Körper K habe als zugehöriges Multiplikationssystem einen normalen Körper $\mathfrak{k}$ vom Typus R_n; die Nullstellen $\alpha^s, \alpha^r, \ldots, \ldots$ des durch das ausgezeichnete Element α bestimmten Polynoms $f(x)$ aus K vom Grade n seien entweder alle reell oder alle imaginär. Dann wird n eine Potenz von 2. *Grell (Jena).*

2.3 Referat, On normal division algebras, 1931

Zentralblatt **MATH**

scanned image, vol. 1,p. 117

117

Albert, A. Adrian: On normal division algebras of type R **in thirty–six units.** Trans. amer. math. Soc. **33**, 235–243 (1931).

Von den im vorangehenden Referat zuletzt besprochenen normalen Körpern vom Typus $R = R_n$ sind die einfachsten diejenigen, bei denen die Galois–Gruppe von $K(\alpha)$ bez. K zyklisch wird. Man kennt bislang noch keine Körper vom Typus R_n von nichtzyklischer Struktur. In der vorliegenden Arbeit wird gezeigt, daß für $n = 6$ alle diese Systeme zyklisch sind.

Grell (Jena).

2.4 Referat, On direct products, 1931

Zentralblatt **MATH**

scanned image, vol. 2,p. 246

246

Albert, A. Adrian: On direct products. Trans. amer. math. Soc. **33**, 690–711 (1931).

Ausgangspunkt der Untersuchungen bildet eine Divisionsalgebra $\mathfrak{A}$, die über dem Körper $\mathfrak{K}$ der Charakteristik Null normal und vom Range n^2 ist; sofern nicht ausdrücklich anders bemerkt, liegen die Koeffizienten der im folgenden auftretenden Polynome sowie die Elemente der Matrizen der vorkommenden Matrizenringe immer in $\mathfrak{K}$, und auf $\mathfrak{K}$ als Grundbereich beziehen sich auch die Begriffe Rang, Grad, Normalität, hyperkomplexes System. Es wird das direkte Produkt $\mathfrak{A}' = \mathfrak{A} \times \mathfrak{K}(\eta)$ aus $\mathfrak{A}$ und einer einfachen algebraischen Erweiterung $\mathfrak{K}(\eta)$ betrachtet. Aus einer Reihe an sich interessanter Ergebnisse sei hier nur der Hauptsatz genannt: 1. Hat η den Grad r, so wird $\mathfrak{A}' = \mathfrak{A} \times \mathfrak{K}(\eta) = \mathfrak{H} \times \mathfrak{B}$, wo $\mathfrak{H}$ ein vollständiger Ring aus Matrizen vom Grade s, $\mathfrak{B}$ eine Divisionsalgebra vom Range rt^2 und $n = st$, $r = se$ mit ganzzahligem e ist. $\mathfrak{B}$ ist normal vom Range t^2 über $\mathfrak{K}(\eta)$. Als eine der Folgerungen von 1. sei erwähnt: 2. Ist $\mathfrak{K}(\eta)$ von Primzahlgrad, so ist $\mathfrak{A} \times \mathfrak{K}(\eta)$ dann und nur dann Divisionsalgebra, wenn kein Element aus $\mathfrak{A}$ Nullstelle des zu η gehörigen irreduziblen Polynoms ist. Durch Verbindung dieser Resultate mit der Galoisschen Theorie folgt: 3. Hat $\mathfrak{A}$ insbesondere den Rang p^2 (p =Primzahl), so gibt es eine einfache algebraische Erweiterung $\mathfrak{K}(\eta)$ vom Grade r mit $(p-1)! \equiv 0 \pmod{r}$, so daß $\mathfrak{A} \times \mathfrak{K}(\eta)$ zyklische normale Divisionsalgebra vom Range p^2 bezüglich $\mathfrak{K}(\eta)$ wird. Ferner: 4. Ist $n = p^e q$ mit $e > 0$, $q > 1$ und $(p, q) = 1$, so gibt es eine einfache algebraische Erweiterung $\mathfrak{K}(\eta)$ vom Grade r mit $(p, r) = 1$, so daß $\mathfrak{A} \times \mathfrak{K}(\eta) = \mathfrak{H} \times \mathfrak{B}$, wo $\mathfrak{H}$ der vollständige Matrizenring vom Range q^2 und $\mathfrak{B}$ eine Divisionsalgebra ist, die bezüglich ihres Zentrums $\mathfrak{K}(\eta)$ normal und vom Range p^{2e} wird. Außerdem besteht noch der Struktursatz 5. Hat $\mathfrak{A}$ den Rang p^{2e} (p =Primzahl) und das Element α den Grad p^e, so existiert eine einfache algebraische Erweiterung $\mathfrak{L} = \mathfrak{K}(\eta)$ vom Grade r mit $(p,r) = 1$, so daß $\mathfrak{A} \times \mathfrak{L}$ normale Divisionsalgebra über $\mathfrak{L}$ ist, $\mathfrak{L}(\alpha)$ über $\mathfrak{L}$ den Grad p^e besitzt und in $\mathfrak{L}(\alpha)$ Elemente $\alpha = \alpha_e, \alpha_{e-1}, \dots, \alpha_1$ existieren, so daß bei $\mathfrak{L}_0 = \mathfrak{L}$, $\mathfrak{L}_i = \mathfrak{L}(\alpha_i)$ $(i = 1, \dots, e)$ der Körper $\mathfrak{L}_i$ zyklisch von der Ordnung p über $\mathfrak{L}_{i-1}$ und vom Grade p^i bezüglich $\mathfrak{K}$ ist. — Ein allgemeines Dicksonsches hyperkomplexes System $\mathfrak{D}$ ist gegeben durch seine Basis $\alpha^a\beta^b$ $(a, b = 0, 1, \dots, n-1)$ mit folgenden Relationen: a) α ist Nullstelle eines zyklischen Polynoms n ten Grades $\Phi(\omega) = (\omega - \alpha^S)(\omega - \alpha^{S^2}) \dots (\omega - \alpha^{S^n})$, wo S der erzeugende Automorphismus der Galoisschen Gruppe, also $S^n = E$ ist; b) $\beta^n = \gamma$ mit γ aus $\mathfrak{K}$; c) für ein beliebiges Element $f(\alpha)$ aus $\mathfrak{K}(\alpha)$ ist $\beta^b f(\alpha) = f(\alpha^{S^b})\beta^b$. $\mathfrak{D} = \mathfrak{K}[\Phi, S, \gamma]$ heißt überdies zyklisch, wenn $\mathfrak{D}$ einfach und normal bezüglich $\mathfrak{K}$ ist. Man hat 6. Dann und nur dann ist ein Dicksonsches System zyklisch, wenn $\gamma \neq 0$, sowie 7. Sind $\mathfrak{D}_1 = \mathfrak{K}[\Phi, S, \gamma_1]$ und $\mathfrak{D}_2 = \mathfrak{K}[\Phi, S, \gamma_2]$ zyklisch vom Range n^2, so wird $\mathfrak{D}_1 \times \mathfrak{D}_2 = \mathfrak{M} \times \mathfrak{C}$, wo $\mathfrak{C} = \mathfrak{K}[\Phi, S, \gamma_1\gamma_2]$ und $\mathfrak{M}$ der volle Matrizenring vom Range n^2 ist. — Für ein einfaches normales hyperkomplexes

247

System $\mathfrak{S}$ definiert man das direkte Produkt $\mathfrak{S}^2$ mittels eines zu $\mathfrak{S}$ isomorphen und von $\mathfrak{S}$ bis auf $\mathfrak{K}$ verschiedenen $\mathfrak{S}^*$ durch $\mathfrak{S}^2 = \mathfrak{S} \times \mathfrak{S}^*$ und entsprechend die direkte Potenz $\mathfrak{S}^\nu = \mathfrak{S}^{\nu-1} \times \mathfrak{S}^*$. Gibt es eine Zahl σ, für die $\mathfrak{S}^\sigma$ vollständiger Matrizenring wird, so heißt die kleinste derartige Zahl ϱ der Exponent von $\mathfrak{S}$. Es gilt 8. Die normale Divisionsalgebra $\mathfrak{A}$ vom Range n^2 hat einen Exponenten ϱ, der Teiler von n und Vielfaches jeder in n aufgehenden Primzahl ist. Zu $\mathfrak{A}$ gibt es eine Reihe untereinander nichtisomorpher normaler Divisionsalgebren $\mathfrak{A}_0 = \mathfrak{K}$, $\mathfrak{A}_1 = \mathfrak{A}, \mathfrak{A}_2, \dots, \mathfrak{A}_{\varrho-1}$ mit den Rangzahlen t_k^2 und ein System voller Matrizenringe $\mathfrak{H}_k$ vom Range s_k^2 mit $n = t_k \times s_k$, so daß bei $\alpha \geq 2$ und $\alpha = \lambda\varrho + k$ mit $\lambda \geq 0$, $0 \leq k < \varrho$ die direkte Potenz $\mathfrak{A}^\alpha$ isomorph wird zu $\mathfrak{M}^{\alpha-1} \times \mathfrak{H}_k \times \mathfrak{A}_k$ ($\mathfrak{M}$ der volle Matrizenring n ten Grades). Ist $i + j \equiv k \pmod{\varrho}$, so wird $\mathfrak{A}_i \times \mathfrak{A}_j$ isomorph zu $\mathfrak{A}_k \times \mathfrak{H}_{ij}$, wo $\mathfrak{H}_{ij}$ ein voller Matrizenring ist. Schließlich wird noch ein Beweis gegeben für den folgenden R. Brauerschen, unabhängig aber vom Verfasser aufgestellten Satz 9. Ist $n = p_1^{e_1} \dots p_m^{e_m}$ die Primzahlzerlegung von n, so wird jede normale Divisionsalgebra $\mathfrak{A}$ vom Range n^2 bis auf Isomorphie eindeutig direktes Produkt $\mathfrak{A} = \mathfrak{B}_1 \times \dots \times \mathfrak{B}_m$ normaler Divisionsalgebren $\mathfrak{B}_i$ vom Range $p_i^{2e_i}$. Während R. B r a u e r Hilfsmittel der Darstellungstheorie heranzieht (vgl. seine auch sonst noch mit der referierten sich berührende Arbeit: Über Systeme hyperkomplexer Zahlen, Math. Z. **30**, 79–107), beruht der hier geführte Beweis auf reinen Struktursätzen.

Grell (Jena).

2.5 Referat, Algebras of degree ..., 1932

Zentralblatt **MATH**

scanned image, vol. 4,p. 100

100

Albert, A. Adrian: Algebras of degree 2^e and pure Riemann matrices. Ann. of Math., II. s. **33**, 311–318 (1932).

Für eine normale Divisionsalgebra $\mathfrak{A}$ vom Grade n ist der Exponent die kleinste natürliche Zahl ϱ, für die das direkte Produkt $\mathfrak{A}^\varrho$ voller Matrizenring wird. Bei der Niederschrift der Arbeit lag das Resultat von H. H a s s e vor, daß der Exponent jeder zyklischen Algebra über einem algebraischen Zahlkörper gleich ihrem Grad sei. Da inzwischen durch R. B r a u e r , H. H a s s e und E. N o e t h e r jede normale Divisionsalgebra über einem Zahlkörper als zyklisch erkannt ist, gilt also diese Aussage über den Exponenten für beliebige normale Divisionsalgebren; das vom Verfasser für solche Algebren des Grades 2^k in dieser Richtung erzielte Resultat ist damit überholt. Von Bedeutung aber ist das mit diesen Untersuchungen in Zusammenhang stehende Ergebnis, daß die einzigen selbstreziproken normalen Divisionsalgebren über einem algebraischen Zahlkörper entweder den Grad eins oder zwei haben. Es ergibt sich daraus nämlich, daß die Multiplikationsalgebren erster Art einer reinen Riemannschen Matrix (vgl. A. A l b e r t , The Structure of pure Riemann matrices ...; Rend. Circ. mat. Palermo **55**, 57–115 (1931); dies. Zbl. **1**, 266) entweder vom Typus eines algebraischen Zahlkörpers oder vom Typus einer verallgemeinerten Quaternionenalgebra über einem solchen Zahlkörper sind. *Grell (Jena).*

2.6 Referat, Normal division algebras ..., 1932

Zentralblatt **MATH**

scanned image, vol. 4,p. 100

100

Albert, A. Adrian: Normal division algebras of degree four over an algebraic field. Trans. Amer. Math. Soc. **34**, 363–372 (1932).

Enthält als wesentlichstes Resultat für den Spezialfall $n = 4$ den Beweis des einige Zeit nach Fertigstellung dieser Arbeit von R. B r a u e r , H. H a s s e und E. N o e t h e r in ihrer gemeinsamen Arbeit „Beweis eines Hauptsatzes in der Theorie der Algebren" (vgl. dies. Zbl. **3**, 244) für allgemeines n bewiesenen Satzes, daß jede normale Divisionsalgebra über einem endlichen algebraischen Zahlkörper zyklisch ist.

Grell (Jena).

2.7 Referat, On normal simple algebras, 1932

Zentralblatt **MATH**

scanned image, vol. 5,p. 50

50

Albert, A. Adrian: On normal simple algebras. Trans. Amer. Math. Soc. **34**, 620 bis 625 (1932).

Eine Algebra $\mathfrak{A}$ über einem (kommutativen) Körper F der Charakteristik Null heißt assoziiert mit einer ebensolchen $\mathfrak{B}$, $\mathfrak{A} \cong \mathfrak{B}$, wenn $\mathfrak{A}$ direktes Produkt $\mathfrak{A} = \mathfrak{M} \times \mathfrak{B}$ von $\mathfrak{B}$ und einem vollen Matrizenring $\mathfrak{M}$ über F wird. Insbesondere ist nach W e d d e r b u r n eine normale einfache Algebra $\mathfrak{A}$ assoziiert mit einer normalen Divisionsalgebra $\mathfrak{D}$, $\mathfrak{A} = \mathfrak{M} \times \mathfrak{D}$; hat diese die Ordnung m^2 (Grad m), so heißt m der Index und der Grad des zugehörigen $\mathfrak{M}$ der Koindex von $\mathfrak{A}$. Sei die normale einfache Algebra $\mathfrak{A}$ assoziiert mit der normalen Divisionsalgebra $\mathfrak{D}$; Z bedeute eine algebraische Erweiterung vom Range r über F. Dann heißt $\mathfrak{A}$ eine Darstellung von Z durch $\mathfrak{D}$, wenn $\mathfrak{A}$ einen zu Z isomorphen Unterkörper enthält. Zu vorgegebenem Z und $\mathfrak{D}$ gibt es immer Darstellungen, insbesondere existiert eine bis auf Isomorphie eindeutig bestimmte kleinste Darstellung $\mathfrak{B} = \mathfrak{H} \times \mathfrak{D}$, deren Koindex der Quotientenindex $q = q(\mathfrak{D}, Z)$ von Z und $\mathfrak{D}$ heißt. Das Hauptresultat der Arbeit besteht nun in folgendem Satz: Jede Darstellung $\mathfrak{A}$ von Z durch $\mathfrak{D}$ ist assoziiert mit einer kleinsten Darstellung $\mathfrak{B}$, d.h. $\mathfrak{A} = \mathfrak{H} \times \mathfrak{B} = \mathfrak{H} \times (\mathfrak{E} \times \mathfrak{D}) = \mathfrak{M} \times \mathfrak{D}$; dabei sind $\mathfrak{M} = \mathfrak{H} \times \mathfrak{E}$, $\mathfrak{H}$ und $\mathfrak{E}$ volle Matrizenringe über F. Der Quotientenindex q ist ein Teiler von r, $r = sq$, und $\mathfrak{D}' = Z \times \mathfrak{D}$ ist eine Divisionsalgebra vom Grade $m' = m/s$ über Z. Ist Z_0 aus $\mathfrak{A}$ ein mit Z isomorphes Teilsystem, so ist die Algebra aller mit Z_0 vertauschbaren Elemente von $\mathfrak{A}$ eine normale einfache Algebra $\mathfrak{H} \times \mathfrak{D}_0$ über Z_0, wobei $\mathfrak{D}_0$ zu $\mathfrak{D}'$ unter Erhaltung des Isomorphismus $Z \leftrightarrow Z_0$ isomorph ist. — Mit Hilfe dieses Resultates wird eine von L.E. D i c k s o n aufgestellte Vermutung über eine gewisse Klasse normaler einfacher Algebren

$\mathfrak{E}$ allgemein bestätigt: die notwendige und hinreichende Bedingung dafür, daß ein solches $\mathfrak{E}$ Divisionsalgebra ist, besteht darin, daß ein bestimmtes Element einer in $\mathfrak{E}$ enthaltenen gewissen Divisionsalgebra $\mathfrak{D}$ nicht Norm eines Elementes aus $\mathfrak{D}$ sein darf. *Grell* (Jena).

Kapitel 3

Namenverzeichnis

Kapitel 4

Stichwortverzeichnis