SYMMETRY OF ALGEBRAS OVER A NUMBER FIELD

SAUNDERS MACLANE

1. **Introduction.** If the field N is a finite normal extension of the field k, and if K is a normal subfield with $N \supset K \supset k$, a fundamental theorem of Galois theory asserts that every automorphism λ of K over k can be extended to an automorphism of N. As Teichmüller in [7][1] and Jacobson [6, p. 36] have shown, the development of a Galois theory for a simple algebra A with center K leads naturally to a related question: can a given automorphism λ of K be extended to an automorphism of the algebra A ? In the event that all automorphisms λ of a finite group Q of automorphisms of K are so extendable, we say that the algebra A is Q-normal. Since any total matric algebra over K is Q-normal for any Q, it follows that any algebra A similar to a Q-normal algebra is Q-normal, and hence that "Q-normality" is a property of algebra classes. Furthermore, if k is the subfield of all elements of K invariant under each automorphism λ of Q, any simple algebra B with center k yields a scalar extension B_K with center K which is Q-normal. The algebra class of any B_K (that is, the algebra classes obtained by scalar extension from k) may thus be termed *trivially* Q-normal. The further investigation of these properties thus raises the problem: are there any algebras which are Q-normal but not trivially so?

If $K \supset k$ are p-adic fields, Köthe [5] has shown that every algebra class over K may be obtained by scalar extension from k, so that in this case all Q-normal algebra classes are trivial. If K is an algebraic number field, he shows that there are algebra classes over K which cannot be obtained by scalar extension. If Q is cyclic, and if K is an algebraic number field, Deuring [2] showed that every Q-normal algebra class is trivially Q-normal. By using three-dimensional cocycles, the same results may be proved for Q cyclic and any field K (Teichmüller, op. cit. p. 149 or Eilenberg-MacLane [3, Corollary 7.3]). In case Q is not cyclic, the answer to our question apparently depends on the arithmetic properties of the field K. In case K is an algebraic number field, the algebra classes can be described completely by the usual arithmetic invariants (cf. for example, Deuring [1, chap. VII]). Using these invariants and the above facts about the cyclic case we obtain in Theorem 3 a complete description of the

Presented to the Society, September, 5, 1947; received by the editors June. 20, 1947.

[1] Numbers in brackets refer to the bibliography at the end of the paper.

group of nontrivial Q-normal algebra classes over a number field. In particular, the existence of nontrivial Q-normal algebras follows (§5), for Q a four group and K a suitable field. In view of the possibility of describing Q-normal algebras by cocycles [3, 7] this also shows that there exist three-dimensional cocycles of Q in K which are not coboundaries.

2. **Invariants of scalar extensions.** A simple algebra B with center an algebraic number field k has for each finite or infinite prime divisor p of k (that is, for each valuation of k) a rational number (B/p) (mod 1) as local invariant. It is known (cf. Deuring [1, p. 119]) that the mapping

$$B \rightarrow \{ \cdots, (B/p), \cdots \}$$

yields an isomorphism of the group of algebra classes over k into a subgroup of the direct sum of groups of rational numbers $\rho(p)$ mod 1, with one summand for each p. The isomorphic image consists of those elements $\{\rho(p)\}$ in the direct sum such that:

(1) only a finite number of $\rho(p)$ are $\not\equiv 0 \pmod 1$;

(2a) if p is a real infinite prime divisor of k, $2\rho(p) \equiv 0 \pmod 1$;

(2b) if p is a complex infinite prime divisor of k, $\rho(p) \equiv 0 \pmod 1$;

(3) $\sum_p \rho(p) \equiv 0 \pmod 1$.

(The third condition expresses the reciprocity theorem in terms of the invariants of an algebra.)

Consider Q, a finite group of automorphisms of the algebraic number field K, and k, the subfield of elements of K invariant under Q. Each prime divisor p in k has $S = S(p)$ factors $P_1, \cdots, P_S$ in K, and these prime divisors P_i of K are all conjugate under automorphisms of Q. The complete field K_{P_i} of K in the valuation associated with P_i is a finite extension of the complete field k_p. The degrees $[K_{P_i}:k_p]$ of these extensions are equal, for $i = 1, \cdots, S$. This degree $M(p)$, called the local degree of p, satisfies

$$M(p)S(p) = n = [K:k]. \tag{4}$$

For any algebra B over k, the scalar extension B_K to K has as invariants

$$(B_K/P_i) = M(p)(B/p), \qquad P_i \mid p \tag{5}$$

(cf. Deuring [1, p. 113, Theorem 4] or Köthe [5, Theorem 3]).

We introduce the integers

$$s = \text{g.c.d. } S(p), \qquad m = \text{l.c.m. } M(p), \qquad \text{over all } p. \tag{6}$$

Then (4) gives $n = sm$.

LEMMA. *The algebra class of A over K can be obtained by scalar extension from an algebra class of an algebra B over k if and only if the invariants (A/P) of A satisfy the conditions*

$$\text{(i)} \qquad (A/P) \equiv (A/P') \quad \textit{for } P, P' \textit{ conjugate over } k,$$

$$\text{(ii)} \qquad \sum_{p} (m/M(p))(A/P) \equiv 0 \pmod 1, \qquad P \mid p,$$

where the sum is taken over all p of k, using some one factor P in K for each p.

PROOF. First suppose that the class of A is that of B_K. Then $(A/P) \equiv (B_K/P) \pmod 1$, and condition (i) follows from (5) above. After choosing some rational number $(A/P)/M(p)$, the invariants of B must be

$$(7) \qquad (B/p) \equiv (A/P)/M(p) + i(p)/M(p) \pmod 1, \qquad P \mid p,$$

for suitable integers $i(p)$. Since $\sum(B/p) \equiv 0 \pmod 1$, summation of (7) over all p and multiplication by m gives (ii).

Conversely, given an A which satisfies (i) and (ii), use (7) to define the invariants of a prospective algebra B. Such an algebra will exist, provided only that $\sum(B/p) \equiv 0 \pmod 1$. By (ii), $\sum(A/P)/M(p)$ is a rational number with denominator m. By suitable choice of integers $i(p)$, the (finite) sum $\sum i(p)/M(p)$ can be made equal to the negative of this quotient. The algebra B which thus exists has $(B_K/P) \equiv (A/P)$ by (5) and (7), hence the class of A is obtained by scalar extension.

COROLLARY. *If Q is cyclic, condition* (ii) *of the lemma may be omitted.*

PROOF. Let λ be a generator of the cyclic group Q. The Tchebotareff density theorem (Hasse [4, p. 133]) shows that there is a prime ideal p in k which has its decomposition group in K generated by λ. This prime p is then unramified and undecomposed in K; hence $M(p) = n$ and $m = n$. Thus $m/M(p) = S(p)$, and in this case condition (ii) reduces simply to the condition (3) which must be satisfied in any event by the invariants of A.

3. Conditions for Q-normality.

THEOREM 1. *The central simple algebra A over K is Q-normal if and only if, for every automorphism $\lambda \in Q$, the algebra class of A can be obtained by scalar extension from an algebra class over K_λ, the subfield of elements of K fixed under λ.*

The proof does not require that K be a number field. In case A is obtained by scalar extension from an algebra B over K_λ, the automorphism λ can clearly be extended to B_K and hence also to the similar algebra A. This gives the required Q-normality. Conversely, the Q-normality of A implies that A is normal for the cyclic subgroup generated by λ. But, by the result quoted in the introduction, every cyclically normal algebra class is trivially such, so that the algebra class of A can be obtained by scalar extension from K_λ, q.e.d.

The condition for normality over a number field now takes the following very simple form.

THEOREM 2. *The algebra A is Q-normal if and only if its invariants satisfy the condition* $(A/P)\equiv(A/P')$ (mod 1) *for every pair of prime divisors P, P' of K conjugate under Q.*

PROOF. Assume that A is Q-normal. Given conjugate divisors P, P', select a $\lambda\in Q$ mapping P into P'. By Theorem 1, the algebra class of A is obtained by scalar extension from an algebra B_λ over K_λ. Since λ maps P into P', P and P' are both factors of the same prime divisor p_λ in K_λ. The condition then follows from the corollary in §2. The converse proof is similar.

4. The group of normal algebra classes.

THEOREM 3. *The group of Q-normal algebra classes over K, modulo the subgroup of those algebra classes which are trivially Q-normal, is a cyclic group of order s, where $s=$*g.c.d. *$S(p)$ is the greatest common divisor for all p of the numbers $S(p)$ of distinct prime factors in K of the prime divisors p of k. To calculate s from the $S(p)$, it suffices to consider only the finite primes (that is, the prime ideals) of k.*

PROOF. Consider first the last remark. An infinite prime divisor p_∞ has $S(p_\infty)=n$ factors in K unless $n\equiv 0$ (mod 2), p_∞ is real, and its factors P_∞ in K are all complex; in this case $S(p_\infty)=n/2$. By the Tchebotareff density theorem, there then exists a prime ideal P in K with cyclic decomposition group of order 2, so that $S(p)=n/2$ for $P|p$, and $S(p_\infty)$ may be omitted in forming the g.c.d.

For each Q-normal algebra A, define

$$J(A) \equiv m\sum_p (A/P)/M(p) \pmod 1, \qquad P\mid p,$$

where P is any one selected factor of p in K. Since $ms=n$,

$$sJ(A) \equiv \sum_p (A/P)[n/M(p)] \equiv \sum_p S(p)(A/P) \equiv \sum_P (A/P) \equiv 0,$$

hence $J(A)$ is a rational number with denominator a factor of s.

Conversely, let t/s be a given rational number, where t is an integer. Since s is the g.c.d. of the $S(p)$, we can find a finite number of finite prime divisors $p_1, \cdots, p_r$ with integers μ_i such that

$$ts = \sum \mu_i S(p_i).$$

In particular, $\sum(\mu_i/s)S(p_i) \equiv 0 \pmod 1$; hence there exists an algebra A with invariants

$$(A/P_{ij}) = \mu_i/s \qquad \text{for each } P_{ij} \text{ with } P_{ij} \mid p_i.$$

By construction, A has equal invariants at conjugate divisors, hence is Q-normal by Theorem 2. Furthermore

$$J(A) \equiv m\sum_i \mu_i/(sM(p_i)) \equiv (m/sn)\sum_i \mu_i S(p_i)$$
$$\equiv tm/n \equiv tm/ms \equiv t/s \pmod 1.$$

Thus $J(A)$ may be any rational number with denominator s.

Therefore J is a homomorphic mapping of the group of Q-normal algebra classes onto the rationals with denominator s, mod 1. By the lemma, the kernel of this homomorphism is precisely the subgroup of trivially Q-normal algebra classes; hence the theorem.

5. **Construction of examples.** By Theorem 3, the construction of nontrivial Q-normal algebras requires only the construction of a normal algebraic number field K over some k with $s>1$. For example, it would suffice to have K with the four group as Galois group such that every prime divisor in k has at least two (and therefore either 2 or 4) prime divisors in K. In other words, one must find a K in which the factorizations $p=P^4$, $p=P^2$, and $p=P$ are impossible. In the third case, the Galois group of K over k would be the group of the local extension K_p/k_p, which is cyclic, and not the four group. There remain only the ramified cases $p=P^4$, $p=P^2$.

Consider $K=R(13^{1/2}, 17^{1/2})$, where R is the field of rationals. By considering the possible inertial groups of a ramified prime, it follows that any ramified prime must be ramified in at least two cyclic subfields, and hence that 13, 17 are the only (finite) ramified primes in K. But 13 has two distinct factors in $R(17^{1/2})$ and hence in K, while 17 has two distinct factors in $R(13^{1/2})$, and hence in K. Thus in both cases $p=(P_1P_2)^2$, and $s=2$ for this field. There thus exists one nontrivial Q-normal algebra over this field. A similar result holds for $R(2^{1/2}, 17^{1/2})$, and so on.

Bibliography

1. M. Deuring, *Algebren*, Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 4, no. 1, Berlin, 1935.

2. ———, *Einbettung von Algebren in Algebren mit kleinerem Zentrum*, J. Reine Angew. Math. vol. 175 (1936) pp. 124–128.

3. S. Eilenberg and S. MacLane, *Cohomology and Galois theory*. I. *Normality of algebras and Teichmüller's cocycle.* To appear in Trans. Amer. Math. Soc.

4. H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil II, *Reziprozitätsgesetze*, Jber. Deutschen Math. Verein. (1930) Ergänzungsband 6.

5. G. Köthe, *Erweiterung des Zentrums einfacher Algebren*, Math. Ann. vol. 107 (1933) pp. 761–766.

6. N. Jacobson, *A note on division rings*, Amer. J. Math. vol. 69 (1947) pp. 27–36.

7. O. Teichmüller, *Über die sogenannte nichtkommutative Galoische Theorie und die Relation* $\xi_{\lambda,\mu,\nu}\xi_{\lambda,\mu\nu,\pi}\xi^{\lambda}_{\mu,\nu,\pi}=\xi_{\lambda,\mu\nu,\pi}\xi_{\mu\lambda,\nu,\pi}$, Deutsche Mathematik vol. 5 (1940) pp. 138–149.

Harvard University