Degrees of Sums in a Separable Field Extension
Author(s): I. M. Isaacs
Source: *Proceedings of the American Mathematical Society*, Vol. 25, No. 3 (Jul., 1970), pp. 638-641
Published by: American Mathematical Society
Stable URL: http://www.jstor.org/stable/2036661
Accessed: 02/06/2010 16:14

DEGREES OF SUMS IN A SEPARABLE FIELD EXTENSION

I. M. ISAACS

Let F be any field and suppose that E is a separable algebraic extension of F. For elements $\alpha \in E$, we let $\mathrm{dg}\alpha$ denote the degree of the minimal polynomial of α over F. Let $\alpha, \beta \in E$, $\mathrm{dg}\alpha = m$, $\mathrm{dg}\beta = n$ and suppose $(m, n) = 1$. It is easy to see that $[F(\alpha, \beta): F] = mn$, and by a standard theorem of field theory (for instance see Theorem 40 on p. 49 of [1]), there exists an element $\gamma \in E$ such that $F(\alpha, \beta) = F(\gamma)$ and thus $\mathrm{dg}\gamma = mn$. In fact, the usual proof of this theorem produces (for infinite F) an element of the form $\gamma = \alpha + \lambda\beta$, with $\lambda \in F$. In this paper we show that in many cases the choice of $\lambda \in F$ is completely arbitrary, as long as $\lambda \neq 0$. In Theorem 63 on p. 71 of [1], it is shown that if $n > m$ and n is a prime different from the characteristic of F, then $\mathrm{dg}(\alpha + \beta) = mn$. The present result includes this.

THEOREM. *Let $E \supseteq F$ be fields as above and let $\alpha, \beta \in E$ with $\mathrm{dg}\alpha = m$, $\mathrm{dg}\beta = n$ and $(m, n) = 1$. Then $\mathrm{dg}(\alpha + \lambda\beta) = mn$ for all $\lambda \neq 0$, $\lambda \in F$ unless the characteristic, $\mathrm{ch}(F) = p$, a prime, and*

(a) *$p \mid mn$ or $p < \min(m, n)$,*

(b) *if m or n is a prime power, then $p \mid mn$ and*

(c) *if $q > m$ for every prime $q \mid n$, then $p \mid n$.*

PROOF. First we reduce the problem to one of group representations. We may assume without loss that E is a finite degree Galois extension of F and let G be the Galois group. Then G transitively permutes the sets of roots $A = \{\alpha_i \mid 1 \leq i \leq m\}$ and $B = \{\beta_j \mid 1 \leq j \leq n\}$ of the minimal polynomials of α and β. Let $V \subseteq E$ be the linear span of $A \cup B$ over F. Then V is a G-module over F and in the action of G on V there exists orbits A and B with $|A| = m$, $|B| = n$ and $(m, n) = 1$. We show by induction on $|G|$ that if $\alpha \in A$ and $\beta \in B$, then $\alpha + \beta$ lies in an orbit of size mn, unless $\mathrm{ch}(F) = p$ and (a), (b) and (c) hold. This will clearly prove the theorem when applied to $\lambda\beta$ in place of β.

Let $H = G_\alpha$ and $K = G_\beta$, the stabilizers in G of α and β. Then $|G:H| = m$, $|G:K| = n$ and since $(m, n) = 1$, a standard argument yields $|G:H \cap K| = mn$ and H and K act transitively on B and A respectively. It follows that G is transitive on $A \times B$ and thus all elements of V of the form $\alpha_i + \beta_j$ are conjugate under the action of G. Suppose that $\alpha + \beta$ does not have exactly mn conjugates. Then not all $\alpha_i + \beta_j$ are distinct and we may assume that $\alpha + \beta = \alpha_a + \beta_b$, where

Received by the editors June 6, 1969.

$\alpha\neq\alpha_a$ or $\beta\neq\beta_b$. Then $\alpha-\alpha_a=\beta_b-\beta\neq 0$ and the subspaces W_1 and W_2 of V, spanned by A and B respectively, intersect nontrivially. Set $U=W_1\cap W_2$ and observe that W_1, W_2 and U are all G-invariant spaces.

We remark at this point that if $\mathrm{ch}(F)\nmid |G|$, an easy contradiction could be obtained using the fact that W_1 and W_2 are homomorphic images of the permutation modules determined by the actions of G on A and B. In this case, the modules would be completely reducible and since $HK=G$, it is not hard to see that they can have only the principal module as a common constituent. It would follow that G acts trivially on U and thus fixes $\alpha-\alpha_a$. A contradiction results since $\alpha_a=\alpha^g$ for some $g\in G$ and the order of this element is prime to $\mathrm{ch}(F)$. It does not appear that this approach will lead to a full proof of the theorem and we continue along a different route.

It may be assumed that G acts faithfully on V or else the inductive hypothesis may be applied to G/N where N is the kernel of the action, and the result follows immediately. Suppose now that there is a subgroup $G_0<G$ which acts so that the orbits A_0 and B_0 of α and β under G_0 satisfy $m_0|m$, $n_0|n$, $\alpha_a\in A_0$ and $\beta_b\in B_0$, where $m_0=|A_0|$ and $n_0=|B_0|$. Then $(m_0, n_0)=1$ and since $\alpha+\beta=\alpha_a+\beta_b$, the number of conjugates of $\alpha+\beta$ under G_0 is $<m_0n_0$. Therefore, induction applies and $\mathrm{ch}(F)=p$, a prime, and by (a), $p|m_0n_0$ or $p<\min(m_0, n_0)$. Since $m_0|m$ and $n_0|n$, (a) holds for m and n. Similarly, (b) and (c) for m_0 and n_0 imply the corresponding statements for m and n. We may assume then that no such subgroup G_0 exists.

Now, G permutes the set of cosets of U in W_1 and is transitive on the set of those cosets which contain elements of A. All of these, therefore, contain equal numbers of elements of A. We have α, $\alpha_a\in U+\alpha$ and if $A_0=A\cap(U+\alpha)$, then $|A_0|\,|m$. Let G_0 be the stabilizer of the coset $U+\alpha$ in G. Clearly, $H\subseteq G_0$ and hence G_0 is transitive on B. We claim that G_0 is transitive on A_0. If $\alpha_i\in A_0$, then for some $g\in G$, $\alpha^g=\alpha_i$. Thus $(U+\alpha)^g=U+\alpha_i=U+\alpha$ and so $g\in G_0$. This establishes transitivity and by the preceding paragraph, we cannot have $G_0<G$. Therefore G stabilizes $U+\alpha$ and hence $A\subseteq U+\alpha$. By similar reasoning, $B\subseteq U+\beta$. Now, $\beta_j=u_j+\beta$ for some $u_j\in U$. Summing over $\beta_j\in B$, we obtain $\sum\beta_j=\sum u_j+n\beta$. Thus $n\beta=u+\gamma$, where $u\in U$ and $\gamma=\sum\beta_j$ is fixed by G. Let $N\lhd G$ be the kernel of the action of G on A. Then N fixes all elements of $W_1\supseteq U$ and thus N fixes $n\beta$. If $\mathrm{ch}(F)\nmid n$, then N fixes β and hence fixes all $\beta_j=u_j+\beta$. Thus N acts trivially on V, the span of $A\cup B$. Therefore, $N=1$ and G is isomorphic to a subgroup of the symmetric group on A. Thus $|G|\,|m!$ and $n|m!$.

Since $n>1$, this shows that the hypotheses of (c) cannot occur if $\mathrm{ch}(F)\nmid n$ and thus (c) is proved.

Now suppose that $\mathrm{ch}(F)\nmid mn$. By interchanging A and B in the above argument, we obtain $|G|\,|n!$ and all prime divisors of $|G|$ are $\leqq \min(m, n)$. If $\mathrm{ch}(F)=0$ or $\mathrm{ch}(F)=p$, a prime $>\min(m, n)$, then $\mathrm{ch}(F)\nmid |G|$. If m or n is a prime power, we may suppose that $m=q^e$ and let Q be a Sylow q-subgroup of K. Then $|K:K\cap H|=q^e$ so $K=(K\cap H)Q$ and it follows that Q is transitive on A. Thus under any of the assumptions: $\mathrm{ch}(F)=0$, $\mathrm{ch}(F)=p>\min(m, n)$ or $m=q^e$, there exists a subgroup $L\subseteq K$ which is transitive on A and such that $\mathrm{ch}(F)\nmid |L|$. The proof will be complete if a contradiction follows from the existence of such an L.

We have seen that $n\beta=u+\gamma$ where $u\in U$ and γ is fixed by G. As $U\subseteq W_1$, we have $u=\sum \xi_i\alpha_i$, where $\xi_i\in F$ and α_i runs over A. Now if $x\in L\subseteq K$, we have

$$(*)\qquad \beta = \beta^x = \frac{1}{n}\sum \xi_i\alpha_i^x + \frac{1}{n}\gamma.$$

Now set $\delta=\sum\alpha_i$, and observe that since L is transitive on A, we have $\sum_{x\in L}\alpha_i^x=(|L|/m)\delta$. Now, summing (*) over L, we obtain

$$|L|\beta = \frac{|L|}{mn}\sum \xi_i\delta + \frac{|L|}{n}\gamma.$$

Note that division by m and n in the above equations makes sense in V since $\mathrm{ch}(F)\nmid mn$. Since γ and δ are fixed by G and $\mathrm{ch}(F)\nmid |L|$, it follows that β is fixed by G. This is a contradiction since $\beta\neq\beta_b$ and the proof is complete.

Now let G be any finite group and suppose that V is any faithful finite-dimensional G-module over a field K. Suppose that $u, v\in V$ are permuted by G into orbits of sizes m and n respectively and that $u+v$ lies in an orbit of size k. Then there exist fields $E\supseteq F\supseteq K$, with E a finite separable extension of F, and elements $\alpha, \beta\in E$ with $\mathrm{dg}\alpha=m$, $\mathrm{dg}\beta=n$ and $\mathrm{dg}(\alpha+\beta)=k$.

The construction is as follows. Let $e=\dim_K(V)$ and let $X_1, X_2, \cdots, X_e$ be indeterminates. Set $R=K[X_1, \cdots, X_e]$ and let E be the quotient field of R. Now fix a basis for V and identify this basis with the X_i so that V is identified with the linear span of the X_i in R. Now it is clear that each element of G determines an automorphism of R and hence of E. Let F be the fixed field of G in E and let α and β be the elements of E corresponding to u and v. These elements clearly have the desired properties.

It follows that to establish the best possible improvement of the present theorem with conditions given in terms of m, n and $\mathrm{ch}(F)$, it suffices to consider only group representations. It is possible that the theorem could be improved by dropping the possibility $p<\min(m, n)$ in (a). Some limitations on possible improvements are given by the following examples for $m=3$ and $n=4$.

EXAMPLE 1. $\mathrm{Ch}(K)=2$. Let $G=A_4$, the alternating group on four symbols. Let V^* be a four dimensional vector space over $GF(2)$ and let G permute a basis, $\{w, x, y, z\}$, in the natural manner. Let $V_0=\{0, w+x+y+z\}$ and let $V=V^*/V_0$. The image of w in V has four conjugates under G and the image of $w+x$ has three conjugates. The sum of these elements has four conjugates.

EXAMPLE 2. $\mathrm{Ch}(K)=3$. Let V be a four dimensional vector-space over $K=GF(3)$, with basis $\{w, x, y, z\}$. Let G be the group generated by the elements ρ, σ, $\tau\in\mathrm{GL}(V)$ whose matrices are

$$\rho=\begin{bmatrix}1&1&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix},\quad \sigma=\begin{bmatrix}1&0&0&0\\0&-1&0&0\\0&1&1&0\\0&1&0&1\end{bmatrix},\quad \tau=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}.$$

Then G is the direct product of the subgroups $\langle\rho, \sigma\rangle$ of order 6 and $\langle\tau\rangle$ of order 2. The orbit of w under G is $\{w, w+x, w-x\}$ and the orbit of y under G is $\{y, y+x, z, z+x\}$. However, the orbit of $w+y$ is $\{w+y, w+y+x, w+y-x, w+z, w+z+x, w+z-x\}$, which has six elements.

REFERENCE

1. I. Kaplansky, *Fields and rings*, Univ. of Chicago Press, Chicago, 1969.

UNIVERSITY OF CHICAGO, CHICAGO, ILLINOIS 60637