INDEPENDENCE OF RADICALS

Joseph Lipman, Purdue University

A natural question in elementary field theory is: *if* $p_1, p_2, \ldots, p_n$ *are distinct prime numbers and* $r_1, r_2, \ldots, r_n$ *are any positive integers, is the field extension degree*

$$[Q(\sqrt[r_1]{p_1}, \sqrt[r_2]{p_2}, \ldots, \sqrt[r_n]{p_n}): Q]$$

(Q = the field of rationals) *as large as possible, namely* $r_1 r_2 \cdots r_n$? In other words, are the *obvious* algebraic relations among the $\sqrt[r_i]{p_i}$ the only ones? This was answered in the affirmative by A. S. Besicovitch [J. London Math. Soc. **15** (1940), pp. 3-6]. The special case $r_1 = r_2 = \ldots = r_n = 2$ appeared in this Monthly as advanced problem #4797: *prove that the square roots of the square free integers are linearly independent over the rationals*. (A solution is given in this Monthly, vol. **67** (1960), p. 188).

More generally, let K be any field, let $x_1, x_2, \ldots, x_n$ be *non-zero* elements of K, and let $r_1, r_2, \ldots, r_n$ be positive integers *not divisible by the characteristic of* K. For each $i = 1, 2, \ldots, n$ let $\sqrt[r_i]{x_i}$ be a root of the polynomial $X^{r_i} - x_i$, say in some fixed algebraically closed field $\overline{K}$ containing K. We ask: *under what conditions will it be true that*

$$[K(\sqrt[r_1]{x_1}, \sqrt[r_2]{x_2}, \ldots, \sqrt[r_n]{x_n}) : K] = r_1 r_2 \ldots r_n \qquad \ldots(*)$$

We may observe that (*) does not depend on which root of $X^{r_i} - x_i$ we happen to select $(i = 1, 2, \ldots, n)$. For if (*) holds, then the field $K(\sqrt[r_1]{x_1}, \ldots, \sqrt[r_n]{x_n})$, being separable over K, admits $r_1 r_2 \ldots r_n$ distinct K-isomorphisms into $\overline{K}$; since any such isomorphism is uniquely determined by its effect on the elements $\sqrt[r_i]{x_i}$, and since each $\sqrt[r_i]{x_i}$ has at most r_i K-conjugates, it must be true that for <u>any</u> choice of roots $y_1, y_2, \ldots, y_n$ of the respective polynomials $X^{r_1} - x_1$, $X^{r_2} - x_2, \ldots, X^{r_n} - x_n$, there is a K-isomorphism f with

$$f(\sqrt[r_i]{x_i}) = y_i \qquad (i = 1, 2, \ldots, n)$$

Applying this f to (*), we obtain

$$[K(y_1, y_2, \ldots, y_n) : K] = r_1 r_2 \ldots r_n.$$

In other words, (*) holds for one particular choice of the respective roots $\sqrt[r_i]{x_i}$ if and only if it holds for all possible such choices.

Necessary and sufficient conditions for (*) are given in the following proposition. (For the case $n = 1$, cf. S. Lang, <u>Algebra</u>, Addison-Wesley 1965; chapter VIII, §9).

<u>PROPOSITION.</u> Maintain the preceding notation. In addition, for any integer q, let I_q be the set consisting of all i such that q divides r_i, and let K^q be the set of q^{th} powers in K. Then (*) is true if and only if the following two conditions hold:

(C_1): For any prime number q, if some product

$$\prod_{i \in I_q} x_i^{a_i} \text{ is in } K^q, \text{ then } q \text{ divides each exponent } a_i.$$

(C_2): If -1 is not a square in K, and if

$$\prod_{i \in I_2} x_i^{b_i} \in -4K^4, \text{ then } b_j \text{ is odd for some } j \notin I_4.$$

<u>REMARKS</u>. 1. The Proposition yields as a corollary a generalization of the result mentioned in the opening paragraph: <u>if our field</u> K <u>is the field of quotients of</u> <u>a</u> unique factorization domain R, <u>and if</u> $x_1, x_2, \ldots, x_n$ <u>are distinct prime elements of</u> R, <u>then</u> (*) <u>holds</u>. Indeed, (C_1) is trivially satisfied in this case; and so is (C_2) since a relation $\prod x_i^{b_i} \in -4K^4$ implies at once that all b_i are even, i.e. -1 <u>is</u> a square in K. (We can weaken the hypotheses on the x_i in various ways; it is enough to assume for example that the x_i are pairwise relatively prime, and that for any prime number q, in the factorization of each x_i with $i \in I_q$ some prime element of R occurs with exponent relatively prime to q).

2. In connection with the assumption that the characteristic of K does not divide $r_1 r_2 \ldots r_n$, note that if k is a field of characteristic $p > 0$ and T is an indeterminate, then with $K = k(T)$,

$$[K(\sqrt[p]{T}, \sqrt[p]{T+1}) : K] = p$$

i.e. (*) does not hold, even though (C_1) and (C_2) are satisfied in this case (cf. preceding remark with $x_1 = T$, $x_2 = T + 1$).

3. Because of the multiplicativity of degrees in successive field extensions, it is clear that in proving the necessity of (C_1) for some prime number q, we may replace $K(\sqrt[r_1]{x_1}, \ldots, \sqrt[r_n]{x_n})$ by its subfield

$$K(\{(\sqrt[r_i]{x_i})^{r_i/q}\}_{i \in I_q}) = K(\{\sqrt[q]{x_i}\}_{i \in I_q});$$

in other words we may assume that $r_1 = r_2 = \ldots = r_n = q$. Similarly, in proving the necessity of (C_2), we may assume that $r_i = 4$ if $i \in I_4$ and $r_i = 2$ if $i \notin I_4$. At this point, the proof (of the necessity) becomes quite straightforward; we prefer to illustrate the idea by some examples, and leave the formal argument to the reader.

(A) $[Q(\sqrt[7]{150}, \sqrt[7]{12}, \sqrt[7]{540}) : Q] < 7.7.7$

In this example (C_1) fails, since

$$150^2.12^3.540^3 = (2.3.5^2)^2(2^2.3)^3(2^2.3^3.5)^3$$

$$= 2^{14}.3^{14}.5^7$$

$$= 180^7$$

150 appears here to the power 2, and, modulo 7, the inverse of 2 is 4; after raising the members of the preceding equation to the power 4/7, we obtain

$$\sqrt[7]{150} = 180^4/\ 150(\sqrt[7]{12})^{12}(\sqrt[7]{540})^{12}$$

(for suitable choice of $\sqrt[7]{150}$), so that

$$Q(\sqrt[7]{150}, \sqrt[7]{12}, \sqrt[7]{540}) = Q(\sqrt[7]{12}, \sqrt[7]{540})$$

(B) $[Q(\sqrt[4]{1350}, \sqrt[2]{-210}, \sqrt[4]{-294}) : Q] < 4.2.4.$

In this example (C_1) is found to be satisfied, but (C_2) fails since

$$(1350)^3(-210)^2(-294) = -(2.3^3.5^2)^3(2.3.5.7)^2(2.3.7^2)$$

$$= -4(2^4.3^{12}.5^8.7^4)$$

$$= -4(9450)^4.$$

From this we obtain

$$1350/\sqrt[4]{1350} = \sqrt[4]{-4}\,(9450/\sqrt[2]{-210}\ \sqrt[4]{-294})$$

(for suitable choice of $\sqrt[4]{1350}$), so that

$$Q(\sqrt[4]{1350},\ \sqrt[2]{-210},\ \sqrt[4]{-294}) \subseteq Q(\sqrt[4]{-4})(\sqrt[2]{-210},\ \sqrt[4]{-294}).$$

Since $\sqrt[4]{-4} = \pm 1 \pm i$, with $i^2 = -1$, $[Q(\sqrt[4]{-4}):Q] = 2$ and our assertion follows.

We turn now to the

PROOF OF SUFFICIENCY. The proof is based on simple properties of "Norm" and "Trace". We may assume $r_1 > 1$. Let p be a prime number dividing r_1, and let $x = (\sqrt[r_1]{x_1})^{r_1/p}$; then $x^p = x_1$ and so $p \geq d = [K(x):K]$. Taking Norms from $K(x)$ to K we have

$$x_1^{\,d} = \text{Norm}(x_1) = \text{Norm}(x^p) = (\text{Norm}(x))^p \in K^p.$$

Because of (C_1) (with $q = p$) p divides d; hence $d = p$ (so that $X^p - x_1$ is the minimal polynomial of x, and $\mathrm{Norm}(x) = (-1)^{p+1}x_1$).

Let $(C_1)^{\#}$, $(C_2)^{\#}$, be the conditions (C_1), (C_2), with $K(x)$ in place of K, x in place of x_1, and r_1/p in place of r_1. Assuming that (C_1) and (C_2) hold, we shall show that $(C_1)^{\#}$, $(C_2)^{\#}$ are satisfied; the conclusion then follows by an obvious induction argument.

We first prove $(C_1)^{\#}$. Let q be a prime number, and let y be an element of $K(x)$ such that

$$y^q = x^{a_1} x_2^{a_2} \cdots x_n^{a_n} \qquad \ldots(1)$$

with $a_1 = 0$ if q does not divide r_1/p, and, for $i \geq 2$, $a_i = 0$ if q does not divide r_i (i.e. if $i \notin I_q$). What we have to show is that q divides $a_1, a_2, \ldots, a_n$.

Taking Norms from $K(x)$ to K we get

$$(\mathrm{Norm}(y))^q = (-1)^{(p+1)a_1} x_1^{a_1} x_2^{pa_2} \cdots x_n^{pa_n} \qquad \ldots(2)$$

If either q or p is odd, then (C_1) applied to (2) shows that $q|a_1$ and $q|pa_i$ for $i \geq 2$; hence if $q \neq p$ we are done.

If $q = p \neq 2$, or if $q = p = 2$ and a_1 is even, (C_1) still shows that $q(=p)$ divides a_1, so that $y^p = x_1^{a_1/p} x_2^{a_2} \dots x_n^{a_n} \in K$. <u>This implies that</u> $yx^a \in K$ <u>for some integer</u> a. (Otherwise, for each a, since $K \subsetneq K(yx^a) \subseteq K(x)$, $[K(yx^a): K]$ (which divides p) must equal p, whence the minimal polynomial of yx^a over K is $X^p - (yx^a)^p$, and consequently $\text{Trace}(yx^a) = 0$; since

$$y^{-1} = c_0 + c_1 x + \dots + c_{p-1} x^{p-1} \qquad (c_i \in K)$$

it follows that

$$p = \text{Trace}(1) = \text{Trace}(yy^{-1}) = \sum_{a=0}^{p-1} c_a \, \text{Trace}(yx^a) = 0$$

in contradiction with our assumption that the characteristic of K does not divide r_1). We have therefore, for some a,

$$x_1^{(pa+a_1)/p} x_2^{a_2} \dots x_n^{a_n} = (yx^a)^p \in K^p$$

and so, by (C_1), $p | a_i$ for $i = 2, 3, \dots, n$. We have already stated that $p | a_1$, so (since $p = q$) we are done in this case also.

There remains the case $p = q = 2$ with a_1 odd. By assumption $p = 2 \neq$ characteristic of K. Let g be the automorphism of $K(x)/K$ which sends x to $-x$, and let $\bar{y} = g(y)$.

Applying g to (1), we get $(\bar{y})^2 = -y^2$, whence $\bar{y} = \pm iy$ with $i^2 = -1$. It follows that

$$y = (1 \pm i)w \qquad \text{where} \quad w = \tfrac{1}{2}(y + \bar{y}) \in K$$

so that (squaring (1))

$$x_1^{a_1} x_2^{2a_2} \ldots x_n^{2a_n} = y^4 = -4w^4 \in -4K^4.$$

Note that since $a_1 \neq 0$, we have by assumption $2 | (r_1/2)$, i.e. $1 \in I_4$. We have also assumed for $i \geq 2$ that $a_i = 0$ if $i \notin I_2$; we find therefore that the preceding equation contradicts (C_2). This establishes $(C_1)^{\#}$.

For proving $(C_2)^{\#}$, let $y \in K(x)$ be such that

$$x^{b_1} x_2^{b_2} \ldots x_n^{b_n} = -4y^4 \qquad \ldots(3)$$

with $b_1 = 0$ if 2 does not divide r_1/p and, for $i \geq 2$, $b_i = 0$ if 2 does not divide r_i.

If p is odd we can take Norms to get

$$x_1^{b_1} x_2^{pb_2} \ldots x_n^{pb_n} = -4(-4)^{p-1} (\mathrm{Norm}(y))^4 \in -4K^4$$

and $(C_2)^{\#}$ follows at once from (C_2).

Now suppose $p = 2$. We may assume that -1 is not a square in K (otherwise $(C_2)^{\#}$ is vacuously true); in particular, $-1 \neq 1$. Let $\bar{y} = g(y)$ be as above. Applying g to (3), we get $\bar{y}^4 = \pm y^4$; since -1 is not a square, $\bar{y}^4 = y^4$ (so that b_1 is even); moreover $\bar{y} \neq \pm iy$, and therefore $\bar{y} = \pm y$. Setting $y = c + dx$ ($c, d \in K$), so that $\bar{y} = c - dx$, we conclude (since $-1 \neq 1$) that either $y = c$ or $y = dx$ (according as $\bar{y} = y$ or $\bar{y} = -y$). So (3) says that

$$x_1^{b_1/2} x_2^{b_2} \ldots x_n^{b_n} = -4c^4 \quad \text{or} \quad -4d^4 x_1^2.$$

Now (C_2) shows that <u>either</u> (i): b_j is odd for some $j \notin I_4$, $j > 1$ <u>or</u> (ii): $b_1/2$ is odd and 4 does not divide r_1. If (i) is true, we are through. But (ii) cannot hold, since by assumption $b_1 = 0$ if 2 does not divide $r_1/2$.

This completes the proof.