VICTOR ALEXANDRU
NICOLAE POPESCU

On subfields of $k(x)$

Rendiconti del Seminario Matematico della Università di Padova,
tome 75 (1986), p. 257-273

<http://www.numdam.org/item?id=RSMUP_1986__75__257_0>
On Subfields of \( k(x) \).

VICTOR ALEXANDRU and NICOLAE POPESCU

Let \( k \) be a field and let \( k(x) \) be the field of rational functions of one variable over \( k \). By intermediate field we understand a field \( K \) between \( k \) and \( k(x) \) and such that \( K \neq k \). If \( K \) is an intermediate field, it is well known that \( k(x)/K \) is a finite extension and \( K = k(\alpha) \), \( \alpha \in k(x) \); i.e., \( K \) is also the field of rational functions of the « variable » \( \alpha \) over \( k \) (Lüroth's Theorem; see [2]). A discussion of the lattice of intermediate fields seems to be interesting.

In what follows we consider some problems related to intersections of intermediate fields. A somewhat surprising remark is that for every field \( k \) there exists simple examples of intermediate fields \( k(\alpha_1) \) and \( k(\alpha_2) \) such that \( k(\alpha_1) \cap k(\alpha_2) = k \) (Proposition 1.8). Our Theorem 1.3 shows that the problem of intersections of intermediate fields can be reduced to the case when \( k \) is algebraically closed. Also in Theorem 1.4, we show that separability over intermediate fields is preserved by intersections. Another results (such as Theorem 2.1) refer to index of ramification of a valuation on \( k(x) \) relative to intermediate fields. Particularly we show that the main result of [3] (Section 2, Theorem) is somewhat true in positive characteristic but in a weak formulation (Corollary 2.2 and Remark 2.5). Some results on Galois extensions \( k(x)/k(x) \) are given in Section 3.

In section 4 one shows that some subfields of \( k(x) \) are uniquely represented as a reduced intersection of indecomposable fields.

Indirizzo degli AA.: V. ALEXANDRU: University of Bucharest, Faculty of Mathematics, Str. Academiei nr. 14, 70109 Bucharest, Romania; N. POPESCU: Department of Mathematics, INCREST, Bdul Pacii 220, 79622 Bucharest, Romania.
In what follows we shall utilise standard notations. However we remind these notations for more clarity.

By a valuation on $k(x)$ we shall mean every valuation which is trivial over $k$. These valuations are defined by irreducible polynomials of $k[x]$ and by $1/x$, the prime at infinity (see [2], Ch. I).

If $G$ is a set, $|G|$ means the cardinality of $G$. If $n, m$ are natural numbers, then $[n, m] = \text{l.c.m.}$ and $(n, m) = \text{g.c.d.}$ of $n$ and $m$.

If $L/K$ is a finite extension, then $[L:K]$ means, as usual, the « degree of $L$ over $K$ ».

1. Some general results.

Let $k$ be a field and let $x$ be an element of $k(x)$, $x \notin k$. We shall say that $x$ is a separable element of $k(x)$ if $k(x)/k(x)$ is a separable extension.

**Lemma 1.1.** Let $x = f(x)/g(x)$, where $f(x)$ and $g(x)$ are relatively prime polynomials. The following assertions are equivalent:

- $a$) $x$ is a separable element.
- $b$) $f(x)$ or $g(x)$ is a separable polynomial.
- $c$) The formal derivative $x' = (f'(x)g(x) - f(x)g'(x))/g^2(x)$ is a non-zero element of $k(x)$.

**Proof.** $a) \Rightarrow b)$. Since $k(x)/k(x)$ is a separable extension, the minimal polynomial of $x$ over $k(x)$ is separable. But the minimal polynomial of $x$ over $k(x)$ is $h(y) = f(y) - axg(y)$, and so $h'(y) = f'(y) - ag'(y)$.

The condition $h'(y) \neq 0$ implies $f'(y) \neq 0$ or $g'(y) \neq 0$.

$b) \Rightarrow c)$. If $x' = 0$, then $f'(x)g(x) = f(x)g'(x)$ and so $f(x)/g(x) = f'(x)/g'(x)$. The conditions $\deg f'(x) < \deg f(x)$, $\deg g'(x) < \deg g(x)$ and the irreducibility of $x$, lead us to a contradiction. Hence $b)$ implies $x' \neq 0$.

The other implications are obvious.

In what follows we shall utilise the following result.

**Lemma 1.2.** Let $k$ be a field and $\bar{k}$ the algebraic closure of $k$. Let $f_1(x), \ldots, f_n(x)$ be elements of $k[x]$ and $a_1, \ldots, a_n$ elements (not all 0) of $\bar{k}$, such that $a_1f_1(x) + \ldots + a_nf_n(x) = 0$. Then there exists ele-
The proof is straightforward.

**Theorem 1.3.** Let $k$ be a field and denote by $\overline{k}$ the algebraic closure of $k$. Let $\alpha_1$, $\alpha_2$ be elements of $k(x)$. Then $k(\alpha_1) \cap k(\alpha_2) \neq k$ if and only if $\overline{k}(\alpha_1) \cap \overline{k}(\alpha_2) \neq k$. Moreover, one has $[k(x) : k(\alpha_1) \cap k(\alpha_2)] = [\overline{k}(x) : \overline{k}(\alpha_1) \cap \overline{k}(\alpha_2)]$.

**Proof.** It is clear that $\overline{k}(\alpha_1) \cap \overline{k}(\alpha_2) \neq k$ whereas $k(\alpha_1) \cap k(\alpha_2) \neq k$. Now let us assume that $\overline{k}(\alpha_1) \cap \overline{k}(\alpha_i) \neq \overline{k}$. Let $\alpha_i = u_i(x)/v_i(x)$, $i = 1, 2$, where $u_i(x)$ and $v_i(x)$, respectively $u_2(x)$ and $v_2(x)$ are relatively prime polynomials. It is easy to see that we can assume the following inequalities are accomplished.

\[(2) \quad \deg u_1(x) > \deg v_1(x), \quad \deg u_2(x) > \deg v_2(x).\]

Let $\overline{k}(\alpha_1) \cap \overline{k}(\alpha_2) = \overline{k}(\beta)$. Then one has

$$\beta = f_1(\alpha_1)/g_1(\alpha_1) = f_2(\alpha_2)/g_2(\alpha_2),$$

where

\[
\begin{align*}
f_1(t) &= a_n t^n + \ldots + a_1 t + a_0, \quad a_n \neq 0, \quad n \geq 1, \\
g_1(t) &= b_m t^m + \ldots + b_1 t + b_0, \quad b_m \neq 0, \quad m \geq 0, \\
f_2(t) &= c_r t^r + \ldots + c_1 t + c_0, \quad c_r \neq 0, \quad r \geq 1, \\
g_2(t) &= d_s t^s + \ldots + d_1 t + d_0, \quad d_s \neq 0, \quad s \geq 0,
\end{align*}
\]

are polynomials of $k[t]$, and such that $f_1(t)$ and $g_1(t)$, respectively $f_2(t)$ and $g_2(t)$ are relatively prime. Let us assume that $n \geq m$. Then necessarily $r > s$. Indeed, let $\nu$ be the valuation on $k(x)$ defined by the prime at infinity. Then $\nu(\beta) = (n - m) (\deg v_1(x) - \deg u_1(x)) = (r - s) (\deg v_2(x) - \deg u_2(x))$, and so by (2) and the assumption $n \geq m$ we infer that $r > s$, as claimed.

Moreover, we always can assume that $n > m$. Indeed, if $n < m$ then we change $\beta$ to $1/\beta$. If $n = m$ we can change $\beta$ to $1/(\beta - a)$, where $ab_n = a_n$. Hence in what follows we assume $n > m$ and, as we already proved, we have also $r > s$. 

On subfields of $k(x)$
Now, the element $\beta$ can be written as follows
\[
\beta = \frac{a_0 v_1(x)^n + \ldots + a_n u_1(x)^n}{(b_0 v_1(x)^m + \ldots + b_m u_1(x)^m) v_1(x)^{n-m}} = \frac{c_0 v_2(x)^r + \ldots + c_r u_2(x)^r}{(d_0 v_2(x)^s + \ldots + d_s u_2(x)^s) v_2(x)^{r-s}}
\]

and according to hypothesis (the polynomials $u_i(x)$, $v_i(x)$, $i = 1, 2$ and $f_i(t)$, $g_i(t)$, $i = 1, 2$, are relatively prime in pairs) one check that
\[
\begin{align*}
(a_0 v_1(x)^n + \ldots + a_n u_1(x)^n) &= c_0 v_2(x)^r + \ldots + c_r u_2(x)^r, \\
(b_0 v_1(x)^m + \ldots + b_m u_1(x)^m) v_1(x)^{n-m} &= (d_0 v_2(x)^s + \ldots + d_s u_2(x)^s) v_2(x)^{r-s}.
\end{align*}
\]

Then, according to Lemma 1.2, there exist elements $a'_0, \ldots, a'_n, c'_0, \ldots, c'_r$ in $k$, not all 0, such that
\[
a'_0 v_1(x)^n + \ldots + a'_n u_1(x)^n = c'_0 v_2(x)^r + \ldots + c'_r u_2(x)^r
\]

and such that $a'_n \neq 0$. But then necessarily $c'_r \neq 0$, since the degree of the polynomial in the left member of (4) is $n \deg u_1(x) = r \deg u_2(x)$ (see (2) and (3)). In the same manner we obtain that there exist elements $b'_0, \ldots, b'_m, d'_0, \ldots, d'_s$ in $k$, not all 0, such that
\[
(b'_0 v_1(x)^m + \ldots + b'_m u_1(x)^m) v_1(x)^{n-m} = (d'_0 v_2(x)^s + \ldots + d'_s u_2(x)^s) v_2(x)^{r-s}
\]

and such that $b'_m \neq 0 \neq d'_s$.

Furthermore, according to (4) and (5) we infer:
\[
\alpha = \frac{a'_0 + \ldots + a'_n x_1^n}{b'_0 + \ldots + b'_m x_1^m} = \frac{c'_0 + \ldots + c'_r x_2^r}{d'_0 + \ldots + d'_s x_2^s}.
\]

The hypotheses $n > m$, $r > s$ and also $a'_n \neq 0 \neq c'_r$, $b'_m \neq 0 \neq d'_s$ show that $\alpha$ is an element of $k(x)$ and $\alpha \notin k$. Since $\alpha \in k(x_1) \cap k(x_2)$ we see that $k(x_1) \cap k(x_2) \neq k$. Now it is easy to see that one has:
\[
[k(x) : k(\alpha_1)] \leq [k(x) : k(\beta)] \leq [k(x) : k(\alpha)]
\]

and so $[k(x) : k(\alpha)] = [k(x) : k(\alpha_1)]$. But then $[k(x) : k(\alpha_1) \cap k(\alpha_2)] \leq [k(x) : k(\alpha)] = [k(x) : k(\alpha_1)] \cap
Hence finally

\[ k(x) : k(\alpha_1) \cap k(\alpha_2) = \left[ \bar{k}(x) : \bar{k}(\alpha_1) \cap \bar{k}(\alpha_2) \right]. \]

**Theorem 1.4.** Let \( k \) be a field and let \( \alpha_1, \alpha_2, \alpha_3 \in k(x) \) be such that \( k(\alpha_1) \cap k(\alpha_2) = k(\alpha_3) \neq k \). Then \( \alpha_1 \) and \( \alpha_2 \) are separable elements if and only if \( \alpha_3 \) is a separable element.

**Proof.** It is enough to show that \( \alpha_1 \) and \( \alpha_2 \) separable imply \( \alpha_3 \) separable. Let:

\[ \alpha_3 = \frac{f_1(\alpha_1)|g_1(\alpha_1) = f_2(\alpha_2)|g_2(\alpha_2)}{g_1(\alpha_1)} \]

where \( f_1(y) \) and \( g_1(y) \), respectively \( f_2(y) \) and \( g_2(y) \) are relatively prime polynomials of \( k[y] \). For the moment let us assume that \( k \) is a perfect field. If \( \alpha_3 \) is not separable, then one has (see Lemma 1.1):

\[ \alpha_3' = \frac{f_1'(\alpha_1)g_1(\alpha_1) - f_1(\alpha_1)g_1'(\alpha_1)}{g_1(\alpha_1)} \alpha_1' = 0. \]

Because \( \alpha_3' \neq 0 \), by hypothesis, one sees that

(6) \[ f_1'(\alpha_1)g_1(\alpha_1) = f_1(\alpha_1)g_1'(\alpha_1). \]

If \( g_1'(\alpha_1) \neq 0 \), then \( f_1(\alpha_1)|g_1(\alpha_1) = f_3'(\alpha_1)|g_3'(\alpha_1) \), a contradiction because \( \deg f_1'(y) < \deg f_1(y), \deg g_1'(y) < \deg g_1(y) \), and \( f_1(y), g_1(y) \) are relatively prime. Hence (6) imply \( f_1'(\alpha_1) = g_1'(\alpha_1) = 0 \) and so \( \alpha_3 = (\bar{f}_1(\alpha_1))^p, g_1(\alpha_1) = (\bar{g}_1(\alpha_1))^p \), \( p \) is the characteristic of \( k \), \( k \) being a perfect field. In the same manner one sees that \( f_2(\alpha_2) = (\bar{f}_2(\alpha_2))^p, g_2(\alpha_2) = (\bar{g}_2(\alpha_2))^p \) and so

\[ \alpha_3 = \left( \frac{\bar{f}_1(\alpha_1)}{\bar{g}_1(\alpha_1)} \right)^p = \left( \frac{\bar{f}_2(\alpha_2)}{\bar{g}_2(\alpha_2)} \right)^p. \]

Let us denote \( \bar{\alpha}_3 = \bar{f}_1(\alpha_1)/\bar{g}_1(\alpha_1) \). Then \( \bar{\alpha}_3 \in k(\alpha_1) \cap k(\alpha_1) \), and obviously \( [k(x) : k(\alpha_3)] > [k(x) : k(\bar{\alpha}_3)] \), a contradiction. Therefore \( \alpha_3' \neq 0 \) and so \( \alpha_3 \) is separable (Lemma 1.1).

Now let us assume that \( k \) is not necessarily perfect, and let \( \bar{k} \) be the algebraic closure of \( k \). Since \( k(\alpha_1) \cap k(\alpha_2) = k(\alpha_3) \neq k \), it follows that \( \bar{k}(\alpha_1) \cap \bar{k}(\alpha_2) = \bar{k}(\beta) \neq \bar{k} \), and \( \beta \) is a separable element. But
according to Theorem 1.3, one sees that $\bar{k}(\beta) = \bar{k}(x_3)$ and so $x_3$ is also a separable element, as claimed.

**COROLLARY 1.5.** Let $k$ be a field and let $x_1, x_2, x_3$ be elements of $k(x)$ such that $k(x_1) \cap k(x_2) = k(x_3) \neq k$. Let us assume that the extensions $k(x)/k(x_i), i = 1, 2$ have the same degree of inseparability, namely $p^s$. Then the degree of inseparability of the extension $k(x)/k(x_3)$ is also $p^s$.

**PROOF.** Let $x_1 = f_1(x)/g_1(x)$, where $f_1(x), g_1(x)$ are relatively prime polynomials. The minimal polynomial of $x$ relative to $k(x_3)$ is $h(t) = f_1(t) - x_1g_1(t) \in k(x_3)[t]$. Since the degree of inseparability of $k(x)/k(x_1)$ is $p^s$, we have $h(t) = \bar{h}(t')$, where $\bar{h}(t)$ is an irreducible polynomials of $k(x_3)[t]$. But then $f_1(t) = \bar{f}_1(t'), g_1(t) = \bar{g}_1(t')$. Hence one has: $x_1 = \bar{f}_1(x')/\bar{g}_1(x')$. In the same way we see that $x_2 = \bar{f}_2(x')/\bar{g}_2(x')$. The extensions $k(x_3)/k(x_1)$ and $k(x_3)/k(x_2)$ are separable by hypothesis; according to Theorem 1.4, the extension $k(x'/x_3)$ is also separable. Hence the degree of inseparability of the extension $k(x)/k(x_3)$ is also $p^s$, as claimed.

**REMARK 1.6.** Utilising the same idea as in the proof of Theorem 1.4, one can prove the following result: "Let $k$ be a field and let $x_1, x_2, x_3 \in k(x)$, be such that $k(x_1) \cap k(x_2) = k(x_3) \neq k$. Let $p^{s_i}$ be the degree of inseparability of the extension $k(x)/k(x_i), i = 1, 2$. Then the degree of inseparability of the extension $k(x)/k(x_3)$ is $\max(p^{s_1}, p^{s_2})$.

**REMARK 1.7.** Let $\bar{k}$ be the algebraic closure of $k$. In ([3], Sect. 2, Proposition) is proves that if $f_1(x), f_2(x)$ are polynomials over $k$ such that $\bar{k}(f_1) \cap \bar{k}(f_2) \neq \bar{k}$ and $k$ is an infinite field, then $k(f_1) \cap k(f_2) \neq k$. Now according to Theorem 1.2, this result follows without any hypothesis on $k$.

At the end of this section we give the following result: (see [2], Added in Proof).

**PROPOSITION 1.8.** Let $k$ be a field of characteristic $p > 0$. Let $n$ be a natural number such that $n > p$ and $(n, p) = 1$. Then $k(x^n) \cap k(x^n + x^p) = k$.

**PROOF.** According to Theorem 1.3 we can assume that $k$ is perfect. Let us assume that $k(x^n) \cap k(x^n + x^p) \neq k$. This means (see [3], Lemma 2) that there exist two polynomials $f(t), g(t) \in k[t]$ such that $f(x^n) = g(x^n + x^p)$ and $f$ and $g$ have minimal degree $> 1$ with this
property. Now passing to derivatives one has:

\[ nx^{n-1}f'(x^n) = nx^{n-1}g'(x^n + x^p) \]

and so \( f'(x^n) = g'(x^n + x^p) \), since \((n, p) = 1\). Let us remark that the polynomial \( g(t) \) does not contain the terms of degree 1 (since in this case \( g(x^n + x^p) \) contains \( x^p \) and \( f(x^n) \) does not contain \( x^p \)). Thus, by (7) one check that \( f'(t) = g'(t) = 0 \) (otherwise the minimality of the degree of \( f(t) \) is violated). Therefore \( f\) and \( g \) are \( p \)-powers in \( k[t] \), and also the minimality of the degree of \( f(t) \) is violated. The contradiction obtained shows that \( k(x^n) \cap k(x^n + x^p) = k \), as claimed.

2. Remarks on valuations.

**Theorem 2.1.** Let \( k \) be an algebraically closed field. Let \( k(\alpha_i), i = 1, 2, 3, \) be intermediate subfields of \( k(x) \) such that \( k(\alpha_3) \cap k(\alpha_1) \subseteq k(\alpha_2) \). Let \( v \) be a valuation on \( k(x) \); denote by \( v_i \) the restriction of \( v \) to \( k(x_i) \) and let \( e_i \) be the ramification index of \( v \) relative to \( v_i \), \( i = 1, 2, 3 \). Denote by \( p \) the characteristic of \( k \). Then:

\[ e_3 = \begin{cases} [e_1, e_2] & \text{if } p = 0 \\ p^{e}[e_1, e_2], & \text{if } p > 0 \end{cases} \]

**Proof.** Case 1. Assume that \( \alpha_1 \) and \( \alpha_2 \) are separable elements. Then, according to Theorem 1.4 \( \alpha_3 \) is also a separable element. Let \( K \) be the completion of \( k(x) \) relative to the valuation \( v \) (see [2], Ch. 3), and let \( K_i \) be the closure of \( k(\alpha_i) \) into \( K \). It is easy to see that \( K_i \) is in fact isomorphic to the completion of \( k(\alpha_i) \) relative to the valuation \( v_i \), \( i = 1, 2, 3 \). Also it is easy to check that \( K/K_3 \) is separable. Let \( L \) be a finite extension of \( K \) which is Galois over \( K_3 \). Denote \( G = \text{Gal}(L/K_3) \) and \( G_i = \text{Gal}(L/K_i), \ i = 1, 2 \). From the general theory of ramification groups (see [5], ch. IV) one knows that \( G \) is the semi-direct product between a \( p \)-group \( H \) and a cyclic group \( \bar{G} \), such that \(|\bar{G}|, p \) = 1; moreover, \( H \) is a normal subgroup of \( G \). Let us write \( G = H \bar{G} \). In the same way we see that \( G_i = H_i \bar{G}_i, \ i = 1, 2, \) i.e. \( G_i \) is the semidirect product between a \( p \)-group \( H_i \) and a cyclic group \( \bar{G}_i \) whose order is prime to \( p \). Now, one has \( H_i \subseteq H, \ i = 1, 2, \) since \( H \) is the unique \( p \)-Sylow subgroup of \( G \). Let \( \varphi: G \to G/H \cong \bar{G} \) be the
canonical morphism. Since \( K_1 \cap K_2 = K_3 \), one sees that \( G_1 \) and \( G_2 \) generate \( G \), and so \( \varphi(G_1) \simeq \bar{G}_1 \) and \( \varphi(G_2) \simeq \bar{G}_2 \) generate \( G/H \simeq \bar{G} \).

Now, since \( \bar{G} \) is cyclic, one sees that \( |\bar{G}| = [\varphi(G_1)], |\varphi(G_2)| = [\bar{G}_1], |\bar{G}_2| \) and so \( |G| = |H| \cdot |\bar{G}| = |H||\bar{G}_1|, |\bar{G}_2| = [H||\bar{G}_1], |H||\bar{G}_2|] \). Furthermore, since \( H \subset H \), one sees that \( |H| = |H||t_i| \), where \( t_i \) is a power of \( p \); hence

\[
|G| = |H||\bar{G}_1|, |H||\bar{G}_2| = [t_1|H_1||\bar{G}_1|, t_2|H_2||\bar{G}_2] = [t_1|G_1|, t_2|G_2|].
\]

On the other hand, one has \( |G| = [L:K_3] = [L:K][K:K_3] = [L:K]e_3 \), and also, \( |G_i| = [L:K]e_i \), \( i = 1, 2 \). Therefore one has \( |G| = [L:K]e_3 = [t_1|G_1|, t_2|G_2| = [t_1[L:K]e_1, t_2[L:K]e_2] = [L:K]t_1e_1, t_2e_2 \), and so \( e_3 = [t_1e_1, t_2e_2] \). Now, since \( t_1 \) and \( t_2 \) are powers of \( p \), we get that \( e_3 = p^s(e_1, e_2) \), as claimed.

**Case 2.** Let us assume that \( \alpha_i \) are not separable elements, but the extensions \( k(x)/k(\alpha_i) \), \( i = 1, 2 \), have the same degree of inseparability, namely \( p^s \). Then \( k(x^{p^s})/k(\alpha_i) \), \( i = 1, 2 \) are separable extensions and so the proof can be reduced to Case 1.

**Case 3.** \( \alpha_1 \) and \( \alpha_2 \) are not separable elements of \( k(x) \) and the degrees of inseparability \( p^s, p^{s_1} \), of \( k(X)/k(\alpha_1), k(x)/k(\alpha_2) \) are not equal. Let us assume that \( e_1 < e_2 \). If we change \( x \) to \( x^{p^s} \), we can assume that \( \alpha_1 \) is separable and \( \alpha_2 \) has degree of inseparability \( p^s, s > 1 \). Since \( k \) is perfect, one has \( \alpha_2 = \beta^{p^s} \). Now,

\[
\alpha_3 = A(\alpha_1)/B(\alpha_1) = C(\alpha_2)/D(\alpha_2)
\]

where \( A(t) \) and \( B(t) \), respectively \( C(t) \) and \( D(t) \) are relatively prime polynomials of \( k[t] \). Hence, passing to derivatives, one has:

\[
\alpha'_3 = \frac{A'(\alpha_1)B(\alpha_1) - A(\alpha_1)B'(\alpha_1)}{B(\alpha_1)^2} \alpha'_1 = \frac{C'(\alpha_2)D(\alpha_2) - C(\alpha_2)D'(\alpha_2)}{D(\alpha_2)^2} \alpha'_2 = 0
\]

and so \( A'(\alpha_1)B(\alpha_1) - A(\alpha_1)B'(\alpha_1) = 0 \), since \( \alpha'_1 \neq 0 \).

This means that \( A'(\alpha_1) = B'(\alpha_1) = 0 \) (see the proof of Lemma 1.1), and so \( A(\alpha_1) = (A(\alpha_1))^p \) and \( B(\alpha_1) = (B(\alpha_1))^p \). By recurrence it follows that \( A(\alpha_1) = (\bar{A}(\alpha_1))^{p^s} \) and \( B(\alpha_1) = (\bar{B}(\alpha_1))^{p^s} \). Therefore one obtains:

\[
\alpha_3 = \frac{A(\alpha_1)}{B(\alpha_1)} = \frac{(\bar{A}(\alpha_1))^{p^s}}{(\bar{B}(\alpha_1))^{p^s}} = \frac{C(\alpha_2)}{D(\alpha_2)} = \frac{C(\beta^{p^s})}{D(\beta^{p^s})} = \left( \frac{\bar{C}(\beta^{p^s})}{\bar{D}(\beta^{p^s})} \right)^{p^s}.
\]
Denote
\[ \beta_3 = \frac{\mathcal{A}(\alpha_1)}{B(\alpha_1)} = \frac{\mathcal{C}(\beta_3)}{D(\beta_3)}. \]

Then \( \alpha_1 \) and \( \beta_1 \) are separable elements and so if we denote by \( \bar{e}_2 \) resp. \( \bar{e}_3 \) ramification index of \( v \) relative to \( k(\beta_2) \) resp. \( k(\beta_3) \) respectively, then by case 1 one has \( \bar{e}_3 = p^s[\bar{e}_1, \bar{e}_2] \).

Now we remark that \( k(x)/k(x^p) \) is a purely inseparable extension and, for every valuation \( v \) on \( k(x) \), the ramification index relative to \( k(x^p) \) is just \( p^s \). Therefore one has \( e_3 = \bar{e}_3 p^s \) and \( e_2 = \bar{e}_2 p^s \), and so \( \bar{e}_3 = p^s[\bar{e}_1, \bar{e}_2] = p^s[p^s e_1, p^s \bar{e}_2] = p^s[p^s e_1, e_2] \). Finally, we remark that \( [p^s e_1, e_2] = p^s[\bar{e}_1, e_2] \), where \( 0 < s' < s \), and so \( e_3 = p^s[p^s e_1, e_2] = p^{s+s'}[e_1, e_2] = p^s[e_1, e_2] \). The proof is complete.

**Corollary 2.2.** Let \( k \) be a field of characteristic \( p \) and let \( k(\alpha_i), i = 1, 2, 3, \) be intermediate fields such that \( k(\alpha_1) \cap k(\alpha_2) = k(\alpha_3) \). Let \( v \) be a valuation on \( k(x) \) and let \( e_i \) be the ramification index of \( v \) relative to \( k(\alpha_i), i = 1, 2, 3. \) Then \( e_3 = [e_1, e_2] \) if \( p = 0 \), and \( e_3 = p^s[e_1, e_2] \) with \( e > 0 \), if \( p > 0 \).

**Proof.** Let \( \bar{k} \) be the algebraic closure of \( k \) and let \( \bar{v} \) be a valuation of \( \bar{k}(x) \) which extend \( v \). Let \( v_i \) (resp. \( \bar{v}_i \)) be the restriction of \( v \) (resp. of \( \bar{v} \)) to \( k(\alpha_i) \) (resp to \( \bar{k}(\alpha_i) \)). Let \( e_i \) be the ramification index of \( \bar{v} \) relative to \( v_i \), \( p^s \) the ramification index of \( \bar{v} \) relative to \( v \) and \( p^s \) the ramification index of \( \bar{v} \) relative to \( v_i \), \( i = 1, 2, 3 \). Then one has \( \bar{e}_i = e_i p^s, i = 1, 2, 3 \) and so the natural numbers \( e_i \) and \( \bar{e}_i \) have the same \( p \)-regular parts (i.e. the greatest divisor which is relatively prime to \( p \)). According to Theorem 2.1, one sees that \( \bar{e}_3 = p^s[\bar{e}_1, \bar{e}_2] \), and so the \( p \)-regular part of \( e_3 \) is in fact the l.c.m. of \( p \)-regular parts of \( e_1 \) and \( e_2 \). Now, since \( e_1|e_3 \) and \( e_2|e_3 \), one sees that \( e_3 = h[e_1, e_2] \) and necessarily \( h \) is of the form \( p^s \), as claimed.

**Corollary 2.3.** The notations and hypotheses are as in Corollary 2.2. Let \( k(\alpha_4) \) be the subfield of \( k(x) \) generated by \( k(\alpha_1) \) and \( k(\alpha_2) \). Denote by \( e_4 \) the ramification index of \( v \) relative to \( k(\alpha_4) \). If \( e_3 \) is relatively prime to \( p \), then \( e_4 = (e_1, e_4) \).

**Proof.** The notations are as in the proof of Theorem 2.1. The extensions \( K/K_2 \) is tamely ramified, and so is cyclic, because \( k \) may be assumed algebraically closed. Therefore \( G_1 \) and \( G_2 \) are subgroups of a cyclic group. It is easy to see that \( \text{Gal}(K/K_4) = G_1 \cap G_2 \), and so \( |G_1 \cap G_2| = e_4 = (|G_1|, |G_2|) = (e_1, e_4) \).
**COROLLARY 2.4. ([3], Section 2).** Let \( k \) be a field of characteristic 0 and let \( \alpha_1, \alpha_2, \alpha_3 \) be polynomials in \( k[x] \) such that \( k(\alpha_1) \cap k(\alpha_2) = k(\alpha_3) \not= k \). Then \( \deg \alpha_1 = [\deg \alpha_1, \deg \alpha_2] \).

The proof follows according to Corollary 2.2, considering the valuation on \( k(x) \) associated to the prime at infinity.

**REMARK 2.5.** Let \( k \) be a field of characteristic 3 and let \( \alpha_1 = 2x^2 + x; \alpha_2 = 2x^2 + 2x \). Then \( k(\alpha_1) \cap k(\alpha_2) = k(\alpha_3) \) where \( \alpha_3 = 2x^2(x^2 + 2)^2 \).

Indeed, \( k(x)/k(\alpha_i) \) is a Galois extension whose Galois group is \( G_i = \{1, \sigma_i\}, \ i = 1, 2, \) where \( \sigma_1(x) = 2x + 1, \sigma_2(x) = 2x + 2 \). The subgroup \( G \) of \( \text{Aut}(k(x)) \) generated by \( G_1 \) and \( G_2 \) is actually isomorphic to the symmetric group \( \Sigma_3 \) (in fact, \( G \) has as elements \( 1, \sigma_1, \sigma_2, \sigma_1\sigma_2, \sigma_2\sigma_1, \sigma_1\sigma_2\sigma_1 \)) and so is a group with 6 elements. This shows that in Theorem 2.1, the factor \( p^a \) does not be generally dropped.

### 3. Galois polynomials.

Let \( k \) be a field and let \( \alpha \in k(x) \). We shall say that \( \alpha \) is a **Galois element** if \( k(x)/k(\alpha) \) is a Galois extension.

**THEOREM 3.1.** Let \( f(x) \) be a Galois polynomial of \( k(x) \) such that \( \deg f(x) \) and \( \text{char } k \) are relatively prime. Then the extension \( k(x)/k(f) \) is cyclic, i.e. \( \text{Gal}(k(x)/k(f)) \) is a cyclic group.

In proving this result, we shall use the following Lemma:

**LEMMA 3.2.** Let \( G \) be a finite group. The following assertions are equivalent:

1) \( G \) is a cyclic group;

2) if \( H_1, H_2 \) are subgroups of \( G \), then \( |H_1 \cap H_2| = (|H_1|, |H_2|) \).

**PROOF of the LEMMA.** Since implication 1) \( \Rightarrow \) 2) is obvious, we shall prove only the reverse implication 2) \( \Rightarrow \) 1). We shall use mathematical induction, relative to \( |G| \).

Let \( p \) be the smallest prime number which divides \( |G| \), and let \( g \in G \) be such that \( g^p = 1 \), i.e. \( \text{ord } g = p \). Then, for all \( a \in G \), \( \text{ord } (aga^{-1}) = p \) and so, by hypothesis \( (g) \cap (aga^{-1}) = (g) = (aga^{-1}) \). This means that every element of \( G \) conjugate to \( g \) belongs to \( (g) \), and so \( t \), the number of elements of \( G \), which are conjugate to \( g \), is at most \( p - 1 \). Since \( t/|G| \), it follows that \( t = 1 \), and so \( C(g) \), the
centralizer of $g$, is necessarily $G$, so that $g$ is in the center of $G$. Let $\tilde{G} = G/\langle g \rangle$. Since every subgroup of $\tilde{G}$ is of the form $\tilde{H} = H/\langle g \rangle$, where $H$ is a subgroup of $G$ which contains $g$, it follows that $\tilde{G}$ satifies also the hypothesis $b)$, and so it is cyclic. Now let $h \in G$ be such that $h\tilde{g}$, its image in $\tilde{G}$, is a generator of $\tilde{G}$. Then one has $\text{ord}(h) = |\tilde{G}|/p$, or $\text{ord}(h) = |G|$. In the first case, if $(p, \text{ord}(h)) = 1$, it follows that $hg$ is a generator of $G$; if $p$ divides $\text{ord}(h)$, then $(g) \subset (h)$, by hypothesis, and so $\text{ord}(h) > \text{ord}(\tilde{h})$, a contradiction. Hence $G$ is a cyclic group as claimed.

Now, we are able to give the proof of Theorem 3.1.

According to ([6], Theorem 14) if $K$ is an intermediate field, $k(f) \subset K \subset k(x)$, then $K = k(g)$, where $g$ is a polynomial in $x$. If $K_1, K_2$ are two intermediate fields, then $K_1 = k(f_i)$, and so if $G_i = \text{Gal}(k(x)/k(f_i))$, then $|G_i| = \text{deg} f_i(x)$, $i = 1, 2$. Let $K$ be the subfield of $k(x)$ invariate by $G_1 \cap G_2$. One has $K = k(g)$, where $\text{deg} g(x) = \text{deg} f_1(x), \text{deg} f_2(x)$ (see Theorem 2.3 and Corollary 2.3), so that

$$|G_1 \cap G_2| = \text{deg} g(x) = (\text{deg} f_1(x), \text{deg} f_2(x)) = (|G_1|, |G_2|).$$

Finally, according to Lemma 3.2 one sees that $G$ is cyclic, q.e.d.

Remark 2.5 shows that Theorem 3.1 is not generally valid without the assumption that $\text{deg}(f)$ and $\text{char} k$ are relatively prime numbers.

Remark 3.3. The above result allows us to describe all polynomials of $k(x)$ which are Galois. They are invariant under affine automorphisms of $k(x)$ associated to matrices

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \quad a \neq 1$$

where $a$ is a root of unity.

4. Remarks on structure of some subfields of $k(x)$.

Let $k$ be a field and denote by $p$ the characteristics of $k$. Let $f(x)$ be a polynomial such that $(\text{deg} f, p) = 1$, in case $p \neq 0$. If $k(f) \subset K \subset k(x)$ is an intermediate subfield, then, according to Noether's Theorem (see [6], Theorem 14) one sees that $K = k(g)$ where $g(x)$ is a polynomial. Let $k(f) \subset k(f_i) \subset k(x)$, $i = 1, 2$. According to Corollary 2.2 and Corollary 2.3 it follows:
(A) \( \deg f_1 \mid \deg f_2 \), if and only if \( k(f_2) \subseteq k(f_1) \). Particularly, \( k(f_1) = k(f_2) \) if and only if \( \deg f_1 = \deg f_2 \).

(B) \( (\deg f_1, \deg f_2) \neq 1 \) if and only if \( k(f_1, f_2) \neq k(x) \). Particularly, \( k(f_1, f_2) = k(x) \) if and only if \( (\deg f_1, \deg f_2) = 1 \).

A subfield \( K \) of \( k(x) \), \( K \neq k \) is called indecomposable if it is an indecomposable element in the lattice of intermediate fields between \( k \) and \( k(x) \), i.e. from \( K = K_1 \cap K_2 \), it follows \( K_1 = K \) or \( K_2 = K \). We shall show that under some conditions a subfield \( K \) of \( k(x) \) is a reduced intersection of indecomposable subfields, in a unique way.

**Theorem 4.1.** Let \( f(x) \) be a nonconstant polynomial such that \( (\deg f(x), p) = 1 \) in case \( p \neq 0 \). Then \( k(f) \) can be represented in a unique way as a reduced intersection of indecomposable subfields of \( k(x) \).

**Proof.** It is easy to see, using induction on \( \deg f \), that \( k(f) \) can be represented as a reduced intersection of indecomposable subfields. In proving that the reduced intersection is also unique we shall utilize induction on \( \deg f \).

When \( \deg f = 1 \), or when \( k(f) \) is indecomposable, the proof is clear. Suppose \( \deg f > 1 \) and assume that the result is valid for all polynomials \( g(x) \) such that \( (\deg g, p) = 1 \) and \( \deg f > \deg g \). Suppose \( k(f) \) is decomposable and let:

\[
k(f) = k(f_1) \cap \ldots \cap k(f_n) = k(g_1) \cap \ldots \cap k(g_s)
\]

be two representations of \( k(f) \) as reduced intersections of indecomposable fields. According to Corollary 2.2 one has:

\[
\deg f = [\deg f_1, \ldots, \deg f_n] = [\deg g_1, \ldots, \deg g_s].
\]

We shall divide the proof in several steps.

I) Assume \( k(f_i), 1 \leq i \leq n \) and \( k(g_j), 1 \leq j \leq s \) are maximal subfield of \( k(x) \). In this case the relation (9) becomes: \( \deg f = \deg f_1 \ldots \deg f_n = \deg g_1 \ldots \deg g_s \). This means that for every \( i, 1 \leq i \leq n \), there exists \( j, 1 \leq j \leq s \) such that \( (\deg f_i, \deg g_j) \neq 1 \). But then, according to (B), one has \( k(f_i) = k(g_j) \); since both intersections of (8) are reduced, the unicity follows in an obvious manner.

II) Assume \( k(f_i) \) is not a maximal subfield of \( k(x) \). According to (9) we may assume that \( (\deg f_1, \deg g_i) = d > 1 \). Then by (B),
there exists a maximal subfield $L = k(h)$ of $k(x)$ such that $k(f_1, g_1) \subseteq L$, and obviously $k(f_1) \neq L$, since $k(f_1)$ is not maximal, by hypothesis. Then one has:

\[(10) \quad k(f) = k(f_1) \cap (k(f_2) \cap L) \cap \ldots \cap (k(f_n) \cap L) =
\]

\[= k(g_1) \cap (k(g_2) \cap L) \cap \ldots \cap (k(g_s) \cap L).\]

Assert that we can choose $L$ such that the first intersection of the equality (10) give a representation of $k(f)$ as a reduced intersection of subfields of $L$. Two situations may occur:

\begin{enumerate}
  \item[(a)] $(\deg f_1, \deg f_i) = 1$, for all $i, 2 < i < n$. In this case the intersection:
  \[(11) \quad k(f) = k(f_1) \cap (k(f_2) \cap L) \cap \ldots \cap (k(f_n) \cap L)\]
  is reduced. Indeed, if there exists an $i, 2 < i < n$ such that $k(f_i) \cap L$ is superflue in intersection (11), then, since $k(f_i) \subseteq L$, it follows that $k(f_i)$ is superflue in intersection (8), a contradiction.

  If we assume that $k(f_i)$ is superflue in (8), then, according to Corollary 2.2 one has $\deg f = [\deg h, \deg f_2, \ldots, \deg f_s]$. But then, condition (9) and relation $\deg f_1 > \deg h$ ($k(f_1)$ is not maximal) led us to a contradiction.

  \item[(b)] There exists an $i, 2 < i < n$, such that $(\deg f_1, \deg f_i) = d > 1$. (We may assume that $i = 2$). Then according to (9) it follows that, for example, $(d, \deg g_1) > 1$. Thus according to $(B)$, there exists a maximal subfield $L = k(h)$ of $k(x)$ such that $k(f_1, f_2, g_1) \subseteq L$. For that $L$, the intersection (11) is reduced.

  Furthermore, in both situations $a)$ or $b)$ one has:

  \item[(c)] the intersection

  \[(12) \quad k(f) = k(g_1) \cap (k(g_2) \cap L) \cap \ldots \cap (k(g_s) \cap L)\]

  is reduced, or

  \item[(d)] $k(g_1) = L$ and $(\deg g_1, \deg g_j) = 1, 2 < j < 1$. (We observed that in this last case, as int he proof of $a)$ or $b)$, for $j > 2, k(g_j) \cap L$ cannot be dropped, and so the intersection $(k(g_2) \cap L) \cap \ldots \cap (k(g_s) \cap L)$ is reduced).

  We consider each situation separately.
e) Assume conditions a) or b) and c) are satisfied and all terms of reduced intersections (11) and (12) are indecomposable subfields in \( L = k(h) \). But then, according to the induction hypothesis (since \([L : k(f)] < \deg f\), and, as one easily sees, \( f = t(h) \), where \( t(y) \) is a polynomial of \( k[y] \), such that \( \deg t(y) < \deg f(x) \)), for all \( i, 1 < i < n \) there exists a unique \( j, 1 < j < n \) such that \( k(f_i) \cap L = k(g_j) \cap L \). Then, according to (B), Corollary 2.2 and the hypothesis that \( k(f_i), k(g_i) \) are indecomposable subfields, it follows that \( k(f_i) \subseteq L \) if and only if \( k(g_j) \subseteq L \). Hence, in this case, \( k(f_i) = k(g_j) \). If \( k(f_i) \cap L = k(g_j) \cap L \), and if \( k(f_i) \nsubseteq L \), then \( (\deg f_i, \deg h) = 1 \), \( (\deg g_j, \deg h) = 1 \), and according to Corollary 2.2, one has \( \deg f_i = \deg g_j \), i.e. \( k(f_i) = k(g_j) \) (see (B)). Finally it follows that \( n = s \) and (up to a renumerotation) \( k(f_i) = k(g_i) \) \( 1 < i < n \), i.e. the unicity of \( k(f) \) as a reduced intersection of indecomposable subfields is proved.

f) Assume conditions a) or b) and d), are satisfied and all terms of the corresponding reduced intersections:

\[
(13) \quad k(f) = k(f_1) \cap (k(f_2) \cap L) \cap ... \cap (k(f_n) \cap L) = (k(g_2) \cap L) \cap ... \cap (k(f_s) \cap L)
\]

are indecomposable subfields of \( L \).

Now we may utilise again the induction hypothesis, and thus there exists \( j > 2 \) such that \( k(f_j) = k(g_j) \cap L \), a contradiction, because \( k(f_i) \) is indecomposable and \( (\deg g_j, \deg h) = 1 \) by hypothesis.

g) Assume that conditions a) or b) and c) or d) are satisfied and not all terms of (11) or (12) are indecomposable subfields of \( L \). For example, assume that \( k(f_i) \cap L \) is decomposable in \( L \); this means that \( k(f_i) \nsubseteq L \). If \( k(f) \) is strictly included in \( k(f_i) \cap L \) it follows, according to the induction hypothesis, that \( k(f_i) \cap L \) is a reduced intersection of indecomposable subfields and another representation cannot exist, which contradicts the assumption that \( k(f_i) \cap L \) is decomposable in \( L \). The same considerations are valid for \( k(g_i) \cap L \). Hence, if one of the terms of the intersection (11), say \( k(f_2) \cap L \), is not indecomposable in \( L \), then necessarily one has:

\[ g' \quad k(f) = k(f_2) \cap L = k(f_1) \cap k(f_2), \text{ since } k(f_1) \subseteq L. \]

Also, if we assume that one of the terms of intersection (12), say \( k(g_2) \cap L \), is not indecomposable in \( L \), then necessarily one has:
First we shall examine the situation $g')$.

Thus necessarily $k(f_2) \notin L$, because it was assumed that $k(f)$ is decomposable. Let $M$ be a maximal subfield of $k(x)$ which contains $k(f_2)$. If $M = k(f_2)$ then $k(f_2) \cap M = L \cap M$. If $k(f_1) \subseteq M$, then $k(f_1) = L \cap M$, a contradiction, because $L \neq M$ and $k(f_1)$ is indecomposable. If $k(f_1) \notin L$, then $(\deg f_1, \deg m) = 1$, where $M = k(m)$, and so, according to Corollary 2.2, it follows $\deg f_1 = \deg h$ ($L = k(h)$), i.e. $k(f_1)$ is maximal, a contradiction.

Now, let us assume that $k(f_2) \neq M$; then

\begin{equation}
(14) \quad k(f) = k(f_2) \cap (k(f_1) \cap M) = k(f_2) \cap (L \cap M)
\end{equation}

give a representation of $k(f)$ as an intersection of subfields of $M$. We assert that (14) is a reduced intersection. Indeed, if $L \cap M \supseteq k(f_2)$, then it follows $k(f) = k(f_2)$, a contradiction, because $k(f)$ is not indecomposable. If $k(f_2) \supseteq k(f_1) \cap M$, i.e. if $k(f) = k(f_1) \cap M = L \cap M$, then as above we come to the conclusion that $k(f_2) = L$ i.e. $k(f_1)$ is maximal, again a contradiction. Hence (14) is a reduced intersection, as claimed.

Furthermore, we assert that $L \cap M$ and $k(f_1) \cap M$ are idemcomposable subfields of $M$. Now we shall utilise the induction hypothesis, since $[h(x): L \cap M] < [k(x): k(f)] = \deg f$ (because (14) is a reduced intersection). Therefore, again, according to induction hypothesis one has: $L \cap M = k(f_1) \cap M$ and so $L = k(f_1)$; a contradiction. Hence the situation $g'$) is impossible. Now we examine the situation $g''$.

One has $k(f) = k(g_2) \cap L = k(g_2) \cap k(g_1)$, and as in the case $g'$), we come to the situation $k(g_1) = L$, i.e. $k(g_1)$ is a maximal subfield, hence $k(f) = L \cap k(g_2)$. If $k(g_2) = M$ is a maximal subfield, then

$$
k(f) = L \cap M = k(f_1) \cap k(f_2) \cap \ldots \cap k(f_n),
$$

and because $(\deg f_1, \deg m) = 1$, where $k(m) = M$, it follows necessarily $k(f_1) = L$, $k(f_2) = M$, i.e. $k(f_1)$ is a maximal subfield, a contradiction.

Now, if $k(g_2)$ is not a maximal subfield, we come to the case, already examined, with $f_1$ replaced to $g_2$. Hence we deduce that the unicity of representation (8) may be shown inductively out, possible, the case
when one has:

\[ k(f) = k(f_1) \cap M = L \cap k(g_2) \]

where \( M, L \) are maximals, \( k(f_1) \subset L, k(f_1) \) not maximal, \( k(g_2) \subset M, k(g_2) \) not maximal. Let \( M = k(m), L = k(h), m, h \in k[x] \).

In this last situation one has \((\deg f_1, \deg m) = 1 = (\deg g_2, \deg h)\), otherwise \( k(f) \) will be indecomposable (see (B)). It is clear that, then one has \( \deg f_1 = s \deg h, \deg g_2 = s \deg m, \) where \( s > 1 \). Therefore, according to (B) there exists a maximal subfields \( S \) of \( k(x) \) such that \( k(f_1, g_2) \leq S \). But, then,

\[ k(f) = k(g_2) \cap (L \cap S) = k(f_1) \cap (M \cap S). \]

It is easy to see that:

\( h \) both therms in the representation (16) are reduced intersections of indecomposable subfields of \( S \) (because of the induction hypothesis). In this case we utilise induction hypothesis, relative to \([S : k(f)]\), to derive the unicity of (16) and also of (9).

1) \( k(f) = L \cap S \). It follows that \( k(f_1) = L, i.e. k(f_1) \) is maximal; a contradiction.

2) \( k(f) = M \cap S \). It follows that \( k(g_2) = M, \) also a contradiction. The proof is complete.

**Remark 4.2.** Let \( k \) be a field of characteristic 3 and consider the polynomial \( f(x) = 2x^2(x^2 + 2)^2 \). It is easy to see that the field \( k(f) \) cannot be uniquely represented as a reduced intersection of indecomposable subfields of \( k(x) \). Indeed, (see Remark 2.5) \( k(x)/k(f) \) is a Galois extension and so the intermediate subfields are in one-to-one correspondence to subgroups of \( \text{Gal}(k(x)/k(f)) = \Sigma_3 \). Now, in \( \Sigma_3 \) there exist distinct subgroups \( H_1, H_2 \) of order two, and a subgroup \( H_3 \) of order three such that \( H_1 H_3 = H_2 H_3 = \Sigma_3 \). If \( L_i \) is the subfield of \( k(x) \) invariate by \( H_i, i = 1, 2, 3, \) then \( L_1 \cap L_3 = L_2 \cap L_3 = k(f) \) and obviously \( L_1 \neq L_2 \).

**REFERENCES**


On subfields of $k(x)$


