ON HERSTEIN'S THEOREM CONCERNING THREE FIELDS

CARL FAITH[1]

Let $L > K \geqq \Phi$, $L \neq K$, be three fields such that: (1) L/K is not purely inseparable, and (2) L/Φ is transcendental. Then Herstein's theorem [2] asserts the existence of $u \in L$ such that $f(u) \notin K$ for every non-constant polynomial $f(X) \in \Phi[X]$. Thus Herstein's theorem can be given the following equivalent form:

THEOREM (Herstein). *If L, K, and Φ are three fields satisfying* (1) *and* (2), *$L \neq K$, then there exists $u \in L$ which is transcendental over Φ such that $K \cap \Phi[u] = \Phi$, where $\Phi[u]$ is the subring generated by Φ and u.*

The main part of Herstein's proof depends on a lemma of Nagata, Nakayama, and Tsuzuku in valuation theory of fields [*On an existence lemma in valuation theory*, Nagoya Math. Journal, vol. 6 (1953)]; the proof of this lemma in turn requires a knowledge of arithmetic in "algebraic number and function fields". In the present note I present an elementary proof of Herstein's theorem in which only the most basic properties of simple transcendental fields are used. In this development the result for the case $L = \Phi(x)$ is sharpened: then there exists a polynomial $q = q(x) \in \Phi[x]$ not in Φ such that $K \cap \Phi[q] = \Phi$.

Herstein's elementary reduction to the pure transcendental case constitutes a reduction for the theorem as stated above so we can assume that $L = \Phi(x)$. In this case it is known[2] that $K \cap \Phi[x]$ is finitely generated over Φ as a ring, for any intermediate field K. The proposition below gives a new proof and at the same time sharpens this result: *Then $K \cap \Phi[x]$ has a single generator over Φ.*

Received March 22, 1961.

[1] North Atlantic Treaty Organization (U.S.A.) Postdoctoral Fellow in the Mathematical Institute, Heidelberg University, on leave from Pennsylvania State University.

[2] This is the one dimensional solution to Hilbert's Fourteenth Problem. See [4] for Zariski's generalization and solution to the one and two dimensional cases of Hilbert's problem.

PROPOSITION 1. *Let $L=\Phi(x)$ be a simple transcendental field extension, and let $K=\Phi(H/G)$ be any intermediate field*[3] $\neq\Phi$, *where H, $G\in\Phi[x]$, $(H, G)=1$, and $H\notin\Phi$. Then a necessary and sufficient condition that $K\cap\Phi[x]\neq\Phi$ is that $K=\Phi(H)$. Then: $K\cap\Phi[x]=\Phi[H]$, and $G=aH+b$, with a, $b\in\Phi$.*

Proof. Let $P(x)\in\Phi[x]$, $P(x)\notin\Phi$, and assume that

$$P=h(H/G)/g(H/G)\in K, \tag{1}$$

where $h(X)$, $g(X)\in\Phi[X]$, $(h, g)=1$, and X a new indeterminant. It can, and will, be assumed that both $h(X)$ and $g(X)$ have leading coefficient $=1$. First suppose that $g(X)\in\Phi$ (then $g(X)=1$) and write

$$h(X)=X^q\sum_{i=0}^{k}a_iX^i,$$

where $a_0a_k\neq 0$. Then,

$$G^{k+q}P=H^q\sum_{i=0}^{k}a_iG^{k-i}H^i. \tag{2}$$

Since $(H, G)=1$, necessarily $(G, \sum_0^k a_iG^{k-i}H^i)=1$. Since $H(x)\notin\Phi$, $k+q=\deg H(x)\neq 0$. It follows, since G divides the left side but is prime to the right side of (2), that $G\in\Phi$, that is, $G=0\cdot H+b\in\Phi$, $K=\Phi(H)$ as required.

Now assume that $g(X)\notin\Phi$. I am indebted to R. Kiehl for the following neat proof of this case. Let A denote the algebraic closure of Φ, and, over A, factor

$$g(X)=\prod_{j=1}^{m}(X-b_j). \tag{3}$$

Furthermore, over A,

$$h(X)=\prod_{i=1}^{n}(X-a_i) \qquad \text{(or, } h(X)=1.) \tag{4}$$

Hence, by (1) and (3),

$$\prod_{j=1}^{m}(H-b_jG)=G^t\prod_{i=1}^{n}(H-a_iG) \qquad \text{(or, } =G^t), \tag{5}$$

where $t=m-n$ (or, $t=m$). Since $(H, G)=1$, clearly

$$(H-b_1G,\ G)=1, \tag{6}$$

[3] This is Lüroth's theorem [3, p. 126].

and,

$$d_j = (H - b_1 G,\ H - a_j G) = 1. \tag{7}$$

To justify (7), note, (since $(h, g) = 1$) that $a_j \neq b_1$, $j = 1, 2, \ldots m$, and write

$$H - b_1 G = (H - a_j G) + (a_j - b_1)G. \tag{8}$$

From (8) it follows that d_j divides G, whence d_j divides $1 = (H, G)$, that is, $d_j = 1$. Now (5)-(7) show that $H - b_1 G$ divides the left side but is prime (even in the case $h(X) = 1$) to the right side of (5). Thus,

$$H - b_1 G = c_1 \in A. \tag{9}$$

Inspection of the coefficients in (9) reveals that b_1, c_1, $\in \Phi$, and, hence,

$$G = b_1^{-1} H - c_1 b_1^{-1} \tag{10}$$

has the required form; $K = \Phi(H)$.

Finally, since $K = \Phi(H)$, (1) can be rewritten

$$P(x) = h(H)/g(H). \tag{11}$$

The results above, and the form of (10), show, by assuming G in (1) is a constant, that $g(X) \in \Phi$. Thus, $P(x) = h(H) \in \Phi[H]$, whence, $K \cap \Phi[x] \subseteqq \Phi[H]$. The reverse inclusion is trivial, so that the last statement in the proposition is proved.

LEMMA 2. *Let $L = \Phi(x)$ be a simple transcendental field extension, and let $K = \Phi(H)$, where $H = H(x) \in \Phi[x]$ is such that x divides $H(x)$, and $K \cap \Phi[xH] \neq \Phi$. Then, $H(x) = ax^n$, $a \in \Phi$.*

Proof. By Proposition 1, $\Phi[H] \geqq \Phi[xH] \cap K$. Let $f(X) = \sum_0^m a_i X^i$, $g(X) = \sum_0^m b_i X^i$, where m is chosen such that one of a_m, $b_m \neq 0$, be such that $f(xH) = g(H) \in \Phi[xH]$ not in Φ. Then

$$0 = g(H) - f(xH) = \sum_0^m (a_i - b_i x^i) H^i. \tag{1}$$

If q is the smallest integer such that one of a_q, $b_q \neq 0$, then (1) is divisible by H^q, so that

$$0 = \sum_q^m (a_i - b_i x^i) H^{i-q}. \tag{2}$$

From (2) one sees that H divides $(a_q - b_q x^q)$. Since $H \notin \Phi$, $q \neq 0$. Since x divides H, necessarily $a_q = 0$, whence H divides x^q, that is, $H(x) = ax^n$, $a \in \Phi$, $n \leqq q$, as needed.

I am now in a position to complete the proof of Herstein's theorem (in its sharpened form in the pure transcendental case.)

THEOREM 3. *If $L = \Phi(x)$ is a simple transcendental field extension and if K is any intermediate field $\neq L$ such that L/K is not purely inseparable, then there exists $u \in \Phi[x]$ not in Φ such that $K \cap \Phi[u] = \Phi$.*

Proof. If the theorem is denied, then by the proposition, $K = \Phi(H)$ with $H = H(x) \in \Phi[x]$. It can be assumed that x divides $H(x)$. Now $K \cap \Phi[xH] \neq \Phi$, so that $K = \Phi(x^n)$ by the lemma. Let $y = x - 1$, note that $L = \Phi(y)$, that $K = \Phi(x^n - 1)$, and assume that

$$K \cap \Phi[(x-1)(x^n-1)] \neq \Phi,$$

that is, that

$$\Phi((y+1)^n - 1) \cap \Phi[y((y+1)^n - 1)] \neq \Phi.$$

Then, since y divides $(y+1)^n - 1$, one can apply Lemma 2 again to see that

$$(y+1)^n - 1 = y^n,$$

or,

$$(y+1)^n = y^n + 1,$$

which, since $n > 1$, is possible only if Φ has characteristic p, and $n = p^e$. Then $K = \Phi(x^n) = \Phi(x^{p^e})$, so that L/K is purely inseparable, contrary to the hypothesis. This completes the proof.

PROPOSITION 4. *Let $L = \Phi(x)$ be a simple transcendental field extension, and let $P, Q \in \Phi[x]$ be such that $\Phi(P) \cap \Phi(Q) \neq \Phi$.* Then $\Phi[P] \cap \Phi[Q] \neq \Phi$.

Proof. Let (1) $h(P)/g(P) = p(Q)/q(Q)$ be a nonconstant element in $M = \Phi(P) \cap \Phi(Q)$, where $h(X)$, $g(X)$, $p(X)$, $q(X) \in \Phi[X]$, and $(h, g) = (p, q) = 1$. Then, (2) $h(P)q(Q) = p(Q)g(P)$. Since $(q(Q), p(Q)) = (h(P), g(P)) = 1$, it follows that (3) $h(P) = p(Q) \in M$, and (4) $q(Q) = g(P) \in M$, so that, by (1), one of (3) and (4) lies outside of Φ.

THEOREM 5. *Let $L = \Phi(x)$ be a simple transcendeutal field extension, and let K be an intermediate field such that $L \neq K$, and L/K is not purely inseparable.*

Then, if $K=\Phi(F(x))$, *where* $P(x)\in\Phi[x]$, *there exists* $Q(x)\in\Phi[x]$, $Q(x)\notin\Phi$, *such that* $K\cap\Phi(Q)=K\cap\Phi[Q]=\Phi$.

Proof. If $\Phi(Q)\cap K\neq\Phi$, for all Q in $\Phi[x]$ not in Φ, then by the proposition, $\Phi[Q]\cap K\neq\Phi$, for all such Q. But this violates Theorem 3, unless L/K is purely inseparable. But this is ruled out by hypothesis, completing the proof.

In [1] Herstein's method of [2] is employed to show that the element u in the statement of his theorem can be chosen such that

$$K\cap\Phi(u)=K\cap\Phi[u]=\Phi.$$

Theorem 5, then, represents a special case of this more general result. It would be interesting therefore to know if the more general statement also has an elementary proof.

In [1] Herstein's theorem is used in the proof of the following result: If A is a transcendental division algebra over the field Φ, and if B is a subalgebra $\neq A$ such that to each $a\in A$ there corresponds a non-constant polynomial $f_a(x)\in\Phi[x]$ such that $f_a(a)\in B$, then A is a field. A consequence of the present note is that this result now also has an elementary proof.

References

[1] Carl Faith, A structure theory for semialgebraic extensions of division algebras, Journal für die reine und angewandte Mathematik, (1961).

[2] I. N. Herstein, A theorem concerning three fields, Canadian Journal of Mathematics, vol. **7** (1955), 202-203.

[3] B. L. van der Waerden, Algebra I, Vierte Auflage, Berlin-Göttingen-Heidelberg, 1955.

[4] O. Zariski, Interprétation algébrico-géométriques du quatorzième problème de Hilbert, Bull. Sci. Math. vol. **78** (1954), 155-168.

Institute for Advanced Study,
Princeton, N. J.