METAMATHEMATICAL CONSIDERATIONS ON THE RELATIVE IRREDUCIBILITY OF POLYNOMIALS

P. C. GILMORE AND A. ROBINSON

1. Introduction. In this paper, infinite fields K will be discussed which satisfy the following condition:

CONDITION C: for any polynomial $p(t, x)$ in x, coefficients in $K(t)$, t transcendental with respect to K, which has no zeros in $K(t)$, there is a t^* in K for which $p(t^*, x)$ has no zeros in K.

This condition is *a priori* weaker than Franz's necessary and sufficient criterion[1] in the field K. As an illustration of the scope of the metamathematical method of proof in algebra, a metamathematical theorem (2.1) will be established for fields satisfying condition C. By means of the theorem it will be shown that for fields satisfying condition C not only does Hilbert's theorem hold, but also two other theorems, one related to results proven by Dörge **(1)** and the other new. The metamathematical theorem to be established is an extension of a theorem proven by Robinson **(6**, pp. 35–52**)**.

Throughout this paper K will denote an infinite field, t an element transcendental over K, and x will be an indeterminate. We will use the usual notation of square and round brackets when adjoining elements to a field to denote the ring of the polynomials in the adjoined elements and the field of rational functions of the adjoined elements respectively. We will further use for logical notation, variables x, y, z, u, v, x' and y', "$\sim$," "$\wedge$," "$\vee$," and "$\supset$" for negation, conjunction, disjunction and implication respectively, and "(x)" and "$(\exists x)$" for universal and existential quantification respectively.

2. A metamathematical theorem. The language of the first order predicate calculus is assumed given with any number of individual parameters and atomic predicates. For any given field K and any element t transcendental with respect to K, the language $\mathfrak{F}$ is the language of the first order predicate calculus applied in the following way: to each member of K and to t is assigned an individual parameter, and these are the individual parameters of $\mathfrak{F}$; to each subset of K, to each subset of the set $K \times K$ of pairs from K, to each subset of the set $K \times K \times K$ of triples from K, etc., is assigned an atomic predicate, and these are the atomic predicates of $\mathfrak{F}$. Finally the language $\mathfrak{L}$ is defined to be identical with $\mathfrak{F}$ except that it is lacking an individual parameter for t.

Received May 10, 1954; in revised form May 12, 1955. Dr. Gilmore's part of this work was done under a postdoctorate National Research Council Fellowship.

[1] See Franz **(2**, §3**)**. In his paper, Franz considers fields K of the form $K = F(\alpha)$, where F is an infinite field and α is transcendental over F. For finite F, see Inaba **(4)**.

https://doi.org/10.4153/CJM-1955-051-7 Published online by Cambridge University Press

This assignment of parameters and predicates for the languages $\mathfrak{F}$ and $\mathfrak{L}$ will remain fixed for this paper, so that when we speak of a statement of $\mathfrak{L}$ or $\mathfrak{F}$ holding for K or $K(t)$, it is assumed to hold under the given assignment. Then $\mathfrak{K}$ is defined to be the set of all statements of $\mathfrak{L}$ holding for $\mathfrak{K}$; i.e., $\mathfrak{K}$ is the largest set of statements of $\mathfrak{L}$ for which K is a model.

THEOREM 2.1. *For any field K fulfilling condition C, there is an extension S' of $S = K(t)$ which is a model of $\mathfrak{K}$ and for which every member of $S' - S$ is transcendental with respect to S.*

Proof. Let the atomic predicates $E(x, y)$, $S(x, y, z)$ and $P(x, y, z)$ be those of $\mathfrak{F}$ which have been assigned to the following sets respectively: the set of all pairs of members of K with the first member of the pair equal to the second member of the pair, the set of all triples from K with the sum of the first two members equal to the third member, and the set of all triples from K with the product of the first two members equal to the third member. Within $\mathfrak{F}$ can then be expressed any polynomial equation $p(t) = 0$ by using the atomic predicates E, S and P, and by using the individual parameters in F corresponding to the coefficients of the polynomials $p(t)$. Thus using the letter τ as the individual parameter of $\mathfrak{F}$ which has been assigned to the element t transcendental with respect to K, the notation

$$\sum_{i=0}^{m} p_i \tau^i \neq 0$$

can be used as an abbreviation for the full statement in $\mathfrak{F}$ for the polynomial equation of the same form. The following sets of statements from $\mathfrak{F}$ are then defined:

$\mathfrak{S}_1$: the set of all statements of the form

$$\sum_{i=0}^{m} p_i \tau^i \neq 0$$

for all m, and for all sets of individual parameters for which the polynomial $p(t) \in K\,[t]$ with coefficients corresponding to the parameters p_i, is not null.

$\mathfrak{S}_2$: the set of all statements of the form

$$(x)\left(\sum_{i=0}^{m} \sum_{j=0}^{n} q_{ij}\, \tau^i x^j \neq 0\right)$$

for all m and n, and for all sets of individual parameters for which the polynomial $q(t, x) \in K[t, x]$ with coefficients corresponding to the parameters q_{ij} is irreducible in x over $K(t)$, and of degree greater than one in x.

The set $\mathfrak{K} \cup \mathfrak{S}_1 \cup \mathfrak{S}_2$ of statements from $\mathfrak{F}$ is consistent, provided we can show that K is a model for any finite subset of the set. Now, given any finite subset of $\mathfrak{K} \cup \mathfrak{S}_1 \cup \mathfrak{S}_2$, let $p_i(t)$ for $i = 1, \ldots, \mu$ be the polynomials in $K[t]$ used to define the statements from $\mathfrak{S}_1$, and let $q_j(t, x)$ for $j = 1, \ldots, \nu$ be the polynomials in $K[t, x]$ used to define the statements from S_2. Then to show that K is a model for this finite subset of statements, we need only find a suitable $t^* \in K$ to which the parameter τ can be assigned, since the given assignment of parameters and predicates is assumed to be fixed. But then t^* need only be chosen so that $p(t^*, x)$ has no root x in K, where the polynomial $p(t, x)$ is defined to be

$$\prod_{i=1}^{\mu} p_i(t) \prod_{j=1}^{\nu} q_j(t, x).$$

Since all the q_j are irreducible in x, $p(t, x)$ has no roots in $K(t)$, and therefore by condition C there is a $t^* \in K$ for which $p(t^*, x)$ has no root in K.

Since the set $\mathfrak{K} \cup \mathfrak{S}_1 \cup \mathfrak{S}_2$ is consistent, it has a model[2] M. Within $\mathfrak{K}$ will be a set of statements containing no quantifiers or variables but only individual parameters of $\mathfrak{L}$, and expressing all possible algebraic relationships between members of K. All of these statements are valid in the model M so that M must contain a subset K' which is a field isomorphic to K. Further, since M is a model for the set $\mathfrak{S}_1$, M must contain a member t' which is transcendental with respect to K' and therefore must contain a subset $K'(t')$ isomorphic with $K(t)$. Since M is also a model of $\mathfrak{S}_2$, every member of $M - K'(t')$ is transcendental with respect to $K'(t')$. Therefore an extension S' of S can be constructed isomorphic to M and such that every member of $S' - S$ is transcendental with respect to S, establishing the theorem.

3. Applications.

Theorem 2.1 will now be applied to establish several results for fields fulfilling condition C. The principle of our method is to establish that a certain statement of $\mathfrak{L}$ holds in S'. It then follows from 2.1 that the statement holds also in K (see proof of Theorem 3.1), although it may be far more difficult to prove this fact directly.

THEOREM 3.1. *If K fulfils condition C, then for any irreducible polynomial $p(t, x)$ in x with coefficients in $K(t)$ there are infinitely many t^* from K such that $p(t^*, x)$ is irreducible in x over K.*

Proof. Let S and S' be given for K as in Theorem 2.1. We will first show that if a polynomial $p(t, x)$ with coefficients in S is irreducible in S then it is also irreducible in S'. For if $p = p_1 . p_2$, with $p_1, p_2 \in S'[x]$, is a non-trivial factorization of p, then in the algebraic closure T' of S', p_1 and p_2 will split into linear factors. But in the algebraic closure T of S, p will split into linear factors and these factors can be identified with factors of p_1 and p_2 in T'. Hence p_1 and p_2 must split into linear factors in T and must therefore be contained in $T[x]$. But since all members of T are algebraic with respect to S, $T \cap S' = S$, and hence $p_1, p_2 \in S[x]$, giving that p is reducible in S.

For any polynomial $p(t, x)$ in x with coefficients from $K(t)$ there can be defined a predicate $I(z)$ in the language $\mathfrak{L}$ such that for any member k of K,

[2] Compare Robinson **(5)** or Henkin **(3)**.

https://doi.org/10.4153/CJM-1955-051-7 Published online by Cambridge University Press

$I(k)$ expresses that $p(k, x)$ is irreducible in x over K. We can assume that $p(t, x)$ is a polynomial

$$\sum_{i=0}^{n} f_i\,(t)\,x^i,$$

where $f_i(t) \in K[t]$ for $0 \leqslant i \leqslant n$, since a factor $q(t) \in K[t]$ does not affect the irreducibility of $p(t, x)$. Then for any given $k \in K$, the fact that $p(k, x)$ has no factor of degree m in x can be expressed by $I_m(k)$, which is defined to be:

$$(x_0)\ldots(x_m)(y_0)\ldots(y_{n-m})(x_0\,y_0 \neq f_0(k) \vee x_0\,y_1{+}x_1\,y_0 \neq f_1(k) \vee \ldots \vee x_m\,y_{n-m}\,f_n(k))$$

where, for example, $x_0\,y_0 \neq f_0(k)$ is an abbreviation for

$$(z)\left(P(x_0, y_0, z) \supset z \neq \sum_{i=0}^{r} p_i\,k^i\right)$$

assuming $f_0(t)$ to be the polynomial

$$\sum_{i=0}^{r} p_i\,t^i$$

and where the other members of the disjunction are abbreviations for corresponding statements. Then if $I(k)$ is defined to be $I_1(k) \wedge I_2(k) \wedge \ldots \wedge I_{n-1}(k)$, $I(k)$ expresses that $p(k, x)$ for $k \in K$ is irreducible in x over K. Hence to show that there is a t^* in K for which $p(t^*, x)$ is irreducible over K, we need only to show that $(\exists x)I(x)$ is valid in K. Further, in order to show that there are infinitely many t^* in K for which $p(t^*, x)$ is irreducible over K, we need only prove that

$$\text{(I)}\quad (\exists z_1)(\exists z_2)\ldots(\exists z_n)(z_1 \neq z_2 \wedge z_1 \neq z_3 \wedge z_2 \neq z_3 \wedge \ldots \wedge z_{n-1} \neq z_n \wedge I(z_1) \wedge I(z_2) \wedge \ldots \wedge I(z_n))$$

is valid in K for any n.

To show that a statement is valid for K it is only necessary to show that it is valid for S', since if a statement is valid for S' but not valid for K, its negation would be valid for K and therefore a member of $\mathfrak{K}$, contradicting that S' is a model for $\mathfrak{K}$. But $(\exists x)I(x)$ is valid for S' since t is a member of S', and therefore since $p(t, x)$ is irreducible over S it must also be irreducible over S'. Also the statement (I) is valid for S' since not only $p(t, x)$ is irreducible over S but also $p(t{+}k, x)$ for any member k of K. Thus the theorem is established.

This theorem shows that for any field fulfilling condition C, Hilbert's irreducibility theorem can be proven.

In **(1)**, Dörge has proven theorems related to Hilbert's irreducibility theorem as the following theorem is related to Theorem 3.1.

THEOREM 3.2. *If K is an ordered field fulfilling condition C, then for any a and b from K for which $a < b$ and for any irreducible polynomial $p(t, x)$ in x with coefficients in $K(t)$, there exists a t^* in K such that $a < t^* < b$ and such that $p(t^*, x)$ is irreducible in x over K.*

https://doi.org/10.4153/CJM-1955-051-7 Published online by Cambridge University Press

Proof. The order in K defines a set of pairs of K to which there will be assigned a predicate $Q(x, y)$ of $\mathfrak{L}$. Q will appear together with E, S and P in statements in $\mathfrak{K}$ expressing that K is an ordered field. For a given irreducible polynomial $p(t, x)$, $I(z)$ will be defined as in the proof of Theorem 3.1. Then for the present theorem it is sufficient to prove that for any parameters α and β of $\mathfrak{L}$

(II) $$(\exists z)(Q(\alpha, \beta) \supset Q(\alpha, z) \wedge Q(z, \beta) \wedge I(z))$$

is valid for S' (and hence that it is valid for K, by Theorem 2.1).

Because S' is a model of $\mathfrak{K}$, it must be an ordered field under some ordering $\prec$ to which Q is assigned. To show then that (II) is valid for S', it is sufficient to show that for any a and b in K such that $a \prec b$, there is a w in S' which satisfies $I(z)$ and is such that $a \prec w \prec b$. But such a w can always be found, for if $1 \prec t$, put $w = a + (b - a)t^{-1}$; if $0 \prec t \prec 1$, put $w = a + (b - a)t$; if $-1 \prec t \prec 0$, put $w = a + (a - b)t$; and finally, if $t \prec -1$, put $w = a + (b - a)t$. No other cases need be considered since t is transcendental with respect to K and hence neither $E(0, t)$ nor $E(1, t)$ can be valid for S'. In each of these cases it is possible to show from the properties of an ordered field, which S' possesses by virtue of being a model for $\mathfrak{K}$, that $a \prec t \prec b$. Further, since in each case w is transcendental over S, $p(w, x)$ is irreducible over S and therefore irreducible over S' (see proof of Theorem 3.1), showing that w satisfies $I(z)$. This proves the theorem.

As final application, we will prove a theorem for fields K with a valuation ψ in an ordered field W. The valuations considered will be non-trivial and hence the function ψ will be such that (7, p. 325):

3.21 for any k, $\psi(k)$ is an element of W,

3.22 for any $k \neq 0$, $0 < \psi(k)$, and $\psi(0) = 0$,

3.23 for any k and k', $\psi(k.k') = \psi(k).\psi(k')$,

3.24 for any k and k', $\psi(k+k') \leqslant \psi(k) + \psi(k')$,

3.25 there is a k such that $\psi(k) \neq 1$ and $\psi(k) \neq 0$.

The following properties can then be proven:

3.26 for any a, k and k', if $\psi(a) \neq 0$ and $\psi(k) < \psi(k')$, then $\psi(k\cdot a) < \psi(k'\cdot a)$ is true. This property follows from the fact that W is an ordered field, and from 3.23.

3.27 for any k, if $k \neq 0$ then $\psi(k) \neq 0$.

3.28 for any a, k and k', if $\psi(a) = \psi(1)$ and $\psi(k) < \psi(k')$, then $\psi(k\cdot a) < \psi(k')$.

THEOREM 3.3. *If K is a field with a valuation ψ in an ordered field W and K fulfils condition C, then for any a and b from K with $b \neq 0$ and for any irreducible polynomial $p(t, x)$ in x with coefficients in $K(t)$, there exists a t^* in K such that $\psi(a - t^*) < \psi(b)$ and such that $p(t^*, x)$ is irreducible in x over K.*

https://doi.org/10.4153/CJM-1955-051-7 Published online by Cambridge University Press

Proof. Let $E^*(x, y)$ and $Q^*(x, y)$ be the atomic predicates of $\mathfrak{L}$ which have been assigned to the following sets respectively: the set of pairs (a, b) of elements from K such that $\psi(a) = \psi(b)$, and the set of pairs (a, b) such that $\psi(a) < \psi(b)$. Then these predicates will appear in statements in $\mathfrak{K}$. For example, in addition to statements expressing that $E^*(x, y)$ is an equivalence relation, the following statements will appear in $\mathfrak{K}$:

$$(x)(y)(z)(Q^*(x, y) \wedge Q^*(x, z) \supset Q^*(x, z)),$$
$$(x)(y)(Q^*(x, y) \vee Q^*(y, x) \supset E^*(x, y)),$$
$$(x)(y)(Q^*(x, y) \vee Q^*(y, x) \vee E^*(x, y)),$$

together with statements corresponding to properties of the valuation function ψ, such as

3.31 $(x)(\sim E(x, 0) \supset Q^*(0, x)) \wedge (x)(E(x, 0) \supset E^*(x, 0)),$

3.32 $(\exists x)(\sim E^*(x, 0) \wedge \sim E^*(x, 1)),$

3.33 $(x)(y)(z)(u)(v)(Q^*(x,y) \wedge P(x,z,u) \wedge P(y,z,v) \wedge \sim E^*(z,0) \supset Q^*(u,v))$

3.34 $(x)(\sim E(x, 0) \supset \sim E^*(x, 0))$

3.35 $(x)(y)(z)(u)(Q(y, z) \wedge E^*(1, x) \wedge P(x, y, u) \supset Q^*(u, z)),$

where "0" and "1" are the individual parameters of $\mathfrak{L}$ corresponding to the zero and the unit of K.

If S' is the extension of K given by Theorem 2.1, then S' is a model for $\mathfrak{K}$. Hence in S' there must be defined relations corresponding to the atomic predicates E^*, Q^*, S and P. This can be expressed in the following way. The equivalence relation $E^*(x, y)$ will determine equivalence classes in S' for which $\bar{\psi}(a)$ for any member a of S' will denote the equivalence class determined by a. Thus for any a and b of S', $\bar{\psi}(a) = \bar{\psi}(b)$ if and only if $E^*(a, b)$ holds in S'. Further, these equivalence classes can be ordered by the relation corresponding to $Q^*(x, y)$, for we can say that for any a and b of S', $\bar{\psi}(a) < \bar{\psi}(b)$ if and only if $Q^*(a, b)$ holds in S', and this will be a proper ordering of the equivalence classes, by the statements listed above as appearing in K. Lastly, in S' will appear relations corresponding to S and P, and these relations will be the usual addition and multiplication relations of S' as in the proofs of Theorems 3.1 and 3.2. Since K is a subfield of S' and since the language $\mathfrak{L}$ contains parameters for all members of K, we can say that for any members a and b of K, $\bar{\psi}(a) = \bar{\psi}(b)$ if and only if $\psi(a) = \psi(b)$; i.e., that the equivalence classes determined in K by $\bar{\psi}$ are the same as those determined in K by ψ.

In order to prove the theorem, it is sufficient to show that for any parameters α and β of $\mathfrak{L}$ the statement

3.36 $(\exists z)(\sim E(\beta, 0) \supset (x)(y)(S(z, x, 0) \wedge S(\alpha, x, y) \supset Q^*(y, \beta)) \wedge I(z))$

holds in K, and hence that it holds in S'. It will hold in S' if and only if for every a and b in K, with $b \neq 0$, there is a w in S' such that $\bar{\psi}(a - w) < \bar{\psi}(b)$.

https://doi.org/10.4153/CJM-1955-051-7 Published online by Cambridge University Press

Now

(i) if $\bar{\psi}(t) < \bar{\psi}(1)$, let $w = a - b.t$;

(ii) if $\bar{\psi}(1) < \bar{\psi}(t)$, let $w = a - b.t^{-1}$; and

(iii) if $\bar{\psi}(t) = \bar{\psi}(1)$, choose k in K, $k \neq 0$, such that $\bar{\psi}(k) < \bar{\psi}(1)$, i.e., such that $\psi(k) < \psi(1)$, and let $w = a - b.k.t$.

In the last case, such a k can be found since 3.32 holds in K, and hence for some k, $k \neq 0$, either $\psi(k) < \psi(1)$ or $\psi(1) < \psi(k)$ and hence either $\psi(k) < \psi(1)$ or $\psi(k^{-1}) < \psi(1)$ by 3.26. Each of the w's chosen can be shown to satisfy $\bar{\psi}(a - w) < \bar{\psi}(b)$, for

(i) since $\sim E(b, 0)$ holds in S' so does $\sim E^*(b, 0)$ by 3.34, and therefore $\bar{\psi}(t.b) < \bar{\psi}(a)$ by 3.33;

(ii) By 3.26, $\bar{\psi}(t^{-1}) < \bar{\psi}(1)$; the remainder of the proof can be completed as in case (i);

(iii) $\bar{\psi}(k.b) < \bar{\psi}(b)$ can be proven following the previous cases, and from this by 3.35 can be proven $\bar{\psi}(k.b.t) < \bar{\psi}(b)$.

Finally, each of the w's will satisfy $I(z)$ since in each case $p(w, x)$ will be irreducible over S and therefore irreducible over S'. Hence we have shown that 3.36 holds in S' for any parameters α and β of $\mathfrak{L}$ and have therefore established the theorem.

References

1. K. Dörge, *Zum Hilbertschen Irreduzibilitätssatz*, Math. Ann., *95* (1926), 84–97.

2. W. Franz, *Untersuchungen zum Hilbertschen Irreduzibilitätssatz*, Math. Z., *33* (1931), 275–293.

3. L. Henkin, *Some interconnections between modern algebra and mathematical logic*, Trans. Amer. Math. Soc., *74* (1953), 410–427.

4. E. Inaba, *Ueber den Hilbertschen Irreduzibilitätssatz*, Japanese J. Math., *19* (1944), 1–25.

5. A. Robinson, *On the metamathematics of algebra* (Amsterdam, North-Holland, 1951).

6. ———, *Les rapports entre le calcul déductif et l'interprétation sémantique d'un système axiomatique*: *Les méthodes formelles en axiomatique* (Colloques Internationaux du Centre National de la Recherche Scientifique, no. 36, Paris, 1950).

7. B. L. van der Waerden, *Modern algebra*, vol. 1 (New York, F. Ungar, 1949).

Pennsylvania State College *University of Toronto*

https://doi.org/10.4153/CJM-1955-051-7 Published online by Cambridge University Press