J. Korean Math. Soc.
Vol. 11, No. 1, 1974

ARBITRARY EXTENSIONS OF A FIELD

BY P. RAMANKUTTY

This note deals with the extension of a field F by an arbitrary subset S of a field E of which F is a subfield. Some of the well known theorems regarding such extensions for finite S are carried over to the case of arbitrary S. The exposition follows a pattern slightly different from what is usually found in the literature and this makes the proofs more concise. To facilitate this the following special notations are used. The terminology is that of [**1**].

Notation

$F<E$: F is a subfield of the field E.

$|S|$ denotes the cardinal number of the set S.

$\mathfrak{F}(S)$ denotes the collection of all finite subsets of S.

$E|K$ normal: E is a normal extension of the field K.

$F[x_1, \cdots\cdots, x_n]$ denotes the ring of polynomials in the variables $x_1, \cdots\cdots, x_n$ over the field F.

$\overset{5}{\Longrightarrow}$ means: this implication is a consequence of the item numbered 5 above.

Definitions and Properties

1. DEFINITION. If $F<E$ and $S\subset E$ then the smallest subfield of E containing F and S is called the *field generated by S over F* and is denoted by $F(S)$. Thus $F(S)=\bigcap\{K\colon F<K<E \text{ and } S\subset K\}$.

2. DEFINITION. If $F<E$ and S is a finite subset of E, say $S=\{\alpha_1, \cdots\cdots, \alpha_n\}$, then $F[S]$ is defined by $F[S]=\{f(\alpha_1, \cdots, \alpha_n) : f(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]\}$.

3. DEFINITION. If $F<E$ and $S\subset E$ then $F[S]=\bigcup\{F[A] : A\in\mathfrak{F}(S)\}$. (No algebraic structure is claimed for $F[S]$ in this definition. Clearly $S\subset T \Longrightarrow \mathfrak{F}(S)\subset\mathfrak{F}(T) \Longrightarrow F[S]\subset F[T]$.)

4. DEFINITION. If $F<E$ and $S\subset E$ then an element $a\in E$ is called *a rational function on S with coefficients in F* iff there exists a positive integer n and polynomials $f(x_1, \cdots, x_n)$, $g(x_1, \cdots, x_n)$ in $F[x_1, \cdots, x_n]$ and a set $\{\alpha_1, \cdots, \alpha_n\}\subset S$ such that $g(\alpha_1, \cdots, \alpha_n)\neq 0$ and $a=f(\alpha_1, \cdots, \alpha_n)/g(\alpha_1, \cdots, \alpha_n)$.

5. *If $F<E$ and $S\subset E$ then* $F(S)=\{a\in E$: *a is a rational function on S with coefficients in F*$\}$.

Received by the editors Jan. 5, 1974.

Proof. If K denotes the set $\{\ \}$ above, then K is a field and $K\subset F(S)$; also $F\subset K$ and $S\subset K$ so that $F(S)\subset K$.

6. *If $F<E$ and $S\subset E$, then $F(S)=\bigcup\{F(A):\ A\in\mathfrak{F}(S)\}$.*

Proof.
$A\subset S\subset F(S)$ *and* $F\subset F(S) \implies F\cup A\subset F(S) \implies F(A)\subset F(S)$ for each $A\in\mathfrak{F}(S)$.
Hence $\bigcup\{F(A):\ A\in\mathfrak{F}(S)\}\subset F(S)$.

Also, $a\in F(S) \overset{5}{\implies} a=f(\alpha_1,\cdots,\alpha_n)/g(\alpha_1,\cdots,\alpha_n)$ for some $\{\alpha_1,\cdots,\alpha_n\}\subset S$ and f, g in $F[x_1,\cdots,x_n]$

$\implies a\in F(\alpha_1,\cdots,\alpha_n)$ using $\{\alpha_1,\cdots,\alpha_n\}$ instead of S in 5 above i.e. $a\in F(S) \implies a\in F(A)$ for some $A\in\mathfrak{F}(S)$. Hence $F(S)\subset\bigcup\{F(A);A\in\mathfrak{F}(S)\}$.

7. *If $F<E$ and $S\subset E$ then $F[S]$ is a subring of $F(S)$* (and hence $F[S]$ is an entire ring).

Proof. If a, b, c are elements of $F[S]$ then there exist A, B, C in $\mathfrak{F}(S)$ such that $a\in F[A]$, $b\in F[B]$, $c\in F[C]$. Then by 3, a, b, c are elements of $F[D]$ where $D=A\cup B\cup C$. So if $D=\{\alpha_1,\cdots,\alpha_n\}$ then $a=f(\alpha_1,\cdots,\alpha_n)$, $b=g(\alpha_1,\cdots,\alpha_n)$, $c=h(\alpha_1,\cdots,\alpha_n)$ for some f, g, h in $F[x_1,\cdots,x_n]$. Since f, g, h satisfy the ring axioms it follows that a, b, c also do.

8. *If $F<E$ and A, B are subsets of E then $F(A)(B)=F(A\cup B)=F(B)(A)$.*

Proof. Writing $S=A\cup B$, $F\cup S\subset F(A)(B) \implies F(S)<F(A)(B)$ and $F(A)\cup B\subset F(S)\cup B=F(S) \implies F(A)(B)<F(S)$. Hence $F(S)=F(A)(B)$ and the rest is clear.

9. *If $F<E$ and $S(\subset E)$ is algebraic over F then $F[S]=F(S)$.*

(DEFINITION. S is algerbraic over F iff each element of S is algebraic over F.)

Proof. *Case I: S finite.* Usual proof by induction on $|S|$.

Case II: S arbitary. $a\in F(S) \overset{6}{\iff} A\in\mathfrak{F}(S)$ such that $a\in F(A) \overset{\text{Case I}}{=\!=} F[A] \iff a\in\bigcup\{F[A]:A\in\mathfrak{F}(S)\}=F[S]$.

10. *If $F<E$ and $S(\subset E)$ is algebraic over F then $F(S)$ is an algebraic extension of F.*

Proof. $a\in F(S) \implies a\in F(A)$ for some $A\in\mathfrak{F}(S)$. But $A\in\mathfrak{F}(S) \implies |A|<\infty \implies F(A)$ is an algebraic extension of F
(extension by a finite number of algebraic elements is an algebraic extension) and then $a\in F(A) \implies a$ is algebraic over F.

11. *If $F<E$ and $S=\{a\in E:\ a$ is algebraic over $F\}$, then $F<S<E$.*

Proof. S algebraic over $F \overset{10}{\implies} F(S)$ algebraic over $F \implies F(S)\subset S$. But of course, $S\subset F(S)$; hence $S=F(S)$.

12. DEFINITION. If E is a field and $\mathfrak{F}$ a family of subfields of E, then the *compositum of the fields of the faimly* $\mathfrak{F}$ is the smallest subfield of E containing all the fields in $\mathfrak{F}$.

NOTE: Clearly,
(i) Compositum $\mathcal{F}=\bigcap\{F: F<E \text{ and } F_i\in\mathcal{F}\Longrightarrow F_i<F\}$,
(ii) if $F\in\mathcal{F}$ and $S=\bigcup\mathcal{F}$, then compositum $\mathcal{F}=F(S)$.

13. *If $F<E$ then E is the compositum of all subfields of E which are finitely generated over F.*

(DEFINITION. If $F<K<E$, then K is said to be finitely generated over F iff $K=F(A)$ for some finite subset A of E.)

Proof. $E=F(E)\overset{6}{=}\bigcup\{F(A):\ A\in\mathcal{F}(E)\}\subset\text{Compositum } F(A);A\in\mathcal{F}(E)\}<E.$

14. *If $k<F<K$ and $S\subset K$ then $k(S)\cdot F=F(S)$.*

Proof. $k<F\Longrightarrow k(S)<F(S)\Longrightarrow k(S)\cup F\subset F(S)\Longrightarrow k(S)\cdot F<F(S)$.
Also, $F\cup S\subset k(S)\cdot F\Longrightarrow F(S)<k(S)\cdot F$.

15. *If $k<F<K$ and $E(<K)$ is an algebraic extension of k, then EF is an algebraic extension of F.*

Proof. E algebraic over $k\Longrightarrow E$ algebraic over $F\overset{10}{\Longrightarrow}F(E)$ algebraic over F.
But $F(E)=E\cdot F$.

16. *Let $k<F<K$.*
(i) *If F is finitely generated over k and K is finitely generated over F, then K is finitely generated over k.*
(ii) *If $E(<K)$ is finitely generated over k then $E\cdot F$ is finitely generated over F.*

Proof.

(i) By hypothesis, there exist $A\subset F$ and $B\subset K$ such that $|A|<\infty$, $|B|<\infty$ and $F=k(A)$, $K=F(B)$. Hence

$K=k(A)(B)\overset{8}{=}k(A\cup B)$. But $A\cup B$ is a finite subset of K.

(ii) Since E is finitely generated over k there exists a finite subset S of E such that $E=k(S)$. Hence

$E\cdot F=k(S)\cdot F\overset{14}{=}F(S)$.

DEFINITION. 17. If $k<K$ and a is a non-zero cardinal then K is said to be ***a*-generated over k** iff there exists a subset S of K such that $K=k(S)$ and $|S|=a$.
(*Note*: The condition $|S|=a$ may be replaced by $|S|\leqslant a$.)

18. *Let a, b be non-zero cardinals of which one is infinite and suppose $k<F<K$. If F is a-generated over k and K is b-generated over F then K is ab-generated over k.*

Proof. Let $A\subset F$, $B\subset K$ be such that $|A|=a$, $|B|=b$ and $F=k(A)$, $K=F(B)$.
Then $K=k(A)(B)\overset{8}{=}k(A\cup B)$. Also $|A\cup B|=\max\{a,b\}=ab$.

19. *If $k<F<K$ and $E(<K)$ is a-generated over k then $E\cdot F$ is a-generated over F.*
Proof. Since E is a-generated over k, $E=k(S)$ for some $S\subset E$ with $|S|=a$. Hence
$E\cdot F=k(S)\cdot F\overset{14}{=}F(S)$.

DEFINITION. 20. If $\{f_i\}_{i\in I}$ is a family of polynomials in $k[x]$ with $\deg f_i \geqslant 1$ for each i, then $K < \bar{k}$ is called the *splitting field of the family* $\{f_i\}_{i\in I}$ iff $K = k(S)$ where $S = \{s \in \bar{k} : f_i(s) = 0$ for some $i \in I\}$.

21. *If $f_i \in k[x]$ for each $i \in I$ and K_i is the splitting field of f_i over k, then the splitting field K of the family $\{f_i\}_{i\in I}$ over k is the compositum of $\{K_i\}_{i\in I}$ in $\bar{k}$.*

Proof. Let $S = \{s \in \bar{k} : f_i(s) = 0$ for some $i \in I\}$ so that $K = k(S)$; let E be the compositum of $\{K_i\}_{i\in I}$. Clearly, K contains all the roots of $f_i \Longrightarrow f_i(x)$ splits in $K[x]$ $\Longrightarrow K_i < K$. Since this is true for each i, $E < K$. Conversely, $s \in S \Longrightarrow s \in K_i$ for some $i \Longrightarrow s \in E$. Hence $S \subset E$ so that $K = k(s) \subset k \cdot E = E$.

22. *If $k < F < L$ and $k < E < L$ then $E|k$ normal $\Longrightarrow EF|F$ normal.*

Proof. Let E be the splitting field of the family $\{f_i\}_{i\in I}$ in $k[x]$ and let $S = \{s \in \bar{k} : f_i(s) = 0$ for some $i \in I\}$.

Then $E = k(S)$ so that $E \cdot F = k(S) \cdot F \overset{14}{=} F(S)$ and this implies that $E \cdot F$ is the splitting extension of F for the family $\{f_i\}_{i\in I}$ in $F[x]$. Hence $EF|F$ is normal.

23. *If k is a field and $\{E_j\}_{j\in J}$ a family of fields such that $E_j|k$ normal for each $j \in J$, then $E|k$ normal where $E =$ compositum $\{E_j\}_{j\in J}$.*

Proof. Let E_j E_j be the splitting field of the faimily $\{f_{j,i}\}_{i\in I_j}$ in $k[x]$ and let $S_j = \{s \in \bar{k} : f_{j,i}(s) = 0$ for some $i \in I_j\}$ so that $E_j = k(S_j)$. Let $\mathfrak{F} = \{f_{j,i} : i \in I_j,\ j \in J\}$ and $S = \cup\{S_j : j \in J\}$. Then $S = \{s \in \bar{k} : f(s) = 0$ forsome $f \in \mathfrak{F}\}$ Now $E_j = k(S_j) < k(S)$ for each $j \in J$ and hence $E < k(S)$. Also, $S_j \subset E_j < E$ for each $j \in J$ so that $S \subset E$. Hence $k(S) < k(E) = E$.

Reference

[1] Lang, S., *Algebra*. Addison-Wesley, 1965.

University of Auckland