PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 18 (32), 1975, pp. 193—195

HOW MANY ALGEBRAIC (FINITE) EXTENSIONS OVER THE RATIONALS

Keng-Teh Tan

(Received April 29, 1974)

1. Introduction

In this note, we will prove the following two results:

Proposition A: The cardinality of the set of all non-isomorphic finite extensions over $\mathbf{Q}$ is $\aleph_0$.

Proposition B: The cardinality of the set of all non-isomorphic algebraic extensions over $\mathbf{Q}$ is $\aleph_1$.

We define the irreducible bound for an arbitrary field k. Some basic properties of fields in terms of this bound are also observed.

All our terminologies and notations are standard, see [1] for instance. Unless otherwise stated, all fields considered here will be of zero characteristic. The letter k always denotes a field. $\mathbf{Q}$, $\mathbf{A}$, $\mathbf{R}$, $\mathbf{C}$, as usual, denote respectively the fields of rational, algebraic, real and complex numbers. Also, $\mathbf{N}$ denotes the set of all positive integers.

2. Proof of The Propositions

We first give the following

Definition: Let k be a field of arbitrary characteristic. Let

$$Ib(k) = \sup\{\deg f(x) \mid f(x) \in k[x],\ f(x) \text{ irreducible}\} \leqslant \infty.$$

We call $Ib(k)$ the irreducible bound of k.

The following facts are well known:

$$\text{(a) } Ib(\mathbf{C}) = 1; \qquad \text{(b) } Ib(\mathbf{R}) = 2;$$

$$\text{(c) } Ib(\mathbf{Q}) = \infty; \qquad \text{(d) } Ib(\mathbf{A}) = 1.$$

In fact, (a) follows from the fundamental theorem of algebra, (c) follows from Eisenstein's theorem, (b) follows from the fact that every irreducible poly-

nomial in $\mathbf{R}[x]$ is either linear or quadratic. (d) follows from the following more general fact:

(e) k is algebraically closed iff $Ib(k)=1$.

We now prove the following result:

(f) Let $n\in\mathbf{N}$. Then $Ib(k)\leq n$ iff every algebraic extension of k is finite of degree at most n.

Proof: ($\Rightarrow$) Let K be an algebraic extension of k. Let $\alpha\in K$ be algebraic of degree t_1 over k with t_1 maximal. Such a t_1 exists by assumption. Then $[k(\alpha):k]=t_1\leq n$. We claim that $K=k(\alpha)$. Assume the contrary. Let $\beta\in K\setminus k(\alpha)$ and the algebraic degree of β over $k(\alpha)$ be t_2. Then

$$[k(\alpha)(\beta):k]=t_1 t_2>t_1.$$

However, since k is of zero characteristic, it is perfect, hence $k(\alpha)(\beta)$, being a finite extension over k, is a finite separable extension over k. Thus there exists $\gamma\in k(\alpha)(\beta)$ such that $k(\alpha)(\beta)=k(\gamma)$, by the primitive element theorem ([1], page 358). It follows that γ is algebraic of degree $t_1 t_2$ over k, contradicting the maximality of t_1.

($\Leftarrow$) Let $f(x)\in k[x]$ be irreducible and $\deg f(x)=m$. Then there exists an extension K over k with $[K:k]\leq m!$ and $f(x)$ splits completely over K. Thus $m\leq m!\leq n$. Hence $Ib(k)\leq n$.

An interesting consequence of (f) is the following known fact:

(g) $\mathbf{C}$ is the only proper algebraic extension of $\mathbf{R}$.

Indeed, every proper algebraic extension of $\mathbf{R}$ must be of degree 2. The uniqueness now follows from the fact that any extension of $\mathbf{R}$ of degree 2 is the splitting field for $f(x)=x^2+1$ over $\mathbf{R}$.

Proof of proposition *A*. Let $n\in\mathbf{N}$ be fixed and K an extension of degree n over $\mathbf{Q}$. Then in view of Theorem 33 [2], page 107, we may assume, without loss of generality, that $K\subseteq\mathbf{A}$. Thus $K=\mathbf{Q}(\alpha)$ for some $\alpha\in\mathbf{A}$ by the primitive element theorem. Since $|\mathbf{A}|=\aleph_0$, it follows that there are at most $\aleph_0$ non-isomorphic extensions of degree n over $\mathbf{Q}$. Consequently, the cardinality of the set of all non-isomorphic finite extensions over $\mathbf{Q}$ is at most $\aleph_0$. Trivially there are at least $\aleph_0$ non-isomorphic finite extensions over $\mathbf{Q}$ by considerations of degrees. This proves proposition *A*.

Proof of proposition *B*. Let $P=\{p_1, p_2, \ldots, p_n, \ldots\}$ be the set of all primes ordered naturally. Let $\alpha_i\in\mathbf{R}$ be such that $\alpha_i^{p_i}=2$. Let T be the collection of all non-empty subsets of P. Then $|T|=\aleph_1$. For $X\in T$, let $\overline{X}=\{\alpha_i \mid p_i\in X\}$. Then $\mathbf{Q}(\overline{X})$ is algebraic over $\mathbf{Q}$, since each element in $\overline{X}$ is algebraic over $\mathbf{Q}$.

We now show that for $X\neq Y$, $X, Y\in T$, $\mathbf{Q}(\overline{X})$ is not isomorphic to $\mathbf{Q}(\overline{Y})$.

Let $q\in X\setminus Y$. Then $\mathbf{Q}(\overline{X})$ contains an element α with $\alpha^q=2$ But for each $y\in\mathbf{Q}(\overline{Y})$, $y^q\neq 2$. Indeed, assume that some $y\in Q(\overline{Y})$ be such that $y^q=2$. Then $\mathbf{Q}\subseteq\mathbf{Q}(y)\subseteq\mathbf{Q}(\overline{Y})$ and $[\mathbf{Q}(y):\mathbf{Q}]=q$ as follows from Eisenstein's theorem ([1], page 255).

Let $|Y|=\omega\leq\aleph_0$ and $Y=\{P_{i\beta} \mid 1\leq\beta\leq\infty\}$.

Then

$$\mathbf{Q}(\overline{Y}) = \sum_{n=1}^{\omega} \mathbf{Q}(\alpha_{i_1}, \ldots, \alpha_{i_n}\}.$$

Thus,

$$y \in \mathbf{Q}(\alpha_{i_1}, \ldots, \alpha_{i_m}) = F,$$

say, for some $m \in \mathbf{N}$. Hence $q \mid [F:\mathbf{Q}]$. Clearly, $[F:\mathbf{Q}] \mid p_{i_1} \ldots p_{i_m}$. So $q \mid p_{i_1} \ldots p_{i_m}$, a contradiction. This proves the claim. Consequently, there are at least $\aleph_1$ non-isomorphic algebraic extensions over $\mathbf{Q}$. However, it is well known that every algebraic extension of $\mathbf{Q}$ is isomorphic to a subfield of $\mathbf{A}$, the algebraic closure of $\mathbf{Q}$ ([2], Theorem 33, page 107) and that $|\mathbf{A}| = \aleph_0$, the proposition now follows.

Remark: The author believes that for each positive integer $n > 1$, there are $\aleph_0$ non-isomorphic extensions of degree n over $\mathbf{Q}$. The author knows of no proof yet.

REFERENCES

[1] J. B. Fraleigh, *A first Course in Abstract Algebra*, Addison-Wesley Publishing Co., 1971.

[2] O. Zariski, P. Samuel, *Cammutative algebra*, vol. I, Von Norstrand, 1965.

Department of Mathematics,
University of Malaya,
Kuala Lumpur,
Malaysia