that Proposition 12 implies each α_i is algebraic over F. Since K is obviously generated over F by $\alpha_1, \alpha_2, \dots, \alpha_n$, we see that K is generated by a finite number of algebraic elements over F. The converse was proved above. The second statement of the theorem is immediate from Corollary 13 and the computation above.

The first example above shows that the inequality for the degree of the extension given in the theorem may be strict. We remark that information helpful in the determination of this degree can often be obtained by determining subfields and then applying Corollary 15.

Corollary 18. Suppose α and β are algebraic over F. Then $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ (for $\beta \neq 0$), (in particular α^{-1} for $\alpha \neq 0$) are all algebraic.

Proof: All of these elements lie in the extension $F(\alpha, \beta)$, which is finite over F by the theorem, hence they are algebraic by Corollary 13.

Corollary 19. Let L/F be an arbitrary extension. Then the collection of elements of L that are algebraic over F form a subfield K of L.

Proof: This is immediate from the previous corollary.

Examples

(1) Consider the extension $\mathbb{C}/\mathbb{Q}$ and let $\overline{\mathbb{Q}}$ denote the subfield of all elements in $\mathbb{C}$ that are algebraic over $\mathbb{Q}$. In particular, the elements $\sqrt[n]{2}$ (the positive n^{th} roots of 2 in $\mathbb{R}$) are all elements of $\overline{\mathbb{Q}}$, so that $[\overline{\mathbb{Q}} : \mathbb{Q}] \geq n$ for all integers $n > 1$. Hence $\overline{\mathbb{Q}}$ is an *infinite* algebraic extension of $\mathbb{Q}$, called the field of *algebraic numbers*.

(2) Consider the field $\overline{\mathbb{Q}} \cap \mathbb{R}$, the subfield of $\mathbb{R}$ consisting of elements algebraic over $\mathbb{Q}$. The field $\mathbb{Q}$ is *countable*. The number of polynomials in $\mathbb{Q}[x]$ of any given degree n is therefore also countable (since such a polynomial is determined by specifying $n + 1$ coefficients from $\mathbb{Q}$). Since these polynomials have at most n roots in $\mathbb{R}$, the number of algebraic elements of $\mathbb{R}$ of degree n is countable. Finally, the collection of all algebraic elements in $\mathbb{R}$ is the countable union (indexed by n) of countable sets, hence is countable. Since $\mathbb{R}$ is uncountable, it follows that there exist (in fact many) elements of $\mathbb{R}$ which are not algebraic, i.e., are transcendental, over $\mathbb{Q}$. In particular the subfield $\overline{\mathbb{Q}} \cap \mathbb{R}$ of algebraic elements of $\mathbb{R}$ is a *proper* subfield of $\mathbb{R}$, so also $\overline{\mathbb{Q}}$ is a proper subfield of $\mathbb{C}$.

It is extremely difficult in general to prove that a given real number is not algebraic. For example, it is known (these are theorems) that $\pi = 3.14159...$ and $e = 2.71828...$ are transcendental elements of $\mathbb{R}$. Even the proofs that these elements are not *rational* are not too easy.

Theorem 20. If K is algebraic over F and L is algebraic over K, then L is algebraic over F.

Proof: Let α be any element of L. Then α is algebraic over K, so α satisfies some polynomial equation

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

where the coefficients $a_0, a_1, \dots, a_n$ are in K. Consider the field $F(\alpha, a_0, a_1, \dots, a_n)$ generated over F by α and the coefficients of this polynomial. Since K/F is algebraic, the elements $a_0, a_1, \dots, a_n$ are algebraic over F, so the extension $F(a_0, a_1, \dots, a_n)/F$ is finite by Theorem 17. By the equation above, we see that α generates an extension of this field of degree at most n, since its minimal polynomial over this field is a divisor of the polynomial above. Therefore

$$[F(\alpha, a_0, a_1, \dots, a_n) : F] = [F(\alpha, a_0, \dots, a_n) : F(a_0, \dots, a_n)][F(a_0, \dots, a_n) : F]$$

is also finite and $F(\alpha, a_0, a_1, \dots, a_n)/F$ is an algebraic extension. In particular the element α is algebraic over F, which proves that L is algebraic over F.

The subfield $F(\alpha_1, \alpha_2, \dots, \alpha_k)$ generated by a finite set of elements $\alpha_1, \alpha_2, \dots, \alpha_k$ of a field K contains each of the fields $F(\alpha_i)$, $i = 1, 2, \dots, k$. By the definitions, it is also the smallest subfield of K containing these fields.

Definition. Let K_1 and K_2 be two subfields of a field K. Then the *composite field* of K_1 and K_2, denoted K_1K_2, is the smallest subfield of K containing both K_1 and K_2. Similarly, the composite of any collection of subfields of K is the smallest subfield containing all the subfields.

Note that the composite K_1K_2 can also be described as the intersection of all the subfields of K containing both K_1 and K_2 and similarly for the composite of more than two fields, analogous to the subgroup generated by a subset of a group (cf. Section 2.4).

Example

The composite of the two fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt[3]{2})$ is the field $\mathbb{Q}(\sqrt[6]{2})$. This is because this field contains both of these subfields ($(\sqrt[6]{2})^3 = \sqrt{2}$ and $(\sqrt[6]{2})^2 = \sqrt[3]{2}$) and conversely, any field containing both $\sqrt{2}$ and $\sqrt[3]{2}$ contains their quotient, which is $\sqrt[6]{2}$.

Suppose now that K_1 and K_2 are finite extensions of F in K. Let $\alpha_1, \alpha_2, \dots, \alpha_n$ be an F-basis for K_1 and let $\beta_1, \beta_2, \dots, \beta_m$ be an F-basis for K_2 (so that $[K_1 : F] = n$ and $[K_2 : F] = m$). Then it is clear that these give generators for the composite K_1K_2 over F:

$$K_1K_2 = F(\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_m).$$

Since $\alpha_1, \alpha_2, \dots, \alpha_n$ is an F-basis for K_1 any power ${\alpha_i}^k$ of one of the α's is a *linear* combination with coefficients in F of the α's and a similar statement holds for the β's. It follows that the collection of linear combinations

$$\sum_{\substack{i=1,2,\dots,n \\ j=1,2,\dots,m}} a_{ij}\alpha_i\beta_j$$

with coefficients in F is *closed* under multiplication and addition since in a product of two such elements any higher powers of the α's and β's can be replaced by linear expressions. Hence, the elements $\alpha_i\beta_j$ for $i = 1, 2, \dots, n$ and $j = 1, 2, \dots, m$ *span* the composite extension K_1K_2 over F. In particular, $[K_1K_2 : F] \leq mn$. We summarize this as:

Proposition 21. Let K_1 and K_2 be two finite extensions of a field F contained in K. Then

$$[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$$

with equality if and only if an F-basis for one of the fields remains linearly independent over the other field. If $\alpha_1, \alpha_2, \ldots, \alpha_n$ and $\beta_1, \beta_2, \ldots, \beta_m$ are bases for K_1 and K_2 over F, respectively, then the elements $\alpha_i\beta_j$ for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, m$ span K_1K_2 over F.

Proof: From $K_1K_2 = F(\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_m) = K_1(\beta_1, \beta_2, \ldots, \beta_m)$, we see as above that $\beta_1, \beta_2, \ldots, \beta_m$ span K_1K_2 over K_1. Hence $[K_1K_2 : K_1] \leq m = [K_2 : F]$ with equality if and only if these elements are linearly independent over K_1. Since $[K_1K_2 : F] = [K_1K_2 : K_1][K_1 : F]$ this proves the proposition.

By the proposition (and its proof), we have the following diagram:

$$\begin{tikzcd}
 & K_1K_2 & \\
K_1 \arrow[ur, dash, "\leq m"] & & K_2 \arrow[ul, dash, "\leq n"'] \\
 & F \arrow[ul, dash, "n"] \arrow[ur, dash, "m"'] &
\end{tikzcd}$$

We shall have examples shortly where the inequality in the proposition is strict. One useful situation where one can be certain of equality is the following:

Corollary 22. Suppose that $[K_1 : F] = n$, $[K_2 : F] = m$ in Proposition 21, where n and m are relatively prime: $(n, m) = 1$. Then $[K_1K_2 : F] = [K_1 : F][K_2 : F] = nm$.

Proof: In general the extension degree $[K_1K_2 : F]$ is divisible by both n and m since K_1 and K_2 are subfields of K_1K_2, hence is divisible by their least common multiple. In this case, since $(n, m) = 1$, this means $[K_1K_2 : F]$ is divisible by nm, which together with the inequality $[K_1K_2 : F] \leq nm$ of the proposition proves the corollary.

Example

The composite of the two fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt[3]{2})$ is of degree 6 over $\mathbb{Q}$, which we determined earlier by actually computing the composite $\mathbb{Q}(\sqrt[6]{2})$.

EXERCISES

1. Let $\mathbb{F}$ be a finite field of characteristic p. Prove that $|\mathbb{F}| = p^n$ for some positive integer n.
2. Let $g(x) = x^2 + x - 1$ and let $h(x) = x^3 - x + 1$. Obtain fields of 4, 8, 9 and 27 elements by adjoining a root of $f(x)$ to the field F where $f(x) = g(x)$ or $h(x)$ and $F = \mathbb{F}_2$ or $\mathbb{F}_3$. Write down the multiplication tables for the fields with 4 and 9 elements and show that the nonzero elements form a cyclic group.
3. Determine the minimal polynomial over $\mathbb{Q}$ for the element $1 + i$.

4. Determine the degree over $\mathbb{Q}$ of $2+\sqrt{3}$ and of $1+\sqrt[3]{2}+\sqrt[3]{4}$.

5. Let $F=\mathbb{Q}(i)$. Prove that x^3-2 and x^3-3 are irreducible over F.

6. Prove directly from the definitions that the field $F(\alpha_1,\alpha_2,\dots,\alpha_n)$ is the composite of the fields $F(\alpha_1), F(\alpha_2),\dots,F(\alpha_n)$.

7. Prove that $\mathbb{Q}(\sqrt{2}+\sqrt{3})=\mathbb{Q}(\sqrt{2},\sqrt{3})$ [one inclusion is obvious, for the other consider $(\sqrt{2}+\sqrt{3})^2$, etc.]. Conclude that $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]=4$. Find an irreducible polynomial satisfied by $\sqrt{2}+\sqrt{3}$.

8. Let F be a field of characteristic $\neq 2$. Let D_1 and D_2 be elements of F, neither of which is a square in F. Prove that $F(\sqrt{D_1},\sqrt{D_2})$ is of degree 4 over F if D_1D_2 is not a square in F and is of degree 2 over F otherwise. When $F(\sqrt{D_1},\sqrt{D_2})$ is of degree 4 over F the field is called a *biquadratic extension of F*.

9. Let F be a field of characteristic $\neq 2$. Let a,b be elements of the field F with b not a square in F. Prove that a necessary and sufficient condition for $\sqrt{a+\sqrt{b}}=\sqrt{m}+\sqrt{n}$ for some m and n in F is that a^2-b is a square in F. Use this to determine when the field $\mathbb{Q}(\sqrt{a+\sqrt{b}})$ $(a,b\in\mathbb{Q})$ is biquadratic over $\mathbb{Q}$.

10. Determine the degree of the extension $\mathbb{Q}(\sqrt{3+2\sqrt{2}})$ over $\mathbb{Q}$.

11. (a) Let $\sqrt{3+4i}$ denote the square root of the complex number $3+4i$ that lies in the first quadrant and let $\sqrt{3-4i}$ denote the square root of $3-4i$ that lies in the fourth quadrant. Prove that $[\mathbb{Q}(\sqrt{3+4i}+\sqrt{3-4i}):\mathbb{Q}]=1$.

(b) Determine the degree of the extension $\mathbb{Q}(\sqrt{1+\sqrt{-3}}+\sqrt{1-\sqrt{-3}})$ over $\mathbb{Q}$.

12. Suppose the degree of the extension K/F is a prime p. Show that any subfield E of K containing F is either K or F.

13. Suppose $F=\mathbb{Q}(\alpha_1,\alpha_2,\dots,\alpha_n)$ where $\alpha_i^2\in\mathbb{Q}$ for $i=1,2,\dots,n$. Prove that $\sqrt[3]{2}\notin F$.

14. Prove that if $[F(\alpha):F]$ is odd then $F(\alpha)=F(\alpha^2)$.

15. A field F is said to be *formally real* if -1 is not expressible as a sum of squares in F. Let F be a formally real field, let $f(x)\in F[x]$ be an irreducible polynomial of odd degree and let α be a root of $f(x)$. Prove that $F(\alpha)$ is also formally real. [Pick α a counterexample of minimal degree. Show that $-1+f(x)g(x)=(p_1(x))^2+\cdots+(p_m(x))^2$ for some $p_i(x), g(x)\in F[x]$ where $g(x)$ has odd degree $<\deg f$. Show that some root β of g has odd degree over F and $F(\beta)$ is not formally real, violating the minimality of α.]

16. Let K/F be an algebraic extension and let R be a *ring* contained in K and containing F. Show that R is a subfield of K containing F.

17. Let $f(x)$ be an irreducible polynomial of degree n over a field F. Let $g(x)$ be any polynomial in $F[x]$. Prove that every irreducible factor of the composite polynomial $f(g(x))$ has degree divisible by n.

18. Let k be a field and let $k(x)$ be the field of rational functions in x with coefficients from k. Let $t\in k(x)$ be the rational function $\dfrac{P(x)}{Q(x)}$ with relatively prime polynomials $P(x), Q(x)\in k[x]$, with $Q(x)\neq 0$. Then $k(x)$ is an extension of $k(t)$ and to compute its degree it is necessary to compute the minimal polynomial with coefficients in $k(t)$ satisfied by x.

(a) Show that the polynomial $P(X)-tQ(X)$ in the variable X and coefficients in $k(t)$ is irreducible over $k(t)$ and has x as a root. [By Gauss' Lemma this polynomial is irreducible in $(k(t))[X]$ if and only if it is irreducible in $(k[t])[X]$. Then note that $(k[t])[X]=(k[X])[t]$.]