and if wM; c Mf for one of the Mu then wM1M2 • ■ • M,. c MlMz ■ • ■ Mr. We shall use these remarks and Lemma 1 to prove checked 18/2

và nếu $wM_i \subset M_i$ đối với một trong các M_i thì $wM_1M_2 \ldots . M_i \subset M_1M_2 \ldots . M_i$. Chúng ta sẽ dùng những tính chất này và Bổ đề 1 để chứng minh

THEOREM 4.23. If E is afield and R is a subring of E, the set A of R-integral elements of E is a subring of E containing R. Moreover, any element of E which is A-integral is R-integral (and so is contained in A).

Định lý 4.23. Nếu E là một trường và R là một vành con của E, tập hợp A các phần tử R-nguyên của E là một vành con của E chứa R. Hơn nữa, bất kỳ phần tử nào của E là A-nguyên cũng là R-nguyên (và vì vậy sẽ nằm trong A).

Proof. Let u and v e A so that there exist finitely generated ^-submodules M and N of E containing 1 such that uM c M and vN cz]V. Then (u + v)MN <= u(MN) + v(MN) <= MN. Also (uv)MN c MN. Since 1 e MN the conditions of Lemma 1 are satisfied for u + v, 1 and uv. Hence these elements are R-integral and A is thus a subring of E. It is clear also that A R. Now let u be A-integral. Then we have an M = An, + • • • + Au,, containing 1 and satisfying uM c M. We may as well assume ut = 1. Since uM c M there exist e A such that uui = £ afjiij. Now there exists a finitely generated i?-submodule jVy such that aijNfj c NfJ and 1 e N;j. Multiplying together the Ntj we obtain a finitely generated module N = Rv± + ■ ■ ■ + Rvm with v1 = 1 satisfying atjN <= N for every av. Let P = Ru,Vj. Then l = u1VisP and u(UiVk) =]T a{jUjVk — £ ufiijVk. Since ai:ivk e N tins is an R-linear combination of the elements UjVk. It follows that uP <= P, and so u is R-integral, by Lemma 1, □

Proof. Let u and $v \in A$ so that there exist finitely generated R-submodules M and N of E containing 1 such that $uM \subset M$ and $vN \subset N$. Then $(u \pm v)MN \subset u(MN) + v(MN) \subset MN$. Also $(uv)MN \subset MN$. Since $1 \in MN$ the conditions of Lemma 1 are satisfied for $u \pm v$, 1 and uv. Hence these elements are R-integral and A is thus a subring of E. It is clear also that $A \supset R$. Now let u be A-integral. Then we have an $M = Au_1 + \cdots + Au_n$ containing 1 and satisfying $uM \subset M$. We may as well assume $u_1 = 1$. Since $uM \subset M$ there exist $a_{ij} \in A$ such that $uu_i = \sum a_{ij}u_j$. Now there exists a finitely generated R-submodule N_{ij} such that $a_{ij}N_{ij} \subset N_{ij}$ and $1 \in N_{ij}$. Multiplying together the N_{ij} we obtain a finitely generated module $N = Rv_1 + \cdots + Rv_m$ with $v_1 = 1$ satisfying $a_{ij}N \subset N$ for every a_{ij}. Let $P = \sum_{i,j} Ru_iv_j$. Then $1 = u_1v_1 \in P$ and $u(u_iv_k) = \sum a_{ij}u_jv_k = \sum u_ja_{ij}v_k$. Since $a_{ij}v_k \in N$ this is an R-linear combination of the elements u_jv_k. It follows that $uP \subset P$, and so u is R-integral, by Lemma 1. □

Chứng minh. Giả sử u và $v \in A$ sao cho tồn tại các R-mô-đun con được sinh hữu hạn M và N của E chứa 1 sao cho $uM \subset M$ và $vN \subset N$. Thế thì $(u \pm v)MN \subset u(MN) + v(MN) \subset MN$. Tương tự $(uv)MN \subset MN$. Bởi vì $1 \in MN$ các điều kiện của Bổ Đề 1 được thỏa mãn đối với $u \pm v$, 1 và uv. Vì thế, những phần tử này là R-nguyên và vì thế A là một vành con của E. Chúng ta cũng dễ dàng thấy rằng $A \supset R$. Bây giờ giả sử u là A-nguyên. Thế thì chúng ta có một $M \supset Au_1 + \cdots + Au_n$, chứa 1 và thỏa mãn $uM \subset M$. Chúng ta cũng có thể giả sử $u_1 = 1$. Bởi vì $uM \subset M$ tồn tại $a_{ij} \in A$ sao cho $uu_i = \sum a_{ij}M_j$. Bây giờ, tồn tại một R-mô-đun con được sinh hữu hạn N_{ij} sao cho $a_{ij}N_{ij} \subset N_{ij}$ và $1 \in N_{ij}$. Cùng nhân với N_{ij} chúng ta thu được một mô-đun được sinh hữu hạn $N = Rv_1 + \cdots . + Rv_m$ cùng với $v_1 = 1$ thỏa mãn $a_{ij}N \subset N$ đối với mỗi a_{ij}. Đặt $\sum_{i,j} Ru_iv_j$. Thế thì $1 = u_1v_1 \in P$ và $u(u_iu_k) = \sum a_{ij}u_ju_k = \sum u_ja_{ij}v_k)$. Bởi vì $a_{ij}v_k \in N$ đây là R-tổ hợp tuyến của các phần tử u_jv_k. Suy ra rằng $uP \subset P$, và vì vậy u là R-nguyên, theo Bổ Đề 1, □

In the case in which R = F is a subfield this result states that the elements of E which are algebraic over F constitute a subring. Moreover, in this case, if u is algebraic, then F(u) = -F[w]> an<i 1,1 is therefore algebraic for u ^ 0. Hence the set of elements of E which are algebraic over F constitute a subfield A of E and every element of E which is algebraic over A is contained in A.

In the case in which $R = F$ is a subfield this result states that the elements of E which are algebraic over F constitute a subring. Moreover, in this case, if u is algebraic, then $F(u) = F[u]$, and u^{-1} is therefore algebraic for $u \neq 0$. Hence the set of elements of E which are algebraic over F constitute a subfield A of E and every element of E which is algebraic over A is contained in A.

We now specialize $E = \mathbb{C}$ and $R = \mathbb{Q}$ or $\mathbb{Z}$. Then the $\mathbb{Q}$-integers are the algebraic numbers and the $\mathbb{Z}$-integers are algebraic integers. We have the following criterion for a complex number to be an algebraic integer:

[redacted]

[redacted]

Proof. If $a \in \mathbb{Z}$ it is $\mathbb{Z}$-integral. On the other hand, if $a \in \mathbb{Q}$ its minimum polynomial over $\mathbb{Q}$ is $x - a$, so if a is an algebraic integer then $a \in \mathbb{Z}$. Now let $u \in \mathbb{C}$ be algebraic over $\mathbb{Q}$ and let $f(x) = x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n \in \mathbb{Q}[x]$ be a polynomial such that $f(u) = 0$. If $b \in \mathbb{Z}$, $b \neq 0$, then bu is a root of $b^n f(b^{-1}x) = 0$ and $b^n f(b^{-1}x) = b^n(b^{-n}x^n + b^{-(n-1)}\alpha_1 x^{n-1} + \cdots + \alpha_n) = x^n + b\alpha_1 x^{n-1} + \cdots + b^n\alpha_n$. If we choose b to be the product of the denominators of the rational numbers α_i we obtain a monic polynomial in $\mathbb{Z}[x]$ having bu as a root. Then bu is an algebraic integer. □

[redacted]

We shall need to use the so-called fundamental theorem of algebra, which states that any polynomial in $\mathbb{C}[x]$ of positive degree has a root in $\mathbb{C}$. This result, which will be proved in section 5.1, implies that every monic polynomial of positive degree with coefficients in $\mathbb{C}$ factors as a product $\prod (x - r_i)$ in $\mathbb{C}[x]$. In other words, $\mathbb{C}$ contains a splitting field for every monic polynomial $\neq 1$ in $\mathbb{C}[x]$. It follows that if S is a finite set of algebraic numbers we can imbed $\mathbb{Q}(S)$ in a Galois extension $K/\mathbb{Q} \subset \mathbb{C}$.

the field of algebraic numbers A and its additive group, we now denote the latter as A' and its elements as u', where $u \to u'$ is an isomorphism of $(A, +, 0)$ onto A'. We write the composition in A' as multiplication. Then $a \to a'$ is $1-1$ and $a'b' = (a + b)'$, $0'$ is the unit of A' and $(-a)'$ is the inverse of a'. The group algebra $A[A']$ we are interested in, is the set of sums $\sum v_i u_i'$, $v_i \in A$, $u_i' \in A'$, where addition is the obvious one, and multiplication is given by the distributive law, and $(v_1 u_1')(v_2 u_2') = v_1 v_2 (u_1 + u_2)'$. Moreover, if $u_1, \ldots, u_n$ are distinct elements of A, then the elements $u_1', u_2', \ldots, u_n'$ are linearly independent over A: that is, $\sum v_i u_i' = 0$ for $v_i \in A$ implies that every $v_i = 0$. Now, in $\mathbb{C}$ we have $e^{u_1} e^{u_2} = e^{u_1 + u_2}$. Hence, by the "universal" property of group algebras given in exercise 8, p. 127, we have a homomorphism ε of $A[A']$ into $\mathbb{C}$ sending $\sum v_i u_i'$ into $\sum v_i e^{u_i}$. Theorem 4.22 can now be restated as: ε is a monomorphism.

[redacted]

[redacted]

[redacted] is a monomorphism.

The group algebra $A[A']$ is commutative. We shall now show that it is a domain. To see this we introduce an ordering in $\mathbb{C}$ which is compatible with addition, the so-called lexicographic ordering of $\mathbb{C}$. If $x = a + bi$ and $y = c + di$ where a, b, c, d are real, then we say that $x > y$ if $a > c$ or if $a = c$ and $b > d$. This ordering satisfies the trichotomy law: for any pair (x, y) either $x > y$, $x = y$, or $y > x$. Moreover, if $x > y$ and $z > t$ then $x + z > y + t$. Now let $\sum_1^n v_i u_i'$, $\sum_1^m z_j t_j'$ be two non-zero elements of $A[A']$. Then we may assume that $v_1 \neq 0$, $z_1 \neq 0$, and $u_1 > u_2 > \cdots > u_n$, $t_1 > t_2 > \cdots > t_m$. Then $(\sum v_i u_i')(\sum z_j t_j') = v_1 z_1 (u_1 + t_1)' +$ a sum of terms of the form wq' where $q < u_1 + t_1$. Clearly this is not zero, so $A[A']$ is a domain.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Suppose $\sum v_i u_i' \in \ker \varepsilon$. We can imbed the u_i and v_i in a Galois subfield $K/\mathbb{Q}$ of $\mathbb{C}$. Then the subset of elements of the form $\sum x_i y_i'$ with $x_i, y_i \in K$ is a subring $K[K']$ of $A[A']$, and if $\eta \in G = \text{Gal } K/\mathbb{Q}$, then η defines two automorphisms in $K[K']$. The first of these, which we shall denote as $\sigma(\eta)$, is $\sum x_i y_i' \to \sum \eta(x_i) y_i'$, and the second is $\tau(\eta): \sum x_i y_i' \to \sum x_i (\eta(y_i))'$. The fact that these are automorphisms is clear. Now suppose $\sum v_i u_i' \neq 0$. Then if $G = \{\eta_1, \eta_2, \ldots, \eta_m\}$ every $\sigma(\eta_j)(\sum v_i u_i') \neq 0$ and hence

[redacted]

[redacted]

[redacted]

Since U contains the factor $\sum v_i u_i'$, $U \in \ker \varepsilon$. It is clear from the commutativity of $A[A']$ that $\sigma(\eta)U = U$ for every $\eta = \eta_k \in G$. Hence if we write U as $\sum z_i t_i'$ with distinct t_i', then $\eta U = U$, that is, $\sum \eta(z_i)t_i' = \sum z_i t_i'$, implies $\eta(z_i) = z_i$ for every z_i and every $\eta \in G$. Then $z_i \in \mathbb{Q} = \text{Inv } G$. We have therefore shown that if we have a non-zero element in ker ε then we have one of the form $\sum v_i u_i'$ with rational v_i. Now apply $\tau(\eta_j)$ to this element and form

[redacted]

Then this is a non-zero element of ker ε satisfying $\tau(\eta)V = V$ for all $\eta \in G$. We can write $V = \sum z_i t_i'$ where the $z_i \in \mathbb{Q}$ and we have $\sum z_i(\eta(t_i)') = \sum z_i t_i'$, $\eta \in G$. We now average these various expressions for V to obtain

[redacted]

[redacted]

[redacted]

[redacted]

We have now shown that $\ker \varepsilon \neq 0$ implies that we have a non-zero element in $\ker \varepsilon$ of the form $\sum v_i T'(t_i)$ where the $v_i \in \mathbb{Q}$. Also, by combining terms we may assume that $T'(t_i) \neq T'(t_j)$ for $i \neq j$, which implies that $t_j \neq \eta(t_i)$ for every $\eta \in G$.

[redacted]

[redacted]

[redacted]

[redacted]

This relation shows that if $\sum v_i T'(t_i) \in \ker \varepsilon$ with $v_i \in \mathbb{Q}$, $v_1 \neq 0$, and $t_j \neq \eta(t_i)$ for every $i \neq j$ and $\eta \in G$, then multiplication by $T'(-t_1)$ gives an element in $\ker \varepsilon$ of the form

[redacted]

[redacted]

[redacted]

with $v_i \in \mathbb{Q}$, $v_0 \neq 0$, $u_i \neq 0$. Multiplication by a suitable integer allows us to assume the v_j are integers. The fact that (64) $\in \ker \varepsilon$ implies that we have the relation (63).

[redacted]

So far the argument has been purely algebraic. We now come to the analytic part of the proof, which will consist of establishing a contradiction to a relation of the form (63) where the v_i are integers, $v_0 \neq 0$, and the u_i are algebraic numbers $\neq 0$. We assume that all the u_i and hence all $\eta_j(u_i)$ are roots of a polynomial $f(x) = \sum_0^t a_k x^k \in \mathbb{Z}[x]$, $a_0 \neq 0$. Let p be a prime and introduce

[redacted]

where $s = tp + p - 1$. Then the $b_j \in \mathbb{Z}$, $b_{p-1} = {a_0}^p$ and for $p - 1 \leq j \leq s$ we have

[redacted]

It is understood here that the first bracket is 0 if $j = p - 1$. Moreover, if $j \geq p$, then $\dfrac{j!}{(j-p)!} = p!\binom{j}{p}$ so this is $p!$ times an integer. A fortiori, $\dfrac{j!}{k!}$, $0 \leq k < j - p$, is $p!$ times an integer and hence the first bracket in (65) is $p!$ times an integral polynomial. Now put

[redacted]

where $g_p(x) \in \mathbb{Z}[x]$. We observe next that

[redacted]

and these are all divisible by $f(x)$ since $h(x) = x^{p-1}f(x)^p$. Hence the first summation in (67), which is $h'(x) + h''(x) + \cdots + h^{(p-1)}(x)$, is divisible by $f(x)$ and this becomes 0 when we put $x = u_i$. Next we need to estimate $|R(u_i)|$ where $R(x)$ is the second summation in (67). We now assume that the prime p is chosen so that $p > 2|u_i|$ for all u_i. Then since $j + 1 \geq p$ also, we have

[redacted]

[redacted]

[redacted]

[redacted]

if M is the largest of the $2n$ numbers $\sum_0^t |a_k| |u_i|^k$ and $\sum_0^t |a_k| |u_i|^{k+1}$ for $i = 1, 2, \ldots, n$. Hence if $p > 2|u_i|$ then we have

[redacted]

[redacted]

[redacted]

Moreover, if in addition $p > |a_0|$, then N_p, which is given by (66), is not divisible by p since $N_p \equiv b_{p-1} = {a_0}^p \equiv a_0 \pmod{p.}$ We therefore have the following

[redacted]

[redacted]

[redacted]

LEMMA 3. *Let u_i, $1 \leq i \leq n$, be non-zero algebraic numbers, $f(x) = \sum_0^t a_k x^k \in \mathbb{Z}[x]$, $a_0 \neq 0$, be a polynomial such that $f(u_i) = 0$ for all i. Let M be the maximum of the $2n$ numbers $\sum_{k=0}^t |a_k| |u_i|^k$ and $\sum_{k=0}^t |a_k| |u_i|^{k+1}$ and let p be a prime $>$ max $(|a_0|, 2|u_1|, \ldots, 2|u_n|)$. Then there exists an integer N_p not divisible by p and a polynomial $g_p(x) \in \mathbb{Z}[x]$* of degree $< tp$ *such that the inequalities* (68) *hold.*[14]

[redacted]

as in Lemma 3. The numbers $\eta_j(u_i)$, $\eta_j \in G = \mathrm{Gal}\, K/\mathbb{Q}$, are also roots of $f(x)$. Hence, by Lemma 3, for all sufficiently large primes p there exists an integer N_p not divisible by p and an integral polynomial $g_p(x)$ of degree $< pt$, $t = \deg f$, such that $|N_p e^{\eta_j(u_i)} - p g_p(\eta_j(u_i))| < 2M^p/(p-1)!$ for all $i = 1, \ldots, n$, $j = 1, \ldots, r\,(= |G|)$. Now let k be a positive integer such that $k u_i^l$ is an algebraic integer for every u_i and every $l \leq t$. The existence of such a k is assured by Theorem 4.24. Then $k^p g_p(u_i)$ is an algebraic integer and hence every $k^p g_p(\eta_j(u_i))$ is an algebraic integer. Also $\sum_{j=1}^{r} k^p g_p(\eta_j(u_i))$ is an algebraic integer, but since it is fixed by G, it is a rational number. Hence this is an integer, by Theorem 4.23.

Now we have

[redacted]

[redacted]

where M is as before and L is a positive upper bound for the $|v_i|$, $1 \leq i \leq n$. The numbers $pk^p v_i \sum_{j=1}^{r} g_p(\eta_j(u_i))$ are integers divisible by p whereas N_p is not. Moreover, if p is sufficiently large then $p \nmid k$ and $p \nmid v_0$ so $p \nmid k^p v_0$. Hence the left-hand side of the inequality

[redacted]

1. Show that $\sin u$ is transcendental for all algebraic $u \neq 0$. (*Hint*: Use $\sin u = (1/2i)(e^{iu} - e^{-iu})$ and the transcendence of e^{iu}.)

2. Show that $\csc u$, $\cos u$, $\sec u$, $\tan u$, $\cot u$ are transcendental for any algebraic $u \neq 0$.

3. Let m be an integer without square factors and let $F = \mathbb{Q}(\sqrt{m})$, the subfield of $\mathbb{C}$ generated by $\sqrt{m}$. Show that F is the set of complex numbers of the form $a + b\sqrt{m}$ where $a, b \in \mathbb{Q}$. Let I be the subset of F of integral algebraic numbers. Show that I is a subring of $\mathbb{C}$ and I is the set of elements $a + b\sqrt{m}$ where a and b are rational numbers such that

[redacted]

We shall now apply the results of Galois theory to derive the main facts about finite fields. We observe first that if F is a finite field then $|F| = p^n$ for some prime p. To begin with we know that the prime field of F can be identified with a field $\mathbb{Z}/(p)$ of residues modulo p for some prime p. We may now regard F as a vector space over $\mathbb{Z}/(p)$ in the usual way. Clearly $[F:\mathbb{Z}/(p)]$ is finite and if $[F:\mathbb{Z}/(p)] = n$, then we have a base $(u_1, u_2, \ldots, u_n)$ for $F/(\mathbb{Z}/(p))$, and every element of F can be written in one and only one way as a linear combination $a_1u_1 + a_2u_2 + \cdots + a_nu_n$, $a_i \in \mathbb{Z}/(p)$. Evidently, this implies that $|F| = p^n$. The same method shows that if $E \supset F$, $[E:F] = n$, and $|F| = q < \infty$ then $|E| = q^n$.

The basic facts on finite fields can now be derived very quickly. We have first

$x^q - x$ in F. We observe first that since $(x^q - x)' = -1$, $x^q - x$ has q distinct roots in F. Next we shall show that $R = \{u_1, u_2, \ldots, u_q\}$ is a subfield of F. For, using the nice binomial theorem $(a + b)^p = a^p + b^p$ for characteristic p, we see that for any i and j, $(u_i \pm u_j)^q = u_i^q \pm u_j^q = u_i \pm u_j$. Hence $u_i \pm u_j \in R$. Also $1 \in R$ and $(u_i u_j)^q = u_i^q u_j^q = u_i u_j \in R$, and if $u_i \neq 0$, then $(u_i^{-1})^q = (u_i^q)^{-1} = u_i^{-1}$. These results show that R is a subfield of F. Then R contains the prime field P and $R = P(R) = F$.

Next let F and F' be two fields such that $|F| = q = |F'|$. Clearly this implies that both F and F' are extensions of $P = \mathbb{Z}/(p)$. Let F^* be the set of non-zero elements of F, so that F^* is a group under multiplication and $|F^*| = q - 1$. Hence if $u \neq 0$ in F then $u^{q-1} = 1$ and $u^q = u$. Since the last relation holds also for $u = 0$, we see that every element of F is a root of $x^q - x$. Since this equation has no more than q distinct roots in any field it is clear that F is a splitting field over P of $x^q - x$. The same is true of F'. Hence the isomorphism theorem for splitting fields (Theorem 4.4, p. 227) implies that F and F' are isomorphic. □

[redacted]

[redacted]

We shall now consider the relative theory of finite fields, that is, we want to study a finite field relative to a subfield. Let $|F| = q(=p^m)$ and let E be an extension field of F with $[E:F] = n$. Then, as we saw before, $E = q^n$. We have seen also that $a \to a^p$ is an automorphism of E (section 4.4). Hence $\eta: a \to a^q$ is an automorphism of E. Moreover, since $|F| = q$, $b^q = b$ for $b \in F$. Hence $\eta \in$ Gal E/F. We now have

[redacted]

Proof. We show first that the order $o(\eta) = n$. For, $|E| = q^n$ so $a^{q^n} = a$ for all $a \in E$. Thus $\eta^n = 1$ and if $\eta^{n'} = 1$ for $0 < n' < n$ then $a^{q^{n'}} = a$. This would contradict the fact that the polynomial $x^{q^{n'}} - x$ has no more than $q^{n'}$ roots in E. Hence $o(\eta) = n$ and $|\langle \eta \rangle| = n$. Let $F' = \text{Inv}\,\langle \eta \rangle$. By the Fundamental Theorem of Galois Theory, we know that $[E:F'] = n$ and $\text{Gal}\,E/F' = \langle \eta \rangle$. On the other hand, since $\eta \in \text{Gal}\,E/F$, $F \subset F' = \text{Inv}\,\langle \eta \rangle$. Since $n = [E:F] = [E:F'][F':F] = n[F':F]$ we have $F' = F$ and so E is Galois over F with $\text{Gal}\,E/F = \langle \eta \rangle$. □

[redacted]

Suppose K is a subfield of E/F. Then $m = [K:F] | n = [E:F]$. On the other hand, let m be any divisor of n. Then the cyclic group Gal E/F has one and only one subgroup of order n/m. Hence, by the Fundamental Theorem of

[redacted]

where the product is taken over all monic irreducible polynomials of degrees dividing n. Since $x^{q^n} - x$ has no multiple roots and hence no multiple factors in $F[x]$, it suffices to show that a monic irreducible polynomial $g(x)$ is a factor of $x^{q^n} - x$ if and only if its degree m is a divisor of n. Let $g(x)$ be a monic irreducible factor of $x^{q^n} - x$ in $F[x]$, deg $g(x) = m$, and let E be an extension field of F with $[E:F] = n$. Then E is a splitting field over F of $x^{q^n} - x$ and hence E contains a root r of $g(x)$. Then $g(x)$ is the minimum polynomial of r over F. Hence $F(r)$ is a subfield of E/F such that $[F(r):F] = m$. Then $m|n$. Conversely, let $g(x)$ be a monic irreducible polynomial in $F[x]$ of degree $m|n$. Then $K' = F[x]/(g(x))$ is an extension field of F with $|K'| = q^m$. Since $m|n$, K' is isomorphic to a subfield K of E/F. Then E contains an element r whose minimum polynomial over F is $g(x)$. Since $r^{q^m} = r$, $g(x)|(x^{q^m} - x)$. This establishes the factorization (70) where $g(x)$ runs through the set of monic irreducible polynomials in $F[x]$ of degree $m|n$. Comparing the degrees of the two sides of (70) we obtain

[redacted]