GALOIS THEORY AND PRIMALITY TESTING

H.W. Lenstra, Jr.
Mathematisch Instituut
Universiteit van Amsterdam
Roetersstraat 15
1018 WB Amsterdam
The Netherlands

1. Introduction.

In this paper we show how Galois theory for rings can be applied to the problem of distinguishing prime numbers from composite numbers. It develops ideas that were first formulated in [11, Section 8; 12].

A positive integer n is prime if and only if the ring $\mathbb{Z}/n\mathbb{Z}$ is a field. Many primality testing algorithms make use of extension rings A of $\mathbb{Z}/n\mathbb{Z}$ that are fields if n is prime. They depend on known properties of such fields and of the Frobenius map $A \to A$ that sends every $x \in A$ to its n-th power. If n is composite then usually one of these properties is found not to be satisfied, and one is finished. If one does not succeed in proving n composite in this way then the problem suggests itself how to prove that n is *prime*. Only after this proof has been completed one knows that the rings one works with are actually fields; in particular, this fact may not be used in the proof. It is for this reason that Galois theory for rings rather than for fields is needed.

Galois theory for rings can be found in [4; 6, Chapter III]. For the convenience of the reader we prove in Section 2 all facts from this theory that we need, starting only from basic properties of tensor products, localizations, and projective modules [1; 2]. In Section 3 we restrict to *finite* rings and *abelian* Galois groups, and we treat the *Artin symbol*, which replaces the Frobenius map. Section 4 is devoted to a special class of extensions of $\mathbb{Z}/n\mathbb{Z}$, which we call *cyclotomic* extensions. These play an important role in primality testing. In Section 5 we prove a result about Gauss sums that can be viewed as a generalization of [5, Theorem (7.8)], and we show how to interpret this result in terms of Artin symbols.

The application to primality testing occupies Section 6. We describe a test that is closely related to the methods of [3], as generalized by Williams (see [14] for references). The second test that we describe is an improvement of the method proposed in [5]. Finally, we show how the theory presented in this paper can be used to combine the two tests. It may be expected that this combined method, once implemented, will perform better than any existing primality testing algorithm.

By *ring* we mean in this paper *commutative ring with unit element*. The unit element is preserved by ring homomorphisms, and it is contained in subrings. If R is a ring, an *R-algebra* is a ring A together with a ring homomorphism $R \to A$. A group G is

said to *act* on an R-algebra A if G acts on the underlying set of A in such a way that for each $\sigma \in G$ the map $A \to A$ sending x to σx is an R-algebra homomorphism. In this situation we write A^G for the sub-R-algebra $\{x \in A: \sigma x = x \text{ for all } \sigma \in G\}$ of A. The unit group of a ring R is denoted by R^*. If x belongs to a multiplicative group, we write $\langle x \rangle$ for the subgroup generated by x. The cardinality of a set S is denoted by $\#S$.

2. Galois theory for rings.

In this section R denotes a ring, A an R-algebra, and G a group that acts on A.

(2.1) Definition. We call A a *Galois extension of* R *with group* G, or *Galois over* R *with group* G, if the following two conditions are satisfied:

(i) as an R-module, A is finitely generated projective of constant non-zero rank;

(ii) the A-algebra homomorphism $A \otimes_R A \to \Pi_{\sigma \in G} A$ sending $a \otimes b$ to $((\sigma a)\cdot b)_{\sigma \in G}$ is an isomorphism; here $A \otimes_R A$ is an A-algebra via the second factor, and the A-algebra operations on $\Pi_{\sigma \in G} A$ are componentwise.

Notice that from (i) it follows that the map $R \to A$ is *injective*, and that A has rank $\#G$ by (ii). If $R \neq 0$ then (ii) implies that distinct elements of G have distinct actions on A, so that G may be considered as a subgroup of $\mathrm{Aut}_R(A)$.

(2.2) Remark. Suppose that R is semi-local or, more generally, a ring over which every finitely generated projective module of constant rank is free [2, II.5.3, Proposition 5]. Then (i) and (ii) imply that there exist $z_1, z_2, \ldots, z_t \in A$ such that

(iii) $A = \Sigma_{i=1}^t Rz_i$, and the map $R \to A$ is injective;

(iv) $t = \#G$, and $\det(\sigma z_i)_{\sigma \in G,\ 1 \le i \le t} \in A^*$.

Conversely, (iii) and (iv) imply (i) and (ii) since the z_i must be independent: if $\Sigma_{i=1}^t r_i z_i = 0$ with $r_i \in R$ then $\Sigma_{i=1}^t r_i \sigma z_i = 0$ for all $\sigma \in G$ so $r_i = 0$ by (iv).

(2.3) Examples. (a) Let $A = R^t$ for some $t > 0$, and let G be any group of order t permuting the coordinates transitively. Then A is Galois over R with group G. Such a Galois extension is said to be *totally decomposed*. This example shows that the group G need not be uniquely determined by R and A.

(b) If K is a field and L is a finite Galois extension of K with Galois group G in the sense of field theory, then L is Galois over K with group G in the sense of (2.1).

(c) Suppose, in the situation of (b), that K and L are algebraic number fields, with rings of integers A_K and A_L. Let I be an ideal of A_K that is relatively prime to the discriminant of L over K. Then A_L/IA_L is Galois over A_K/I with group G.

(d) If A_i is Galois over R with group G_i, for $i = 0, 1$, then $A_0 \otimes_R A_1$

is Galois over R with group $G_0 \times G_1$.

(2.4) Base change and localization. Let B be any R-algebra. Then the action of G on A induces an action of G on the B-algebra $A \otimes_R B$, and if A is Galois over R with group G then $A \otimes_R B$ is Galois over B with group G. In particular, if A is Galois over R with group G then A_P is Galois over R_P with group G, for every prime ideal P of R. Conversely, if A_P is Galois over R_P with group G for every prime ideal P of R, and A is finitely generated as an R-module, then A is Galois over R with group G (cf. [2, II.5.2, Théorème 1]).

(2.5) Proposition. The R-algebra A is Galois over R with group G if and only if there exists an R-algebra B such that:
(i) as an R-module, B is finitely generated projective of constant non-zero rank;
(ii) $A \otimes_R B$ is a totally decomposed Galois extension of B with group G.

Proof. For the "only if"-part it suffices to take $B = A$. For the "if"-part, we need from (i) only that B is faithfully flat over R (see [2, I.3.1 and I.2.4(1)]) and from (ii) only that $A \otimes_R B$ is Galois over B with group G; the assertions then follow from [2, I.3.6, Proposition 12 and I.3.1, Proposition 2]. This proves (2.5).

(2.6) Proposition. Let A be Galois over R with group G. Then we have:
(a) $A^G = R$;
(b) if H is any subgroup of G, then A is Galois over A^H with group H;
(c) if H is any normal subgroup of G, then A^H is Galois over R with group G/H.

Proof. If the Galois extension is totally decomposed it is straightforward to verify these assertions. In the general case one chooses B as in (2.5) to reduce the proof to the previous case. It then remains to verify that the natural map $A^H \otimes_R B \to (A \otimes_R B)^H$ is an isomorphism. To do this, one considers the exact sequence of R-modules $0 \to A^H \to A \to \prod_{\sigma \in H} A$ in which the last map sends a to $(a - \sigma a)_{\sigma \in H}$. Since B is flat over R, the sequence remains exact upon tensoring with B over R, as required. This proves (2.6).

(2.7) Proposition. Suppose that A is Galois over R with group G. Let I be an ideal of A and $H = \{\sigma \in G: \sigma I = I\}$. Then we have:
(a) A/I is Galois over $A^H/(I \cap A^H)$ with group H;
(b) as an ideal, I is generated by $I \cap A^H$;
(c) if $A/I \neq 0$, then distinct elements of H have distinct actions on A/I.

Proof. Since A is Galois over A^H with group H, we may as well assume, by change of notation, that $G = H$ and $R = A^H$. Further, by localizing with respect to prime ideals of R containing $I \cap R$, we may assume that A is free as an R-module. Let $z_1, z_2, \ldots, z_t \in A$ be as in (2.2)(iii), (iv). Then (2.2)(iii), (iv) is also valid with R, A, z_i replaced by $R/(I \cap R)$, A/I, $(z_i \bmod I)$, and (a) follows.

Assertion (c) is generally true for non-zero Galois extensions, as we noted after (2.1). To prove (b), let J be the ideal of A generated by $I \cap R$. Then there is a surjective map $A/J \to A/I$. Since A/J and A/I are free over $R/(I \cap R)$ of the same rank, this map must be an isomorphism, so $J = I$. This proves (2.7).

(2.8) Proposition. Suppose that $R \neq 0$, and let A_i be a Galois extension of R with group G_i, for $i = 0, 1$. Let $f: A_0 \to A_1$ be an R-algebra homomorphism such that for every $\sigma \in G_1$ there exists $\tau \in G_0$ with $f\tau = \sigma f$. Then for every $\sigma \in G_1$ there exists a *unique* $\tau \in G_0$ with $f\tau = \sigma f$, and the map $\psi: G_1 \to G_0$ that maps σ to τ if $f\tau = \sigma f$ is a group homomorphism. Moreover, the image of f is equal to $A_1^{\ker \psi}$, and this is a Galois extension of R with group $\psi[G_1]$.

Proof. The uniqueness of τ for given σ follows from (2.7)(c), with $A = A_0$, $I = \ker f$. It is trivial that ψ is a group homomorphism, and that $f[A_0]$ is contained in $A_1^{\ker \psi}$. From (2.7)(a), with R and G replaced by $A_0^{\psi[G_1]}$ and $\psi[G_1]$, we see that $f[A_0]$ is Galois over $f[A_0^{\psi[G_1]}]$ with group $\psi[G_1]$. But $R \subset f[A_0^{\psi[G_1]}] \subset A_1^{G_1} = R$, so $f[A_0^{\psi[G_1]}] = R$, and the rings $f[A_0]$ and $A_1^{\ker \psi}$ are both Galois over R with the same group $\psi[G_1] \cong G_1/\ker \psi$.

To prove that $f[A_0] = A_1^{\ker \psi}$ it now suffices to show that if A' and A'' are Galois over R with the *same* group G, and there is an inclusion $A' \subset A''$ respecting the G-action, then $A' = A''$. By a base change as in (2.5) this is reduced to the case that both Galois extensions are totally decomposed, and by localization to the case that R has no idempotents except 0 and 1, and $0 \neq 1$. Then each of A' and A'' has precisely $2^{\#G}$ idempotents, so all idempotents of A'' lie in A'. Since A'', as an R-module, is spanned by its idempotents this implies that $A' = A''$. This proves (2.8).

(2.9) Proposition. Suppose that R has no idempotents except 0 and 1, with $0 \neq 1$, and that A is Galois over R with an *abelian* group G. Then any R-algebra homomorphism $\tau: A \to A$ satisfying $\tau\sigma = \sigma\tau$ for all $\sigma \in G$ belongs to G.

Proof. First suppose that the Galois extension is totally decomposed. Then we may identify A with $\prod_{\rho \in G} R$, the G-action on the latter algebra being given by $\sigma((r_\rho)_{\rho \in G}) = (r_{\rho\sigma})_{\rho \in G}$, for $\sigma \in G$. Considering the idempotents of A one easily proves that any R-algebra homomorphism $\tau: A \to A$ is given by $\tau((r_\rho)_{\rho \in G}) = (r_{f(\rho)})_{\rho \in G}$, for some set-theoretic map $f: G \to G$. If moreover $\tau\sigma = \sigma\tau$ for all $\sigma \in G$ then f commutes with right multiplication by σ, for any σ, so $f(\rho) = f(1 \cdot \rho) = f(1) \cdot \rho$. Then f is left multiplication by $f(1)$, and since G is abelian this implies that $\tau = f(1) \in G$.

In the general case we choose B as in (2.5) such that the rank of B is as small as possible. Suppose that $B \cong B_0 \times B_1$ for certain rings B_i. Then each B_i is a finitely generated projective R-module, and by our assumption on R it is of constant rank [2, II.4.3, Corollaire 2 to Proposition 15]. Also, $A \otimes_R B_i$ is totally

decomposed over B_i, for $i = 0, 1$. Our minimality assumption on the rank now implies that one B_i equals B and the other is zero. Hence the ring B has exactly two idempotents, and the first part of the proof applies. This proves (2.9).

(2.10) Galois extensions of finite rings. In the sequel we are only interested in the case that R is *finite*, for example $R = \mathbb{Z}/n\mathbb{Z}$ for some positive integer n. In this case the Galois extensions have been completely classified. Since we do not need this classification we give it without proof.

First let R be a finite field, for example $R = \mathbb{Z}/n\mathbb{Z}$ with n prime, and denote by L an algebraic closure of R. Let G be a finite group, and fix an element $\tau \in G$. Define the subring A of $\prod_{\rho \in G} L$ by

$$A = \{(x_\rho)_{\rho \in G}: \ x_{\tau\rho} = x_\rho^{\#R} \text{ for all } \rho \in G\}.$$

Notice that A, as a ring, is isomorphic to the product of $\#G/\langle\tau\rangle$ copies of a field of order $(\#R)^{\#\langle\tau\rangle}$. We let G act on A by $\sigma((x_\rho)_{\rho \in G}) = (x_{\rho\sigma})_{\rho \in G}$. Then A is Galois over R with group G. Moreover, if τ ranges over all elements of G, up to conjugacy, then all Galois extensions of R with group G are obtained in this way, up to isomorphism.

Next let R be a finite local ring, with maximal ideal M; for example, $R = \mathbb{Z}/n\mathbb{Z}$ where $n = r^k$ with r prime and $k \geq 1$, in which case $R/M \cong \mathbb{Z}/r\mathbb{Z}$. If A is Galois over R with group G, then A/MA is Galois over the field R/M, by (2.4). Conversely, if B is Galois over R/M with group G, then there is a Galois extension A of R with group G, unique up to isomorphism, such that $A/MA \cong B$ as Galois extensions of R/M.

Finally, let R be an arbitrary finite ring. We can write R as the product of finitely many finite local rings R_i, see [1, Chapter 8]. For example, if $n = \prod r^{k(r)}$, with r ranging over a finite set of primes and $k(r) > 0$ for each r, then $\mathbb{Z}/n\mathbb{Z} \cong \prod \mathbb{Z}/r^{k(r)}\mathbb{Z}$. Now the Galois extensions A of R with group G are uniquely of the form $\prod A_i$, where each A_i is Galois over R_i with group G.

3. The Artin symbol.

In this section R denotes a *finite* ring, and A a Galois extension of R with an *abelian* group G.

(3.1) Let M be a maximal ideal of R. Then A/MA is Galois over R/M with group G, and the map $\tau: A/MA \to A/MA$ defined by $\tau(x) = x^{\#R/M}$ is an R/M-algebra endomorphism of A/MA that commutes with all elements of G. From (2.9) we therefore see that τ belongs to G. This element is called the *Artin symbol* of M, notation: ϕ_M. We have $\phi_M x \equiv x^{\#R/M} \bmod MA$ for all $x \in A$, and this property characterizes ϕ_M as an element of G. (It does not in general characterize ϕ_M as an element of $\mathrm{Aut}_R(A)$.)

The *Grothendieck group* $G(R)$ is defined by generators and relations. There is one generator $[Q]$ for each finite R-module Q, and one relation $[Q] = [Q'] + [Q'']$ for

each exact sequence $0 \to Q' \to Q \to Q'' \to 0$ of finite R-modules. Each finite R-module Q has a sequence of submodules $Q = Q_0 \supset Q_1 \supset \ldots \supset Q_k = \{0\}$ such that for each i with $0 \le i < k$ there is a maximal ideal M of R for which $Q_i/Q_{i+1} \cong R/M$. Using this fact one proves that $G(R)$ is a free abelian group with independent generators $[R/M]$, one for each maximal ideal M of R.

We conclude from the above that there is a unique group homomorphism $\phi\colon G(R) \to G$ for which $\phi([R/M]) = \phi_M$ for each M. We call ϕ the *Artin map*, and its image $\phi[G(R)]$ in G the *decomposition group* of the Galois extension, notation: D. This is a subgroup of G. The element $\phi([R])$ of D is called the *Artin symbol* of the Galois extension, notation: ϕ_R.

(3.2) Examples. (a) Let n be a positive integer. We are mainly interested in the case that R is equal to the ring $\mathbb{Z}/n\mathbb{Z}$, which we denote by n. The set of primes r dividing n is in bijective correspondence with the set of maximal ideals M of n, by $M = rn$. This allows us to identify $G(n)$ with the multiplicative subgroup of $\mathbb{Q}^*$ generated by the primes dividing n, so that $[Q] \in G(n)$ is identified with $\#Q \in \mathbb{Q}^*$, for each finite n-module Q. With this convention, we write ϕ_x instead of $\phi(x)$, so that $\phi_r = \phi_{rn}$ and $\phi_n = \phi_R$.

(b) Let n and n be as in (a), and let L be a quadratic number field whose discriminant Δ over $\mathbb{Q}$ is relatively prime to n. Denote by A_L the ring of integers of L, and $A = A_L/nA_L$. From (2.3)(c) we see that A is Galois over n with a group G of order 2; let this group be identified with $\{\pm 1\}$. One easily checks that for $x \in G(n)$ we have $\phi_x = \left(\frac{\Delta}{x}\right)$; here $\left(\frac{\Delta}{\cdot}\right)$ is the Kronecker symbol, extended to $G(n)$ by multiplicativity. In particular we have $\phi_n = \left(\frac{\Delta}{n}\right)$.

(c) Let n and s be two positive integers with $\gcd(n, s) = 1$, and $n = \mathbb{Z}/n\mathbb{Z}$. Denote by ζ_s a primitive s-th root of unity in an extension field of $\mathbb{Q}$. By (2.3)(c) the ring $A = \mathbb{Z}[\zeta_s]/n\mathbb{Z}[\zeta_s]$ is Galois over n with group $(\mathbb{Z}/s\mathbb{Z})^*$, where $(x \bmod s) \in (\mathbb{Z}/s\mathbb{Z})^*$ acts on A by raising ζ_s to the power x. For $x \in G(n)$ we have $\phi_x = (x \bmod s)$; even for non-integral x this is a well-defined element of $(\mathbb{Z}/s\mathbb{Z})^*$, since x is built up from primes not dividing s. In particular we see that D is generated by $\{r \bmod s\colon r \text{ is a prime dividing } n\}$, and that $\phi_n = (n \bmod s)$.

(d) Suppose that A_i is Galois over R with abelian group G_i, for $i = 0, 1$. Denote by $\phi^{(i)}\colon G(R) \to G_i$ the Artin map and by $\phi_R^{(i)} \in G_i$ the Artin symbol. Then for the Galois extension $A = A_0 \otimes_R A_1$ of R with group $G = G_0 \times G_1$ the Artin map $\phi\colon G(R) \to G$ is given by $\phi(x) = (\phi^{(0)}(x), \phi^{(1)}(x))$, and the Artin symbol $\phi_R \in G$ equals $(\phi_R^{(0)}, \phi_R^{(1)})$.

(3.3) Remark. Suppose that $R = \mathbb{Z}/n\mathbb{Z}$ for some positive integer n. If we wish to calculate the Artin symbol ϕ_n of a Galois extension from its definition, then we need to know the prime factorization of n. But there are cases, such as examples (b) and (c) above, in which one can calculate ϕ_n without this information. It would be interesting to know how generally this can be done.

(3.4) Proposition. Let R be a finite non-zero ring, and A_i a Galois extension of R with an abelian group G_i, for $i = 0, 1$. Denote by $\phi^{(i)}: G(R) \to G_i$ the Artin map, by D_i the decomposition group in G_i, and by $\phi_R^{(i)} \in D_i$ the Artin symbol, for $i = 0, 1$. Let $f: A_0 \to A_1$ be an R-algebra homomorphism such that for every $\sigma \in G_1$ there exists $\tau \in G_0$ with $f\tau = \sigma f$, and let $\psi: G_1 \to G_0$ be the group homomorphism from (2.8). Then we have

$$\phi^{(0)} = \psi \circ \phi^{(1)}, \qquad D_0 = \psi[D_1], \qquad \phi_R^{(0)} = \psi(\phi_R^{(1)}).$$

Proof. Suppose first that R is a field. Then $\phi_R^{(i)}(x) = x^{\#R}$ for all $x \in A_i$, so $f\phi_R^{(0)} = \phi_R^{(1)} f$. By the definition of ψ this means that $\psi(\phi_R^{(1)}) = \phi_R^{(0)}$.

In the general case, let M be a maximal ideal of R and denote by $\phi_M^{(i)}$ the Artin symbol of M in G_i. By the previous case, with R/M in the role of R, we have $\psi(\phi_M^{(1)}) = \phi_M^{(0)}$. The assertions of (3.4) now follow immediately. This proves (3.4).

(3.5) Corollary. Let $H \subset G$ be a subgroup. Then the composite of the Artin map $G(R) \to G$ and the natural map $G \to G/H$ is the Artin map for the Galois extension A^H of R with group G/H.

Proof. Apply (3.4) to $A_0 = A^H$ and $A_1 = A$, with $f: A_0 \to A_1$ the inclusion map. This proves (3.5).

(3.6) Remark. Let H be a subgroup of G. If R is a *field*, or a local ring, then the decomposition group for the Galois extension A of A^H with group H is equal to $H \cap D$. For general R the group $H \cap D$ may be bigger. It is true in general that the Artin symbol ϕ_{AH} for the Galois extension A of A^H with group H is equal to $\phi_R^{\#G/H}$.

The following proposition explains the name "decomposition group".

(3.7) Proposition. Suppose that $R \neq 0$. Let H be a subgroup of G, and $B = A^H$. Then the following three assertions are equivalent:

(i) $D \subset H$;

(ii) the Galois extension B of R with group G/H is totally decomposed;

(iii) there is an R-algebra homomorphism $B \to R$.

Proof. The implication (ii) $\Rightarrow$ (iii) is obvious. To prove (iii) $\Rightarrow$ (i) one applies (3.4) to $A_0 = B$ and $A_1 = R$. Then one finds that the decomposition group D_0 is trivial, so (3.5) implies that $D \subset H$.

Finally we prove (i) $\Rightarrow$ (ii). By change of notation we may assume that $A = B$, so that F is trivial. By (i), the group D is trivial as well.

First assume that R is a field, and let N be a maximal ideal of A. Since D is trivial we have $x^{\#R} = x$ for all $x \in A$, so the field A/N satisfies $\#A/N \leq \#R$. It contains R, so $A/N \cong R$. From (2.7)(b) one deduces that the natural map $A \to \prod_{\sigma \in G} A/\sigma N \cong \prod_{\sigma \in G} R$ is injective, so by a counting argument it is bijective. This proves (ii) if R is a field.

Next let R be a local ring with a nilpotent maximal ideal M. We claim that each idempotent of A/MA can be lifted in a unique way to an idempotent of A. To prove this, let $(e \bmod MA) \in A/MA$ be idempotent. Since A is finite there exist integers k, ℓ with $k > \ell \geq 0$ for which $e^{2^k} = e^{2^\ell}$. Then $e^{2^k - 2^\ell}$ is idempotent, and $e^{2^k-2^\ell} \equiv e \bmod MA$. If e_0 and e_1 are idempotent then we have $(e_1 - e_0)^3 = e_1^3 - 3e_1^2e_0 + 3e_1e_0^2 - e_0^3 = e_1 - e_0$; if also $e_0 \equiv e_1 \bmod MA$ then this implies $e_1 - e_0 = 0$, because MA is nilpotent. This proves our claim.

By the case already dealt with there is an isomorphism $A/MA \cong \prod_{\sigma \in G} R/M$ of R/M-algebras. Let the idempotents corresponding to this decomposition be lifted to A. By the uniqueness statement this gives rise to a collection of idempotents that annihilate each other, are transitively permuted by G, and add up to 1. Hence $A \cong \prod_{\sigma \in G} R'$ for some R-algebra R'. Since the map $R \to A$ is injective the same is true for $R \to R'$. By a counting argument we now have $R \cong R'$ as R-algebras, and (ii) follows.

Since any finite ring can be written as the product of finitely many local rings with nilpotent maximal ideals, see [1, Chapter 8], the general case follows immediately. This proves (3.7).

(3.8) Proposition. The ring A is a field if and only if R is a field and $G = \langle \phi_R \rangle$.

Proof. The "only if"-part is easy. To prove the "if"-part, let N be a maximal ideal of A. From $\phi_R x = x^{\#R}$, for all $x \in A$, we see that $\phi_R N = N$, so by (2.7)(b) the ideal N is generated by $N \cap A^G = N \cap R$. Hence $N = 0$ and $A \cong A/N$ is a field. This proves (3.8).

4. Cyclotomic extensions.

In this section we fix an integer n with $n > 1$. We denote the ring $\mathbb{Z}/n\mathbb{Z}$ by n, and we use the notation introduced in (3.2)(a). Further, we let t be a positive integer with $\gcd(t, n) = 1$ and we let u be the order of $(n \bmod t)$ in the group $(\mathbb{Z}/t\mathbb{Z})^*$. By Φ_t we denote the t-th cyclotomic polynomial.

(4.1) Definition. A *t-th cyclotomic extension* of n is an n-algebra A together with an automorphism σ of A and an element ζ of A, such that the following conditions are satisfied:

(i) A is Galois over n with group generated by σ;

(ii) $\Phi_t(\zeta) = 0$ and $\sigma\zeta = \zeta^n$;

(iii) $\sigma^u = \mathrm{id}_A$.

It is well-known that such extensions exist for any t if n is prime. If $\langle n \bmod t \rangle = (\mathbb{Z}/t\mathbb{Z})^*$, then $A = \mathbb{Z}[\zeta_t]/n\mathbb{Z}[\zeta_t]$ is a t-th cyclotomic extension of n, with $\zeta = (\zeta_t \bmod n)$ and $\sigma\zeta = \zeta^n$. These observations are generalized in the following proposition.

(4.2) Proposition. A t-th cyclotomic extension of n exists if and only if for each divisor r of n there exists an integer i with $r \equiv n^i \bmod t$. Moreover, if A, σ, ζ constitute a t-th cyclotomic extension of n, then we have:

(a) σ equals the Artin symbol ϕ_n of the extension, and σ has order u;

(b) if $r \in G(n) \subset \mathbb{Q}^*$, and $i \in \mathbb{Z}$, then $r \equiv n^i \bmod t$ if and only if $\phi_r = \sigma^i$;

(c) $A = n[\zeta]$.

Proof. To prove the "if"-part, suppose that $(r \bmod t) \in \langle n \bmod t \rangle$ for all divisors r of n. Then the decomposition group D_0 of the Galois extension $A_0 = \mathbb{Z}[\zeta_t]/n\mathbb{Z}[\zeta_t]$ of n with group $(\mathbb{Z}/t\mathbb{Z})^*$ equals $\langle n \bmod t \rangle$, see (3.2)(c). By (3.7) there is now a ring homomorphism $B = A_0^{\langle n \bmod t \rangle} \to n$. Let $A = A_0 \otimes_B n$ and ζ the image of ζ_t in A. Since A_0 is Galois over B with group $\langle n \bmod t \rangle$ the same is true for A over n. It follows that A, together with the action of $(n \bmod t)$ and the element $\zeta \in A$, is a t-th cyclotomic extension of n.

Conversely, let A, σ, ζ be as in (4.1)(i), (ii), (iii), and let A_0 be as above. The ring homomorphism $f: A_0 \to A$ sending $(\zeta_t \bmod n)$ to ζ then satisfies the conditions of (2.8), with $A_1 = A$, and the group homomorphism $\psi: \langle\sigma\rangle \to (\mathbb{Z}/t\mathbb{Z})^*$ from (2.8) maps σ to $(n \bmod t)$. From (4.1)(iii) we now see that ψ is injective and that σ has order u. By (2.8) the injectivity of ψ implies that f is surjective, which is (c). Further, (3.4) and (3.2)(c) imply that $\psi(\phi_n) = (n \bmod t) = \psi(\sigma)$, so $\sigma = \phi_n$. This proves (a). Finally, in the situation of (b) the assertions $r \equiv n^i \bmod t$ and $\phi_r = \sigma^i$ are both equivalent to $\psi(\phi_r) = \psi(\sigma)^i$. This proves both (b) and the "only if"-part of the first assertion.

This proves (4.2).

From (4.2) we see that the existence of a t-th cyclotomic extension implies the existence of a t_1-th cyclotomic extension for each divisor t_1 of t. One can also prove this directly by raising ζ to the power t/t_1 and applying the following result.

(4.3) Proposition. Let A be an n-algebra, σ an automorphism of A and ζ an element of A such that conditions (i) and (ii) of (4.1) are satisfied. Then $n[\zeta]$, together with the restriction of σ to $n[\zeta]$ and the element ζ, is a t-th cyclotomic extension of n.

Proof. This easily follows from (2.8) with A_0 as above, $A_1 = A$, and $f(\zeta_t \bmod n) = \zeta$. This proves (4.3).

(4.4) Proposition. Let A be a Galois extension of n with a cyclic group $\langle\sigma\rangle$ of order u. Suppose that for each prime divisor q of t there exists $\alpha = \alpha_q \in A$ such that $\sigma\alpha = \alpha^n$ and such that

$$\alpha \notin rA, \qquad \alpha^{(n^u-1)/q} - 1 \notin rA$$

for each prime r dividing n. Put $\zeta = \prod_q \alpha_q^{(n^u-1)/q^{m(q)}}$, where $m(q)$ is the number of factors q in t. Then A, σ, ζ is a t-th cyclotomic extension of n.

Proof. First let q be fixed, and α as in the proposition. Let $I = \alpha A$. From $\sigma\alpha = \alpha^n$ it follows that $\sigma I \subset I$, so $\sigma I = I$ because σ has finite order. By (2.7)(d) this implies that $I = dA$ for some divisor d of n. But $I \not\subset rA$ for each prime r dividing n, so $d = 1$ and $\alpha \in A^*$. In the same way one proves that $\alpha^{(n^u-1)/q} - 1 \in A^*$. From $\sigma\alpha = \alpha^n$ and $\sigma^u = \mathrm{id}_A$ it follows that $\alpha^{n^u} = \alpha$, so $\alpha^{n^u-1} = 1$ because $\alpha \in A^*$. The element $\beta_q = \alpha^{(n^u-1)/q^{m(q)}}$ now satisfies

$$\beta_q^{q^{m(q)}} = 1, \qquad \beta_q^{q^{m(q)-1}} - 1 \in A^*,$$

so it is a zero of the $q^{m(q)}$-th cyclotomic polynomial. It follows that $\zeta = \prod_q \beta_q$ is a zero of Φ_t. The other conditions of (4.1) are clear. This proves (4.4).

(4.5) Proposition. Let the n-linear map λ from $n[X]/\Phi_t n[X]$ to itself be defined by $\lambda(X^i \bmod \Phi_t) = (X^{ni} - X^i \bmod \Phi_t)$, for $0 \le i < \deg \Phi_t$. Suppose that $h, g_1, g_2, \ldots, g_k \in n[X]$ have the following three properties:

(i) $\lambda(g_i \bmod \Phi_t) = 0$ for $1 \le i \le k$;

(ii) h has leading coefficient 1, and $0 < \deg h \le u$;

(iii) $hn[X] = \Phi_t n[X] + \Sigma_{i=1}^k g_i n[X]$ as ideals of $n[X]$.

Put $A = n[X]/hn[X]$ and $\zeta = (X \bmod h) \in A$. Then A has an automorphism σ with $\sigma\zeta = \zeta^n$, and A, σ, ζ constitute a t-th cyclotomic extension of n. Moreover, $\deg h = u$.

(4.6) Remark. To motivate this proposition we remark the following. Let first n be prime. Then one can construct a t-th cyclotomic extension of n by letting A be the field $n[X]/hn[X]$ for some irreducible factor h of Φ_t in $n[X]$, and defining σ and ζ by $\zeta = (X \bmod h)$ and $\sigma\zeta = \zeta^n$. To find h, one can apply Berlekamp's algorithm [8, Section 4.6.2; 9, Section 4] to factor the polynomial Φ_t in $n[X]$. Studying this algorithm one discovers that each irreducible factor of Φ_t produced by this algorithm is, as in (iii), of the form $\gcd(\Phi_t, g_1, g_2, \ldots, g_k)$ for certain $g_i \in n[X]$ satisfying (i). It is well-known that each irreducible factor of Φ_t in $n[X]$ has degree u.

If n is not known to be prime one can still attempt to use Berlekamp's algorithm to find a factor h of Φ_t in $n[X]$ of degree u. However, if n is not prime this attempt is not likely to be successful (except if $\langle n \bmod t \rangle = (\mathbb{Z}/t\mathbb{Z})^*$, in which case one finds $h = \Phi_t$). The above proposition asserts that *if* Berlekamp's algorithm produces a factor h as just described, then h does give rise to a t-th cyclotomic extension of n.

Proof of (4.5). There is a ring isomorphism $n[X]/\Phi_t n[X] \to A_0 = \mathbb{Z}[\zeta_t]/n\mathbb{Z}[\zeta_t]$ that maps $(X \bmod \Phi_t)$ to $(\zeta_t \bmod n)$, and it is easily seen that this isomorphism maps the kernel of λ onto the subring $B = A_0^{\langle n \bmod t \rangle}$. Denote by $h(\zeta_t)$, $g_i(\zeta_t)$ the images of h, g_i in A_0, so that $A = A_0/h(\zeta_t)A_0$. From $A = A_0/\Sigma_{i=1}^k g_i(\zeta_t)A_0$ and $g_i(\zeta_t) \in B$ we see that $A = A_0 \otimes_B B'$, where B' denotes the image of B in A. Hence A is Galois over B' with group $\langle n \bmod t \rangle$; in particular, A is free of rank u as a

B'-module. But (ii) implies that A is free of rank deg h ≤ u as a module over the subring n of B'. Counting A shows that we must have deg h = u and n = B'. This implies (4.5).

(4.7) Proposition. Let $h \in n[X]$ be a polynomial of degree u with leading coefficient 1, and $A = n[X]/hn[X]$. Assume that $\alpha = (X \bmod h)$ has the following properties:

(i) $h(\alpha^n) = 0$;

(ii) $\alpha^{n^u} = \alpha$;

(iii) $\alpha^{n^{u/p}} - \alpha \in A^*$ for every prime p dividing u.

Then A is Galois over n with group $\langle\sigma\rangle$, where $\sigma\alpha = \alpha^n$.

Proof. From (i) we see that there is a ring homomorphism $\sigma: A \to A$ with $\sigma\alpha = \alpha^n$, and from (ii) that $\sigma^u = id_A$. Further $1, \alpha, \ldots, \alpha^{u-1}$ is an n-basis for A. By (2.2) and Vandermonde's determinant it remains to prove that $\sigma^i\alpha - \sigma^j\alpha \in A^*$ for $i \not\equiv j \bmod u$. Suppose that $I = (\sigma^i\alpha - \sigma^j\alpha)A$ is different from A. By $\sigma\alpha = \alpha^n$ and $\sigma^u = id_A$ we have $\sigma I = I$, so $H = \{\tau \in \langle\sigma\rangle: \tau\alpha \equiv \alpha \bmod I\}$ is a subgroup of $\langle\sigma\rangle$ containing σ^{i-j}. By (iii) it does not contain $\sigma^{u/p}$ for any prime p dividing u. Hence H is trivial and $i \equiv j \bmod u$. This proves (4.7).

(4.8) Remark. Suppose that n is prime in (4.7). Then clearly $\sigma = \phi_n$, and A is a field by (3.8). Notice that (i) is automatically satisfied for prime n, and that (ii), (iii) constitute a well-known irreducibility test for h, see [8, Exercise 4.6.2.16; 9, Section 5].

If n is not prime we need not have $\sigma = \phi_n$, as is shown by the example $n = 35$, $f = 2$, $h = X^2 - 15X + 1$ or $h = X^2 - 14X + 1$.

5. Gauss sums.

As in the previous section, let n be an integer, $n > 1$, and write $n = \mathbb{Z}/n\mathbb{Z}$. Let further t be a positive integer with $\gcd(t, n) = 1$, and put $u = \#\langle n \bmod t\rangle$.

(5.1) Proposition. Suppose that

(i) $\gcd(t, (n^u - 1)/t) = 1$,

(ii) there exists a t-th cyclotomic extension of n.

Let t' be a positive integer satisfying

(iii) each prime factor of t' divides t, and if $t \equiv 2 \bmod 4$ then $t' \not\equiv 0 \bmod 8$.

Then a t'-th cyclotomic extension of n exists.

Proof. By the remark following (4.2) we may assume that t' is a multiple of t. Then (iii) precisely means that the kernel J of the natural map $(\mathbb{Z}/t'\mathbb{Z})^* \to (\mathbb{Z}/t\mathbb{Z})^*$ is cyclic of order t'/t. For each prime p dividing t'/t the kernel J_p of the natural map $(\mathbb{Z}/t'\mathbb{Z})^* \to (\mathbb{Z}/pt\mathbb{Z})^*$ has index p in J, so the groups J_p are exactly the maximal subgroups of J. From $n^u \equiv 1 \bmod t$ it follows that $(n^u \bmod t') \in J$,

and from $\gcd(t, (n^u - 1)/t) = 1$ that $(n^u \bmod t') \notin J_p$ for each p. Therefore $(n^u \bmod t')$ generates J, so any integer that is congruent to a power of n modulo t is congruent to a power of n modulo t'. By (4.2), this proves (5.1).

(5.2) Remark. Let t, t' be as in (5.1) with t dividing t', and let A, σ, ζ be a t-th cyclotomic extension of n. Then a t'-th cyclotomic extension of n is given by A', σ', ζ', where $A' = A \otimes_{\mathbb{Z}[\zeta_t]} \mathbb{Z}[\zeta_{t'}]$, $\zeta' = 1 \otimes \zeta_{t'}$, and σ' acting as σ on A and as $(n \bmod t')$ on $\mathbb{Z}[\zeta_{t'}]$.

(5.3) Remark. Let t satisfy (5.1)(i), (ii), and let r be a divisor of n. Then (5.1) implies that there exists $i \in \varprojlim \mathbb{Z}/(ut'/t)\mathbb{Z}$ such that $r = n^i$ in the profinite group $\varprojlim (\mathbb{Z}/t'\mathbb{Z})^*$; here both projective limits are taken over the set of multiples t' of t satisfying (5.1)(iii). We denote this value of i, which is uniquely determined, by $\ell_t(r)$. It may be thought of as a "t-adic logarithm of r to the base n". In fact, if p is an odd prime dividing t then the image of $\ell_t(r)$ under the natural projection $\varprojlim \mathbb{Z}/(ut'/t)\mathbb{Z} \to \mathbb{Z}_p$ equals $(\log_p r)/\log_p n$, where $\log_p$ is the p-adic logarithm. The same assertion holds for $p = 2$ if $t \equiv 0 \bmod 4$. Notice that $t' = t^2$ satisfies (5.1)(iii), so it is meaningful to consider $\ell_t(r)$ modulo t.

(5.4) Gauss sums. Let A, σ, ζ be a t-th cyclotomic extension of n. Let further m be a positive integer with $\gcd(n, m) = 1$, and $\chi: (\mathbb{Z}/m\mathbb{Z})^* \to \langle\zeta\rangle$ a group homomorphism that is *primitive* in the sense that it does not factor through the natural map $(\mathbb{Z}/m\mathbb{Z})^* \to (\mathbb{Z}/d\mathbb{Z})^*$ for any divisor $d < m$ of m. For $x \in G(n) \subset \mathbb{Q}^*$ we write $\chi(x) = \chi(x \bmod m)$, cf. (3.2)(a), (c).

The *Gauss sum* $\tau(\chi)$ is the element of $A \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_m]$ defined by

$$\tau(\chi) = \Sigma_y \, \chi(y) \otimes \zeta_m^y;$$

here ζ_m denotes a primitive m-th root of unity as in (3.2)(c), and y ranges over $(\mathbb{Z}/m\mathbb{Z})^*$. From the well-known formula $\tau(\chi)\tau(\chi^{-1}) = \chi(-1)m$ and $\gcd(m, n) = 1$ it follows that $\tau(\chi)$ belongs to the unit group $(A \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_m])^*$.

We let σ act on $A \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_m]$ via A, and we write the induced module structure of $(A \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_m])^*$ over the group ring $\mathbb{Z}[\langle\sigma\rangle]$ exponentially.

(5.5) Theorem. Let n and t be integers with $n > 1$, $t > 0$, $\gcd(t, n) = 1$ and $\gcd(t, (n^u - 1)/t) = 1$, where $u = \#\langle n \bmod t\rangle$. Let the further hypotheses and notations be as in (5.4). Then we have:

(a) if n is prime, then $\tau(\chi)^{1 - n/\sigma} = \chi(n)$;

(b) conversely, if $\eta \in \langle\zeta\rangle$ is such that $\tau(\chi)^{1 - n/\sigma} = \eta$, then $\eta = \chi(n)$ and $\chi(r) = \chi(n)^{\ell_t(r)}$ for each divisor r of n, with $\ell_t(r)$ as in (5.3).

Proof. Assertion (a) follows by a computation as in [5, Lemma (7.3)].

We prove (b). Let j be a positive integer. Raising $\tau(\chi)^{1 - n/\sigma} = \eta$ to the power $\Sigma_{i=0}^{j-1} (n/\sigma)^i$ and using that n/σ acts as the identity on $\langle\zeta\rangle$ we find that

$$\tau(\chi)^{1 - n^j/\sigma^j} = \eta^j.$$

Putting $j = u$ and $v = (n^u - 1)/t$ we see that the order of $\tau(\chi)$ divides $t(n^u - 1) = t^2 v$.

Let now r be a prime dividing n, and let ℓ be a positive integer congruent to $\ell_t(r)$ modulo tu, so that $n^\ell \equiv r \bmod t^2$. Putting $j = \ell$ in the above equation we find that

$$\tau(\chi)^{(1 - n^\ell/\sigma^\ell)v} = \eta^{\ell v}.$$

But $n^\ell v$ is congruent to rv modulo the order of $\tau(\chi)$, and $\sigma^\ell = \phi_r$ by (4.2)(b), so the equality simplifies to

$$\tau(\chi)^{(1 - r/\phi_r)v} = \eta^{\ell v}.$$

Since r is prime, the argument used to prove (a) leads to $\tau(\chi)^{1 - r/\phi_r} \equiv \chi(r) \bmod r$. Therefore

$$\chi(r)^v \equiv \eta^{\ell v} \bmod r.$$

The identity $\prod_{i=1}^{t-1} (1 - \zeta^i) = t$ shows that no two distinct elements of $\langle\zeta\rangle$ are congruent modulo r, cf. [5, (7.17)]. Hence $\chi(r)^v = \eta^{\ell v}$, and since by hypothesis $\gcd(t, v) = 1$ we find that we have proved

$$\chi(r) = \eta^{\ell_t(r)}$$

for each prime r dividing n. By multiplicativity, the same equality is valid for each $r \in G(n) \subset \mathbb{Q}^*$. With $r = n$ we see that $\chi(n) = \eta$, so $\chi(r) = \chi(n)^{\ell_t(r)}$ for each $r \in G(n)$.

This proves (5.5).

(5.6) We show how to interpret (5.5) in terms of Artin symbols. Let m and χ be as in (5.4). The field $\mathbb{Q}(\zeta_m)$ is Galois over $\mathbb{Q}$ with group $(\mathbb{Z}/m\mathbb{Z})^*$, and we let $L = \mathbb{Q}(\zeta_m)^{\ker \chi}$ be the subfield corresponding to $\ker \chi \subset (\mathbb{Z}/m\mathbb{Z})^*$, with ring of integers A_L. Then A_L/nA_L is Galois over n with group equal to the image of χ, by (2.3)(c). This group is cyclic of order dividing t. From (3.2)(c) and (3.5) it follows that the Artin symbol ϕ_x in this extension equals $\chi(x)$, for each $x \in G(n)$, and in particular $\phi_n = \chi(n)$. Thus we see that the conclusion of (5.5)(b) is equivalent to the assertion that, for each t' as in (5.1)(iii), the decomposition group of the Galois extension $(\mathbb{Z}[\zeta_{t'}]/n\mathbb{Z}[\zeta_{t'}]) \otimes_n (A_L/nA_L)$ of n with group $(\mathbb{Z}/t'\mathbb{Z})^* \times (\text{image } \chi)$ is generated by the Artin symbol ϕ_n of the extension.

Viewing $A \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_m]$ as a Galois extension of A with group $(\mathbb{Z}/m\mathbb{Z})^*$ one checks easily that the action of any $y \in (\mathbb{Z}/m\mathbb{Z})^*$ on the Gauss sum $\tau(\chi)$ is given by multiplication by $\chi(y)^{-1}$. This implies that $\tau(\chi)$ is a *Lagrange resolvent* for the Galois extension $A \otimes_{\mathbb{Z}} A_L$ of A with group image χ; i.e., we have $A \otimes_{\mathbb{Z}} A_L = A[\tau(\chi)]$ with $\tau(\chi)^{\#\text{image } \chi} \in A^*$, and the Galois action of any $\chi(y) \in \text{image } \chi$ on $\tau(\chi)$ is given by multiplication by $\chi(y)^{-1}$.

(5.7) We close this section with two remarks of computational interest. First, the element $\tau(\chi)^{1 - n/\sigma}$ of $A \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_m]$ belongs in fact to the subring of A generated by the image of χ. It can be expressed in terms of certain Jacobi sums that belong to that ring. One can use these expressions to calculate $\tau(\chi)^{1 - n/\sigma}$ without leaving the

ring A.

Secondly, Theorem (5.5) and its proof are also valid if throughout $\tau(\chi)$ is replaced by $w\tau(\chi)$ for some $w \in A^*$. This remark can be applied if there are divisors m_0 and m_1 of m and primitive group homomorphisms $\chi_i: (\mathbb{Z}/m_i\mathbb{Z})^* \to \langle\zeta\rangle$ for $i = 0, 1$, such that $\chi(y) = \chi_0(y \bmod m_0)\cdot\chi_1(y \bmod m_1)$ for all $y \in (\mathbb{Z}/m\mathbb{Z})^*$. In that case one has $\tau(\chi_0)\tau(\chi_1)/\tau(\chi) \in A^*$, so one may work with $\tau(\chi_0)\tau(\chi_1)$ instead of $\tau(\chi)$.

6. Applications to primality testing.

Galois theory for rings can be applied to the problem of how to recognize whether an integer $n > 1$ is prime. For background information on this problem we refer to [14; 10; 7].

Composite numbers are usually easy to recognize by means of tests that are based on Fermat's theorem and its generalizations. A single such test that n fails to pass suffices to show that n is composite, although it does not readily yield a factorization of n. However, if n passes many tests of this sort then it is very likely that n is a prime number, and the problem becomes how to *prove* that n is a prime number.

Let n be an integer, $n > 1$, put $R = \mathbb{Z}/n\mathbb{Z}$, and let $G(R) \subset \mathfrak{P}^*$ be as in (3.2) (a). Clearly, n is prime if and only if it generates $G(R)$, and if this is the case then for any Galois extension A of R with an abelian group the decomposition group D is generated by ϕ_n. To prove that n is prime, one can apply the theory from the preceding sections to show that $D = \langle\phi_n\rangle$ for many choices of A, and use this information to check that n has no divisors except 1 and n. A more precise outline of how one might proceed is as follows.

(6.1) To prove that n is prime one proceeds in three stages.

(a) In the first stage one selects two auxiliary positive integers s and t. The precise conditions that s and t should satisfy depend on the method that is used. They include:

s is "large" (e.g. $s > n^{1/2}$),

t is "small",

$n^t \equiv 1 \bmod s$,

the complete prime factorization of s is known.

(b) In the second stage one constructs one or more Galois extensions of R with abelian groups, and one performs certain calculations in these Galois extensions. Using results like (4.2) and (5.5) one proves that the decomposition group of the Galois extension $\mathbb{Z}[\zeta_s]/n\mathbb{Z}[\zeta_s]$ of R with group $(\mathbb{Z}/s\mathbb{Z})^*$ is generated by $(n \bmod s)$; or, equivalently, that for each divisor r of n there exists $i \pmod t$ such that $r \equiv n^i \bmod s$.

(c) In the third stage one uses the information from (b) about the divisors of n to prove that 1 and n are the only divisors of n, so that n is prime. It is for

this stage that one needs s to be "large". For more details about this stage, which has nothing to do with Galois theory, we refer to [5, Section 3].

Several of the rings occurring in this primality proof turn out to be fields in the end. This applies for example to n itself and to the cyclotomic extensions from (4.1). But using this information in the proof would obviously give rise to a circular argument. Thus we are in the paradoxical situation that we generalized Galois theory from fields to rings in order to apply it to rings that are in fact fields.

Before we give examples of algorithms that proceed in the above way we treat some auxiliary algorithms.

(6.2) Constructing cyclic extensions. Let u be a positive integer. We describe four algorithms to obtain an explicit presentation of a Galois extension A of n with a cyclic group $\langle\sigma\rangle$ of order u, with the property that $\sigma = \phi_n$ if n is prime. (So A becomes a field if n is prime, see (3.8).)

(a) Suppose that a small positive integer t with $\gcd(t, n) = 1$ can be found for which $u = \#\langle n \bmod t\rangle$. Then we can use Berlekamp's algorithm to construct a t-th cyclotomic extension A, σ, ζ of n, see (4.6). This is a Galois extension of n with a cyclic group $\langle\sigma\rangle$ of order u, and $\sigma = \phi_n$, by (4.2)(a).

(b) Alternatively, one can determine a polynomial $h \in n[X]$ with leading coefficient 1 and degree u, such that h is irreducible if n is prime. See [9, Section 5] for methods to do this. Next one uses (4.7) to construct the desired extension; if any of the conditions of (4.7) is found not to be satisfied then n is not prime (see (4.8)). It is, with this construction, not guaranteed that $\sigma = \phi_n$ (see (4.8)), but if n is prime it is of course true. Usually it is possible to choose h such that its coefficients are "small", which facilitates the multiplication in $A = n[X]/hn[X]$. Method (a) does not have this advantage (unless $h = \Phi_t$ in (a)).

(c) Suppose that one can find a small positive integer m with $\gcd(m, n) = 1$ and a group homomorphism $\chi: (\mathbb{Z}/m\mathbb{Z})^* \to \langle\zeta_u\rangle$ such that $\chi(n)$ generates $\langle\zeta_u\rangle$. This is usually easy to do, unless n is a p-th power for some prime p dividing u. Let L be the subfield of $\mathbb{Q}(\zeta_m)$ corresponding to $\ker\chi$, with ring of integers A_L. Then $A = A_L/nA_L$ is Galois over n with group $\langle\zeta_u\rangle$, and the Artin symbol ϕ_n equals $\chi(n)$, cf. (5.6). To obtain an explicit presentation of A one can choose $\alpha \in A_L$ such that $L = \mathbb{Q}(\alpha)$ and such that the discriminant of the irreducible polynomial h of α over $\mathbb{Q}$ is coprime to n. Then $A \cong n[X]/hn[X]$. From a computational point of view this is an attractive presentation: not only the multiplication is easy to perform, as in (b), but also the Galois action of the group $\langle\zeta_u\rangle$. If χ is an *isomorphism* we can take $\alpha = \zeta_m$ and $h = \Phi_m$, which in this case also results from (a) (with $t = m$).

(d) Suppose that $u = u_0u_1$, where u_0 and u_1 are positive integers with $\gcd(u_0, u_1) = 1$. Suppose further that A_i is Galois over n with a cyclic group $\langle\sigma_i\rangle$ of order u_i, for $i = 0, 1$. Then $A = A_0 \otimes_n A_1$ is Galois over n with a cyclic group $\langle\sigma_0\rangle \times \langle\sigma_1\rangle = \langle(\sigma_0, \sigma_1)\rangle$ of order u, by (2.3)(d). Moreover, if each σ_i is the Artin symbol for A_i, then (σ_0, σ_1) is the Artin symbol for A, by

(3.2)(d).

(6.3) Composite numbers. The properties of the algorithms in (6.2) that are relevant in the context of primality testing are: (i) if n is prime, then the algorithms are likely to terminate within a reasonable time limit; (ii) if any of these algorithms terminates, then the result is a Galois extension with the stated properties (even if n is composite). In particular, in primality testing it is irrelevant whether the algorithms terminate if n is composite. This is nevertheless a question of independent interest. We stated already in (4.6) that method (a) is not likely to work for composite n, except if $\langle n \bmod t \rangle = (\mathbb{Z}/t\mathbb{Z})^*$. The behaviour of algorithm (b) probably depends on the particular method that is chosen to determine h. Algorithm (c) works for any n that is not a p-th power for any prime p dividing u. The method in (d) can be used for any n to reduce the problem to the case that u is a prime power.

(6.4) Isomorphism of subextensions. Suppose that A_i is Galois over n with a cyclic group $\langle\sigma_i\rangle$ of order u_i, for $i = 0, 1$, and let u be a common divisor of u_0 and u_1. Then $B_i = A_i^{\langle\sigma_i^u\rangle}$ is Galois over n with a cyclic group of order u generated by the restriction of σ_i, for $i = 0, 1$. If n is prime and $\sigma_i = \phi_n$ for each i, so that each A_i is a field (see (3.8)), then we know that B_0 is isomorphic to B_1 as a Galois extension of n. We describe an algorithm to find such an isomorphism. As in (6.3) we want the algorithm to have two properties: (i) if n is prime and $\sigma_i = \phi_n$ for each i then the algorithm is likely to terminate within a reasonable time limit; (ii) if the algorithm terminates then the result is an isomorphism $f: B_0 \to B_1$ with $\sigma_1 f = f\sigma_0$ (even if the A_i are not known to be fields).

There are situations in which the isomorphism $B_0 \cong B_1$ is obvious. This is the case, for example, if there is a Galois extension A of n with a cyclic group $\langle\sigma\rangle$ such that each A_i is contained in A, with $\sigma_i = \sigma|A_i$. If this is not the case one might try to construct such an A, but it is more efficient to proceed as follows.

One begins by constructing, as in (6.2), a Galois extension B of n with a cyclic group $\langle\sigma\rangle$ of order u. Next one constructs ring homomorphisms $f_i: B \to A_i$ for $i = 0, 1$. If $B = n[X]/hn[X]$ for some $h \in n[X]$ this comes down to finding a zero of h in A_i, which can be done by the methods described in [9, Section 3]. If B is a tensor product of several rings $n[X]/h_j n[X]$ it suffices to find a zero of each h_j in A_i.

Once the f_i have been constructed one checks that $f_i\sigma = \sigma_i f_i$, as must be the case if n is prime and σ, σ_i are the Artin symbols. If $f_i\sigma = \sigma_i f_i$ then by (2.8) the map f_i yields an isomorphism $B \cong B_i$, for $i = 0, 1$. This leads to the required isomorphism $B_0 \cong B_1$.

(6.5) Construction of cyclotomic extensions. Let t be a positive integer that is coprime to n, and suppose that the complete prime factorization of t is known. We describe an algorithm to construct a t-th cyclotomic extension of n that is likely to be successful if n is prime and the number $u = \#\langle n \bmod t \rangle$ is not too large.

One begins by constructing a Galois extension A of n with group $\langle\sigma\rangle$ of order u, as in (6.2). If one uses method (6.2)(a) to do this, with the same t, this leads by (4.5) to the required extension. Otherwise, one continues as follows.

For each prime q dividing t one does the following. One finds, by trial and error, an element $\alpha = \alpha_q \in A$, $\alpha \neq 0$, such that

$$\sigma\alpha = \alpha^n, \qquad \alpha^{(n^u-1)/q} \neq 1.$$

If n is prime and $\sigma = \phi_n$ then any α has the first property, and it has the second property with probability $1 - 1/q$; so α should not be hard to find. If α has been found one expresses α and $\alpha^{(n^u-1)/q} - 1$ on a basis of A over n. Let $c_q \in n$ be one of the non-zero coefficients of the first of these expressions, and $d_q \in n$ of the second.

This being done for each q, one checks by means of the Euclidean algorithm that $\prod_q (c_q d_q) \in n^*$, as must be the case if n is prime. Then the conditions of (4.4) are satisfied, so if ζ is as in (4.4) then A, σ, ζ is a t-th cyclotomic extension of n.

Notice that the same construction actually yields a t_0-th cyclotomic extension of n, where t_0 is the largest divisor of $n^u - 1$ that is built up from the primes dividing t.

We remark that the calculations involved in the above construction can often be done in proper subextensions of A. For example, if $q^{m(q)}$ is a prime power dividing t, as in (4.4), then the search for $\alpha = \alpha_q$ can be done in the subextension of rank equal to $\#\langle n \bmod q^{m(q)}\rangle$, which may be smaller than t. Explicit presentations for such subextensions can be obtained as in (6.4).

(6.6) Classical primality tests. Our first example of a primality test that proceeds as in (6.1) is as follows.

First one constructs s and t as in (6.1)(a), with t as small as possible. This is done by looking for prime factors of $\Phi_1(n) = n - 1$, $\Phi_2(n) = n + 1$, $\Phi_3(n) = n^2 + n + 1$, $\Phi_4(n) = n^2 + 1$, ..., and letting s be equal to the product of the primes that are found, with the proper multiplicities. If one is lucky this leads to a number s that is sufficiently large, and one puts t equal to the order of $(n \bmod s)$ in $(\mathbb{Z}/s\mathbb{Z})^*$. For example, if $n = 2^k + 1$ for some $k \geq 1$ one can take $s = n - 1 = 2^k$, $t = 1$, and if $n = 2^k - 1$ for some $k \geq 2$ one can choose $s = 2(n + 1) = 2^{k+1}$, $t = 2$. If one does not succeed in finding a sufficiently large value for s in this way there is still the possibility of applying a technique that depends on lower bounds for the unknown prime factors of $n - 1$, $n + 1$, ..., see [14].

Suppose that s and t have been found, with $t = \#\langle n \bmod s\rangle$. Then one constructs, by the method of (6.5), an s-th cyclotomic extension of n, which is an extension of rank t. From (4.2) it now follows that for each divisor r of n there exists $i \pmod t$ with $r \equiv n^i \bmod s$. With this information one can proceed to part (c) of (6.1).

If $t = 1$ or 2 then the above test is essentially contained in [3], except for the language that is used. Larger values for t, all dividing 12, were employed by

Williams [14].

(6.7) Gauss sum tests. We next describe a test depending on Theorem (5.5). It generalizes a method that was proposed in [5].

First one chooses s and t as in (6.1)(a), but with the condition $n^t \equiv 1 \bmod s$ replaced by

$$a^t \equiv 1 \bmod s \qquad \text{for all } a \in \mathbb{Z} \text{ with } \gcd(a, s) = 1.$$

We refer to [5, Section 4] for methods to choose s and t. The number t will usually be somewhat larger than in (6.6). To give an impression of the size of these numbers we remark that for $n \leq 10^{100}$ one can take $t = 5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$ and

$$s = 2t \cdot \prod_{q \text{ prime},\ q-1 \mid t} q$$
$$= 2^6 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 29 \cdot \ldots \cdot 1009 \cdot 2521 \approx 1.532 \cdot 10^{52}.$$

If s and t have been chosen one checks that $\gcd(st, n) = 1$.

Next one puts $u = \#\langle n \bmod t \rangle$, and one constructs a Galois extension A of n with a cyclic group $\langle \sigma \rangle$ of order u, as in (6.2). Notice that u divides 12 if $t = 5040$. One now replaces t by the largest divisor of $n^u - 1$ that is built up from the primes dividing t, so that (5.1)(i) is satisfied. Using the method of (6.5) one finds $\zeta \in A$ such that A, σ, ζ is a t-th cyclotomic extension of n.

At this point we know from (5.1) that for each divisor r of n and each t' as in (5.1)(iii) we have

$$r \equiv n^{\ell_t(r)} \bmod t',$$

where $\ell_t(r)$ is as in (5.3). We wish to prove the same congruence modulo s.

Let s' be the largest divisor of s that is relatively prime to t. (By [5, (4.1)], the number s' is squarefree.) One selects a set Y of pairs (m, χ) such that: (i) for each pair, m is a divisor of s' and χ is a primitive group homomorphism $(\mathbb{Z}/m\mathbb{Z})^* \to \langle \zeta \rangle$ (see (5.4)); (ii) the induced group homomorphisms $(\mathbb{Z}/s'\mathbb{Z})^* \to \langle \zeta \rangle$ sending $(x \bmod s')$ to $\chi(x \bmod m)$ generate the group of all group homomorphisms $(\mathbb{Z}/s'\mathbb{Z})^* \to \langle \zeta \rangle$ if (m, χ) ranges over Y.

For each $(m, \chi) \in Y$ one now checks the condition $\tau(\chi)^{1 - n/\sigma} \in \langle \zeta \rangle$ of Theorem (5.5)(b). As we remarked in (5.7), this verification can de done within the subring of A generated by the image of χ. If $\tau(\chi)^{1 - n/\sigma} \notin \langle \zeta \rangle$ for some $(m, \chi) \in Y$ then n is not prime, by (5.5)(a). Hence assume that $\tau(\chi)^{1 - n/\sigma} \in \langle \zeta \rangle$ for all $(m, \chi) \in Y$, and let r divide n. Then $\chi(r) = \chi(n)^{\ell_t(r)}$ for each $(m, \chi) \in Y$, by (5.5)(b), and property (ii) above now implies that $\chi(r) = \chi(n)^{\ell_t(r)}$ for *all* group homomorphisms $\chi: (\mathbb{Z}/s'\mathbb{Z})^* \to \langle \zeta \rangle$. Since the exponent of $(\mathbb{Z}/s'\mathbb{Z})^*$ divides t, this yields

$$r \equiv n^{\ell_t(r)} \bmod s'.$$

To prove the same congruence modulo s it now suffices to do it modulo s/s', since $\gcd(s', s/s') = 1$. Because $t' = s/s'$ is built up from primes dividing t it usually satisfies (5.1)(iii), so that $r \equiv n^{\ell_t(r)} \bmod s/s'$ is automatic. The only situation in which $t' = s/s'$ does not satisfy (5.1)(iii) is given by

$$n \equiv 3 \bmod 4, \qquad u \text{ is odd}, \qquad t \equiv 2 \bmod 4, \qquad s \equiv s/s' \equiv 8 \bmod 16.$$

This minor problem can be solved in three ways. The first is to avoid this case in the

selection of s and t. The second is to observe that $t' = \frac{1}{2}s/s'$ does satisfy (5.1) (iii), and to be content with the slightly weaker conclusion $r \equiv n^{\ell_t(r)} \bmod \frac{1}{2}s$. The third is to check $\tau(\chi)^{1 - n/\sigma} \in \langle\zeta\rangle$ for one more pair (m, χ), with now m not being a divisor of s' but a multiple of 8; for example we can take $m = 8$ and $\chi(\pm 3^j \bmod 8) = (-1)^j$, in which case $\tau(\chi)^{1 - n/\sigma} \in \langle\zeta\rangle$ is equivalent to $8^{(n-1)/2} \equiv \pm 1 \bmod n$. If $r \equiv n^{\ell_t(r)} \bmod \frac{1}{2}s$ and $\chi(r) = \chi(n)^{\ell_t(r)}$ for a pair (m, χ) as just described, then $r \equiv n^{\ell_t(r)} \bmod s$.

If, finally, it has been proved that $r \equiv n^{\ell_t(r)} \bmod s$ for each r dividing n, one can proceed to part (c) of (6.1).

This concludes our description of the Gauss sum method.

(6.8) Comparison of the two methods. The methods discussed in (6.6) and (6.7) differ in two important respects. The first is that whereas in (6.6) the numbers s and t should satisfy

$$n^t \equiv 1 \bmod s,$$

they should in (6.7) satisfy the much stronger condition

$$a^t \equiv 1 \bmod s \qquad \text{for all } a \in \mathbb{Z} \text{ with } \gcd(a, s) = 1.$$

This implies that the second method is less sensitive to special properties of the number n: the same values for s and t can be used for all n of the same order of magnitude, and several quantities can be computed once and for all (cf. [5, Section 12, Step 1]).

The stronger condition that s and t should satisfy in (6.7) also implies that the value for t is larger in (6.7) than it is in (6.6). This is compensated for in the other difference between the two methods: whereas the main calculations in (6.6) are performed in a ring of *rank* t over n, the calculations in (6.7) are performed in a t-th *cyclotomic* extension of n, the rank of which is usually much smaller than t.

(6.9) Combination of the two methods. We shall now see how the formalism of Galois theory allows the two methods to be combined. Suppose that method (6.6) has been applied with auxiliary numbers s_0, t_0, and method (6.7) with numbers s_1, t_1. Then one knows that for each divisor r of n there exist integers $i_0 \pmod{t_0}$ and $i_1 \pmod{t_1}$ such that

$$r \equiv n^{i_0} \bmod s_0, \qquad r \equiv n^{i_1} \bmod s_1.$$

Suppose moreover that each of the numbers s_0, s_1 is too small for stage (c) of (6.1) to be practicable, but that the number $s = \operatorname{lcm}(s_0, s_1)$ is sufficiently large. Then one would like to show that for each divisor r of n there exists an integer i modulo $t = \operatorname{lcm}(t_0, t_1)$ such that $r \equiv n^i \bmod s$. This clearly holds if $i \equiv i_0 \bmod t_0$ and $i \equiv i_1 \bmod t_1$, so one is faced with the task of proving $i_0 \equiv i_1 \bmod \gcd(t_0, t_1)$. That is easy to do if $\#\langle n \bmod \gcd(s_0, s_1)\rangle = \gcd(t_0, t_1)$, but in many cases $\#\langle n \bmod \gcd(s_0, s_1)\rangle$ is smaller.

One can solve this problem by interpreting the above congruences as relations between the Artin symbols ϕ_r and ϕ_n in suitable Galois extensions of n and by exhi-

biting isomorphic subextensions, as in (6.4). Instead of describing *in abstracto* how to proceed let me use a few "seminumerical" examples to indicate the possible techniques.

Suppose that $t_1 = 5040$ and assume for simplicity that the number $u = \#\langle n \bmod t_1 \rangle$ from (6.7) equals 12. Then the Gauss sum calculations are performed in a Galois extension A_1 of n with a cyclic group $\langle \sigma_1 \rangle$ of order 12. They lead to the conclusion that for r dividing n we have

$$r \equiv n^{\ell(r)} \bmod s_1$$

for some integer $\ell(r)$ (mod 5040). If ϕ_r, ϕ_n denote the Artin symbols for A_1 we also have $\phi_r = \phi_n^{\ell(r)}$, and this determines $\ell(r)$ modulo 12.

Assume now first that t_0 divides 12, as is the case with the tests described by Williams [14]. Then the calculations involved in (6.6) are performed in a Galois extension A_0 of n with a cyclic group $\langle \sigma_0 \rangle$ of order dividing 12. Suppose that there is a ring homomorphism $f: A_0 \to A_1$ with $f\sigma_0 = \sigma_1 f$; this is the case, for example, if one has chosen A_0 to be a subextension of A_1, with $\sigma_0 = \sigma_1 | A_0$, and in any case f may be constructed as in (6.4). Then the equality $\phi_r = \phi_n^{\ell(r)}$ for A_1 implies the corresponding equality for A_0, by (3.4). From (4.2)(b) one then obtains $r \equiv n^{\ell(r)} \bmod s_0$, so $r \equiv n^{\ell(r)} \bmod \operatorname{lcm}(s_0, s_1)$, as desired.

Let it next be assumed, still with $t_1 = 5040$ and $u = 12$, that $t_0 = 5$. Then A_0 has rank 5 over n, so to establish a connection between the two tests we need a Galois extension of n of degree divisible by 5 that is associated to the Gauss sum test. Suppose, for simplicity, that there is a pair (m, χ) in the set Y occurring in (6.7) with the property that the image of χ has order 5 and is generated by $\chi(n)$. Let $L = \mathbb{Q}(\zeta_m)^{\ker \chi}$ and A_L be as in (5.6). Then the equality $\chi(r) = \chi(n)^{\ell(r)}$ resulting from (5.5)(b) exactly means that $\phi_r = \phi_n^{\ell(r)}$ for the Galois extension A_L/nA_L of n occurring in (5.6). Hence if we establish an isomorphism $A_0 \cong A_L/nA_L$ of Galois extensions then we also have $\phi_r = \phi_n^{\ell(r)}$ for A_0. This leads, as before, to the congruence $r \equiv n^{\ell(r)} \bmod \operatorname{lcm}(s_0, s_1)$ that we wished to prove.

The conclusion is that it is advisable to construct the Galois extension A_0 used in (6.6) from Galois extensions that arise in connection with (6.7). This makes it possible to combine the two methods without extra effort. It may be expected that this combination will lead to important practical improvements in primality testing.

References.

1. M.F. Atiyah, I.G. Macdonald, Introduction to commutative algebra, Addison-Wesley, Reading, Mass., 1969.
2. N. Bourbaki, Algèbre commutative, Chapitres 1 et 2, Hermann, Paris, 1961.
3. J. Brillhart, D.H. Lehmer, J.L. Selfridge, New primality criteria and factorizations of $2^m \pm 1$, Math. Comp. 29 (1975), 620-647.
4. S.U. Chase, D.K. Harrison, A. Rosenberg, Galois theory and Galois cohomology of commutative rings, Memoirs Amer. Math. Soc. 52 (1965), 15-33.
5. H. Cohen, H.W. Lenstra, Jr., Primality testing and Jacobi sums, Math. Comp. 42 (1984), 297-330.
6. F. DeMeyer, E. Ingraham, Separable algebras over commutative rings, Lecture Notes

in Math. 181, Springer-Verlag, Berlin, 1971.
7. J.D. Dixon, Factorization and primality tests, Amer. Math. Monthly 91 (1984), 333-352.
8. D.E. Knuth, The art of computer programming, vol. 2, Seminumerical algorithms, 2nd ed., Addison-Wesley, Reading, Mass., 1981.
9. A.K. Lenstra, Factorization of polynomials, pp. 169-198 in [13].
10. H.W. Lenstra, Jr., Primality testing, pp. 55-77 in [13].
11. H.W. Lenstra, Jr., Primality testing algorithms (after Adleman, Rumely and Williams), Sém. Bourbaki 33 (1980/1981), Exposé 576, pp. 243-257 in: Lecture Notes in Math. 901, Springer-Verlag, Berlin, 1981.
12. H.W. Lenstra, Jr., Primality testing with Artin symbols, pp. 341-347 in: N. Koblitz (ed.), Number theory related to Fermat's last theorem, Progress in Mathematics 26, Birkhäuser, Boston, 1982.
13. H.W. Lenstra, Jr., R. Tijdeman (eds), Computational methods in number theory, Mathematical Centre Tracts 154/155, Mathematisch Centrum, Amsterdam, 1982.
14. H.C. Williams, Primality testing on a computer, Ars Combin. 5 (1978), 127-185.