ACTA ARITHMETICA
115.1 (2004)

Computing Galois groups by means of Newton polygons

by

Michael Kölle and Peter Schmid (Tübingen)

Newton polygons are useful for computing decompositions of primes in extension rings, and for computing Galois groups. Suppose f is a polynomial with coefficients in an algebraic number field K and $\mathfrak{p}$ is a finite prime of K. Then, following Ore [10], one can associate to f certain polynomials $f_m \in K[X]$ according to the slopes, m, of the sides of its Newton polygon with respect to $\mathfrak{p}$. Under some mild assumptions the Galois groups of the f_m, viewed as polynomials over the $\mathfrak{p}$-adic completion $K_{\mathfrak{p}}$, turn out to be constituents of $\mathrm{Gal}_{K_{\mathfrak{p}}}(f)$. The point is that the f_m are usually much easier to handle than f, often they are pure polynomials.

1. Introduction. Originally Newton introduced polygons in order to investigate complex curves of two variables leading to what is now called the Puiseux series of a curve (cf. [1, pp. 494 ff.] for details). The method also applies to polynomials in one variable by looking at the various g-adic expansions. Such a theory has been developed by Ore [10] some eighty years ago. Ore's work has found recent interest (e.g. see [2], [5], [7], [8]). The objective of the present paper is to show how his ideas apply for computing Galois groups of (global) polynomials.

We fix an algebraic number field K, a finite prime $\mathfrak{p}$ of K, and a normalized polynomial $f \in K[X]$ of degree $n \geq 1$:

$$f = \sum_{i=0}^{n} (-1)^i a_i X^{n-i} = X^n - a_1 X^{n-1} + \cdots + (-1)^n a_n.$$

Here "normalized" means that $a_0 = 1$ *and* that $a_n \neq 0$. Denote by $v_{\mathfrak{p}}$ the (exponential) $\mathfrak{p}$-adic valuation of K. The (standard) *Newton polygon* of f with respect to $\mathfrak{p}$ (and to $g(X) = X$) is the convex hull of the points $(i, v_{\mathfrak{p}}(a_i))$, with $a_i \neq 0$, in the Euclidean $\mathbb{R}^2$. We pick a side S_m of this polygon, determined by its slope m. Write $m = h/e$, where h and e are

2000 *Mathematics Subject Classification*: Primary 11S20; Secondary 11R32.

relatively prime rational integers and $e > 0$; this is made unique by letting $e = 1$ in case $m = 0$. Let S_m begin with the point $(s, v_{\mathfrak{p}}(a_s))$ and end with $(t, v_{\mathfrak{p}}(a_t))$. Then there is a unique positive integer d such that $de = t - s$ is the *length* of S_m and $dh = v_{\mathfrak{p}}(a_s^{-1}a_t)$ is its *height*.

Let us fix some further notation. Let L be "the" splitting field of f and $G = \mathrm{Gal}(L|K)$. We write $G = \mathrm{Gal}_K(f)$ when G is understood as a permutation group on the set Z_f of zeros of f. Let $\mathfrak{P}$ be a prime of L above $\mathfrak{p}$ (unique up to G-conjugacy) and denote by $G_{\mathfrak{P}}$ and $I_{\mathfrak{P}}$ its decomposition and inertia groups, respectively. We extend $v_{\mathfrak{p}}$ uniquely to the $\mathfrak{p}$-adic completion $K_{\mathfrak{p}}$ and to some algebraic closure $\overline{K}_{\mathfrak{p}}$ containing $L_{\mathfrak{P}}$. Then $L_{\mathfrak{P}} = K_{\mathfrak{p}}L$ is the topological closure of L in $\overline{K}_{\mathfrak{p}}$ and $G_{\mathfrak{P}} = \mathrm{Gal}(L_{\mathfrak{P}}|K_{\mathfrak{p}})$ in the natural way. Let $k_{\mathfrak{p}}$ be the (finite) residue class field of $K_{\mathfrak{p}}$.

The rational numbers m_i occurring as slopes of the sides of the Newton polygon of f are characterized by the property that the sets Z_{f,m_i} of roots of f with $v_{\mathfrak{p}}$-value m_i are not empty (see Statement 1 below). Moreover,

$$Z_f = \biguplus_i Z_{f,m_i}$$

is a decomposition into blocks of $G_{\mathfrak{P}}$. By its very definition the Newton polygon only can give information on $G_{\mathfrak{P}}$. Hence our target is to describe the constituent $G_{\mathfrak{P}}^{Z_{f,m}}$ (for the chosen slope m).

If f is *separable* (nonzero discriminant) one knows that $|Z_{f,m}| = de$ (Statement 1), and from a result of van der Waerden [11] one gets some information on the action of $G_{\mathfrak{P}}$ on $Z_{f,m}$ (see Statement 4). But this is helpful for computations only when knowing precisely the decomposition of $\mathfrak{p}$ in the root fields $K(\theta)$ for $\theta \in Z_{f,m}$. The basic idea is to replace $Z_{f,m}$ by the roots of a polynomial f_m easily obtained from S_m. Following Ore [10] we introduce this *factor* f_m and the polynomial f_S *associated* to $S = S_m$. For each $i \geq 0$ we have $v_{\mathfrak{p}}(a_s^{-1}a_{s+i}) \geq im$, and equality holds precisely when $(s+i, v_{\mathfrak{p}}(a_{s+i})) \in S_m$. The factor is defined by

$$f_m = \sum_{\substack{i=0 \\ (s+i, v_{\mathfrak{p}}(a_{s+i})) \in S_m}}^{de} (-1)^i a_s^{-1} a_{s+i} X^{de-i},$$

ignoring the points not lying on S_m. The polynomial $f_m \in K[X]$ is normalized and its Newton polygon consists of one side, say S, with length de and slope m. Since $m = h/e$ and $(h, e) = 1$ only points of the form (jh, je) arise from f_m on S $(0 \leq j \leq d)$. So, fixing an element π in K of order 1 at $\mathfrak{p}$ $(v_{\mathfrak{p}}(\pi) = 1)$, we may "shorten" f_m obtaining a normalized polynomial $f_S \in K[X]$ of degree d such that f_m is obtained from f_S by substituting $X \mapsto \pi^{-h}X^e$ and multiplying the resulting polynomial with π^{dh}.

The nonzero coefficients of f_S are $\mathfrak{p}$-units. This f_S as well as the reduction $\bar{f}_S = f_S \bmod \mathfrak{p}$ will be called the *polynomial*(s) *associated to* S (or to S_m).

THEOREM. *Suppose that* $\mathfrak{p}$ *does not divide the discriminant of* f_S, *that is*, $\bar{f}_S = f_S \bmod \mathfrak{p}$ *is separable. Then* f_m *is separable and* $|Z_{f,m}| = de$ ($= \deg(f_m) =$ *length of the side* S_m). *If in addition* $\mathfrak{p} \nmid e$, *then the following hold*:

(i) *For every root* β *of* f_m *there exists* $\theta \in Z_{f,m}$ *such that* $K_{\mathfrak{p}}(\beta) = K_{\mathfrak{p}}(\theta)$, *and vice versa.*

(ii) *The constituent* $G_{\mathfrak{P}}^{Z_{f,m}}$ *is permutation isomorphic to* $\mathrm{Gal}_{K_{\mathfrak{p}}}(f_m)$.

(iii) $I_{\mathfrak{P}}^{Z_{f,m}}$ *is cyclic generated by an element which is the product of* d *disjoint* e*-cycles on* $Z_{f,m}$.

(iv) $G_{\mathfrak{P}}^{Z_{f,m}}/I_{\mathfrak{P}}^{Z_{f,m}}$ *is, as a permutation group on the set of orbits of* $I_{\mathfrak{P}}$ *on* $Z_{f,m}$, *permutation isomorphic to* $\mathrm{Gal}_{k_{\mathfrak{p}}}(\bar{f}_S)$.

Following Ore [10] we say that the side S_m is *regular* provided $\bar{f}_S$ is separable. This, as well as possible factorizations of $\bar{f}_S$, are (essentially) independent of the choice of the prime element π in the definition of f_S. For altering π amounts to a substitution $X \mapsto uX$ in $f_S(X)$ for some $\mathfrak{p}$-unit $u \in K$, followed by multiplication with u^{-d}. If S_m is *not* regular, then there is a normalized $\mathfrak{p}$-integral polynomial $g \in K[X]$ whose reduction mod $\mathfrak{p}$ is irreducible and a multiple divisor of $f_S \bmod \mathfrak{p}$ ($g \nmid f$). Then one should examine the *g-adic Newton polygon* of f with respect to $\mathfrak{p}$ (see Section 7 below).

Let us describe two interesting special cases of the Theorem:

COROLLARY 1. *Suppose that the length of* S_m *divides its height. If* $\bar{f}_S = f_S \bmod \mathfrak{p}$ *is a product of pairwise distinct normalized irreducible polynomials in* $k_{\mathfrak{p}}[X]$ *of degrees* d_i, *then* $G_{\mathfrak{P}}^{Z_{f,m}}$ *is generated by a permutation which is the product of the corresponding disjoint* d_i*-cycles.*

Here $e = 1$. By assumption S_m is regular. By statement (iii) of the Theorem $I_{\mathfrak{P}}^{Z_{f,m}} = 1$ and so

$$G_{\mathfrak{P}}^{Z_{f,m}} \cong \mathrm{Gal}_{k_{\mathfrak{p}}}(\bar{f}_S)$$

by statement (iv). This yields the corollary, which generalizes a classical result due to Dedekind and Bauer (e.g. see Matzat [6, p. 127]).

COROLLARY 2. *Suppose that length and height of* S_m *are nonzero and relatively prime. If* $\mathfrak{p}$ *does not divide* e, *then* $G_{\mathfrak{P}}^{Z_{f,m}} = I_{\mathfrak{P}}^{Z_{f,m}}$ *is cyclic of order* e.

Here $d = 1$. It follows that $f_m = X^e - b$ is a pure polynomial and that $f_S = X - \pi^{-h}b$ is linear, where $b = (-1)^{e+1}a_s^{-1}a_{s+e}$ and $\pi^{-h}b$ is a $\mathfrak{p}$-unit in K. The Theorem applies. Note also that f_m must be irreducible over $K_{\mathfrak{p}}$ and that its splitting field agrees with that of a certain prime factor of f over $K_{\mathfrak{p}}$.

The assumption $\mathfrak{p} \nmid e$ refers to *tame ramification.* The Theorem indeed implies the familiar result on totally and tamely ramified local extensions (see [9, II.7.7]). In this case f is an Eisenstein polynomial with respect to $\mathfrak{p}$, the Newton polygon of f consisting of one side $S = S_m$ with slope $m = 1/n$. Here we have $f_m = X^n - (-1)^{n+1}a_n$ and $f_S = X - u$ for some $\mathfrak{p}$-unit u. If $\mathfrak{p}$ does not divide $e = n$ (tame ramification) then, by the Theorem, $K_{\mathfrak{p}}(\theta) = K_{\mathfrak{p}}(\sqrt[n]{(-1)^{n+1}a_n})$ for a root θ of f (suitably chosen).

Our terminology follows Neukirch [9] (number theory) and Dixon–Mortimer [3] (permutation groups).

2. Background. We keep the assumptions and notations introduced above. Thus S_m is a side of the Newton polygon of f with respect to $\mathfrak{p}$ which has length de and slope $m = h/e$, with the *extreme points* $(s, v_{\mathfrak{p}}(a_s))$ and $(t, v_{\mathfrak{p}}(a_t))$, $s < t$ $(t - s = de)$.

Statement 1. *Let the roots $\theta_1, \ldots, \theta_n$ of f (counting multiplicities) be indexed in such a way that $v_{\mathfrak{p}}(\theta_i) \le v_{\mathfrak{p}}(\theta_j)$ if $i < j$. Then $\theta_{s+1}, \ldots, \theta_t = \theta_{s+de}$ are just those roots with $v_{\mathfrak{p}}$-value m, and the polynomial $\widehat{f}_m = \prod_{i=1}^{de}(X - \theta_{s+i})$ has its coefficients in $K_{\mathfrak{p}}$.*

For a proof we refer to [9, Theorems II.6.3 and II.6.4]. We regard $\widehat{f}_m \in K_{\mathfrak{p}}[X]$ as a *local* polynomial (though its coefficients are in $K_{\mathfrak{p}} \cap L$). We have $|Z_{f,m}| \le de$ and equality holds if and only if $\widehat{f}_m$ is separable.

Recall that $|I_{\mathfrak{P}}| = e_{\mathfrak{P}}$ is the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$ ([9, II.9.9]). Since $v_{\mathfrak{P}}(\theta_t) = e_{\mathfrak{P}} v_{\mathfrak{p}}(\theta_t) = h \cdot e_{\mathfrak{P}}/e$ is an integer, we see that e is a divisor of $|I_{\mathfrak{P}}|$. This is a basic, and often used, information on the order of the Galois group G which is immediate from the Newton polygon.

Statement 2. *Let $f = \prod_i f^{(i)}$ be a factorization over K into normalized polynomials $f^{(i)}$. Then S_m is obtained by "joining" the sides $S_m^{(j)}$ of the Newton polygons of those $f^{(j)}$ admitting the slope m. Moreover, f_m and $\prod_j f_m^{(j)}$ give rise to the same points on S_m and $f_S \equiv \prod_j f_S^{(j)} \pmod{\mathfrak{p}}$.*

For $\mathfrak{p}$-integral polynomials (and $m > 0$) this follows from the results proved in Chapter 1 of [10] (see Theorems 5 and 7). That it is true in general may be seen from Statement 1 on the basis of Proposition 1 below. Of course, to a normalized polynomial $\widehat{f} \in K_{\mathfrak{p}}[X]$ we assign the obvious Newton polygon (with respect to $v_{\mathfrak{p}}$). Statement 2 carries over to such local polynomials. If the polygon of $\widehat{f}$ consists of one side $\widehat{S}$ then, ignoring the coefficients of the polynomial yielding points not lying on $\widehat{S}$ and shortening the resulting factor, picking the same prime element $\pi \in K$ as before, we obtain an associated (local) polynomial $\widehat{f}_{\widehat{S}}$.

Statement 3. *Suppose $\widehat{f} \in K_{\mathfrak{p}}[X]$ is normalized, irreducible and $\widehat{N} = K_{\mathfrak{p}}(\theta)$ for some root θ of $\widehat{f}$. Then the Newton polygon of $\widehat{f}$ consists of one side $\widehat{S}$ and the associated polynomial $\widehat{f}_{\widehat{S}} \bmod \mathfrak{p}$ is a power of an irreducible polynomial $\bar{g} \in k_{\mathfrak{p}}[X]$. The degree of $\bar{g}$ divides the residue class degree $r(\widehat{N}|K_{\mathfrak{p}})$.*

From Statement 1 it is immediate that the Newton polygon is as asserted (see also [9, II.6.5]). By abuse of notation let $\widehat{f} = f$ and $\widehat{S} = S_m = S$ (so that $\deg(\widehat{f}) = n = de$ and $m = h/e$). So by definition

$$f_m(X) = \pi^{dh} f_S(\pi^{-h} X^e).$$

If $m = 0$ then f and $f_m = f_S$ are integral and have the same reduction mod $\mathfrak{p}$, which must be a power of an irreducible $\bar{g}$ by Hensel's lemma ([9, II.4.6]). Then the image of θ in the residue class field of $\widehat{N}$ is a root of $\bar{g}$. It follows that $\deg(\bar{g})$ divides $r(\widehat{N}|K_{\mathfrak{p}})$. Recall that the maximal unramified subextension of $\widehat{N}|K_{\mathfrak{p}}$ is cyclic of degree $r(\widehat{N}|K_{\mathfrak{p}})$. (Our notation differs from that in [9], reserving the letter f for polynomials.)

The general case is treated as follows (cf. [10, Theorem 3 in Chap. 2] for the case $m > 0$). We know from Statement 1 that $v_{\mathfrak{p}}(\pi^{-h}\theta^e) = -h + em = 0$. Hence $\pi^{-h}\theta^e$ is a unit in $\widehat{N}$. Let $\bar{g}$ be the minimum polynomial over $k_{\mathfrak{p}}$ of its residue class. Then $\deg(\bar{g})$ divides $r(\widehat{N}|K_{\mathfrak{p}})$. Let g be the minimum polynomial over $K_{\mathfrak{p}}$ of $\pi^{-h}\theta^e$. Then g is integral and the reduction $g \bmod \mathfrak{p}$ a power of $\bar{g}$ (Hensel). Let $t = \deg(g)$. Define the polynomial $\widetilde{g}$ by

$$\widetilde{g}(X) = \pi^{th} g(\pi^{-h} X^e).$$

Observe that g and $\widetilde{g}$ are normalized. We even know that $g(0)$ is a unit in $K_{\mathfrak{p}}$. Using the fact that g is integral this shows that the Newton polygon of $\widetilde{g}$ is a side $\widetilde{S}$ with length te and slope m. Its associated polynomial $\widetilde{g}_{\widetilde{S}}$ is obtained from g by leaving out those monomials where the coefficients are nonunits. In particular, it has the same reduction mod $\mathfrak{p}$. Now θ is a root of $\widetilde{g}$ and so $\widetilde{g} = f \cdot \widetilde{f}$ for some $\widetilde{f} \in K_{\mathfrak{p}}[X]$, because f is the minimum polynomial of θ. It follows from Statement 2 that $f_S \bmod \mathfrak{p}$ (like $\widetilde{g}_{\widetilde{S}} \bmod \mathfrak{p}$) is a power of $\bar{g}$, as desired.

The local polynomial $\widehat{f}_m$ of Statement 1 is normalized. By considering the elementary symmetric functions of its roots we see that its polygon consists of one side of length de and slope m which, therefore, may be identified with the side S assigned to the global polynomial f_m. In what follows we write $\widehat{f}_S$ in place of $(\widehat{f}_m)_S$ for the associated polynomial.

Statement 4. *Suppose f is irreducible over K and $N = K(\theta)$ $(\subseteq L)$ for some root θ of f. Let $\mathcal{M}$ denote the set of primes $\wp$ of N above $\mathfrak{p}$ satisfying $v_\wp(\theta) = e_\wp m$, where $e_\wp$ is the ramification index over $\mathfrak{p}$. Then there are normalized irreducible polynomials $\widehat{f}_\wp \in K_\mathfrak{p}[X]$ of degree $e_\wp r_\wp$, with $r_\wp$ denoting the residue class degree, such that*

$$\widehat{f}_m = \prod_{\wp\in\mathcal{M}} \widehat{f}_\wp.$$

Over the unramified extension field of $K_\mathfrak{p}$ of degree $r_\wp$ the polynomial $\widehat{f}_\wp$ decomposes into a product of Galois conjugate irreducible polynomials of degree $e_\wp$ $(\wp \in \mathcal{M})$.

This follows from a classical result of van der Waerden [11]. In fact, the roots of $\widehat{f}_\wp$ belong to an orbit of Z_f under the action of $G_\mathfrak{P}$, which in turn decomposes under $I_\mathfrak{P}$ into $r_\wp$ orbits of length $e_\wp$ (see also [6, Theorem 1, p. 126]). The 1-1 correspondence $\wp \leftrightarrow \widehat{f}_\wp$ is achieved as follows: A double coset $G_\theta\sigma G_\mathfrak{P}$ for $\sigma \in G$ corresponds to the $G_\mathfrak{P}$-orbit of θ^σ and determines the prime $\wp = \mathfrak{P}^{\sigma^{-1}} \cap N$ (so that the $\mathfrak{P}^{(\tau\sigma\gamma)^{-1}}$ for $\tau \in G_\theta = \mathrm{Gal}(L|N)$, $\gamma \in G_\mathfrak{P}$, are all the primes in L above $\wp$).

We have $v_\wp(\theta) = v_{\wp^\sigma}(\theta^\sigma)$ for all primes $\wp$ of N above $\mathfrak{p}$ and all $\sigma \in G$. It follows that $\wp \in \mathcal{M}$ if and only if there is $\sigma \in G$ such that $\mathfrak{P} \mid \wp^\sigma$ and $\theta^\sigma \in Z_{f,m}$, which gives the statement.

The primes $\wp$ in $\mathcal{M} = \mathcal{M}_\theta$ are said to *belong to the side* S_m. Since $v_\wp(\theta) = h \cdot e_\wp/e$ is an integer, e divides $e_\wp$.

3. Global and local polynomials to a side.

By definition the local polynomial $\widehat{f}_m$ is a divisor of f over $K_\mathfrak{p}$ whereas the global polynomial f_m is just constructed using certain coefficients of f. Computation of $\widehat{f}_m$ from f is not easy and often appears even impracticable.

Lemma. *Write $\widehat{f}_m = \sum_{i=0}^{de}(-1)^i c_i X^{de-i}$ (so that $c_0 = 1$). We have*

$$v_\mathfrak{p}(a_s^{-1}a_{s+i} - c_i) > im \quad \textit{for all } i = 0,\dots,de = t - s.$$

Proof. We order the roots $\theta_1,\dots,\theta_n$ of f totally as in Statement 1. Then we have $v_\mathfrak{p}(\theta_j) < m$ for $j \le s$ and $v_\mathfrak{p}(\theta_j) > m$ for $j > t = s + de$. The coefficients a_i of f for $i \ne 0$ are the elementary symmetric functions of the θ_j. We have $v_\mathfrak{p}(a_i) = v_\mathfrak{p}(\theta_1\cdots\theta_i)$ whenever $(i, v_\mathfrak{p}(a_i))$ is an extreme point of the polygon. This holds, in particular, for $i = s$ (with the obvious convention when $s = 0$). The coefficients c_i, $i \ne 0$, of $\widehat{f}_m$ are the elementary symmetric functions of the $\theta_{s+1},\dots,\theta_t$ (Statement 1). Hence

$$c_i = \sum_{s<l_1<\cdots<l_i\le t} \theta_{l_1}\cdots\theta_{l_i}$$

for each $i = 1, \ldots, de$. It follows that $v_{\mathfrak{p}}(c_i) \geq im$. Consider

$$\varrho_i = a_{s+i} - a_s c_i = \sum_{1 \leq l_1 < \cdots < l_{s+i} \leq n} \theta_{l_1} \cdots \theta_{l_{s+i}} - \Big(\sum_{1 \leq l_1 < \cdots < l_s \leq n} \theta_{l_1} \cdots \theta_{l_s} \Big) c_i.$$

Taking into account the expression for c_i, this ϱ_i is the difference of terms where each term is a sum of products of just $s+i$ of the roots θ_j (allowing certain multiplicities). The partial sum

$$(\theta_1 \cdots \theta_s) \cdot \sum_{s < l_1 < \cdots < l_i \leq t} \theta_{l_1} \cdots \theta_{l_i}$$

occurs in both a_{s+i} and $a_s c_i$, hence disappears in ϱ_i. But the $v_{\mathfrak{p}}$-value of this part is at least equal to $v_{\mathfrak{p}}(a_s) + im$, and all other products appearing in ϱ_i have larger $v_{\mathfrak{p}}$-values. We conclude that $v_{\mathfrak{p}}(\varrho_i) > v_{\mathfrak{p}}(a_s) + im$. The result follows. ■

PROPOSITION 1. *The points lying on S resulting from f_m and from $\widehat{f}_m$ are the same and $f_S \equiv \widehat{f}_S \pmod{\mathfrak{p}}$.*

Proof. It follows from the lemma that both polynomials f_m and $\widehat{f}_m$ yield the same points lying on S. Recall that $\widehat{f}_S = (\widehat{f}_m)_S$ is obtained from (the factor to) $\widehat{f}_m$, like f_S from f_m, using the same prime element π. Thus the lemma even tells us that $f_S - \widehat{f}_S$ is divisible by π. The proof is complete. ■

4. Regularity. In this section we assume that S_m is regular. Our discussion is motivated by the main theorem in Ore [10] (Theorem 5 in Chap. 2; see [2] and [7] for re-statements).

PROPOSITION 2. *Suppose $\mathfrak{p}$ does not divide the discriminant of f_S. Then both $\widehat{f}_m$ and f_m are separable* (*of degree de*). *There is a* 1-1 *correspondence $\varphi \leftrightarrow \psi$ between the normalized prime factors over $K_{\mathfrak{p}}$ of f_m and $\widehat{f}_m$ such that*:

(i) *Both φ and ψ have the same Newton polygon* (*a side with slope m*) *and the same associated polynomial $\bar{g} \in k_{\mathfrak{p}}[X]$, which is irreducible over $k_{\mathfrak{p}}$.*

(ii) *Letting θ and β denote roots of φ and ψ, respectively, both $K_{\mathfrak{p}}(\theta)$ and $K_{\mathfrak{p}}(\beta)$ have over $K_{\mathfrak{p}}$ ramification index e and residue class degree* $\deg(\bar{g})$.

Proof. By hypothesis and Proposition 1 we may write

$$\widehat{f}_S \bmod \mathfrak{p} = f_S \bmod \mathfrak{p} = \prod_i \bar{g}_i,$$

where the $\bar{g}_i$ are distinct normalized irreducible polynomials over $k_{\mathfrak{p}}$. Consider the normalized prime factors $f^{(j)}$ of f over K whose Newton polygon with respect to $\mathfrak{p}$ has a side $S_m^{(j)}$ with slope m. From Statements 1 and 2 it follows that each $f^{(j)}$ is a simple divisor of f and that $\widehat{f}_m = \prod_j \widehat{f}_m^{(j)}$ is separable of degree de.

Even more is true. By Statement 2 the associated polynomial mod $\mathfrak{p}$ to $f^{(j)}$ and $S_m^{(j)}$ is a product $\widetilde{g}_j$ of certain of the $\bar{g}_i$, and $\prod_j \widetilde{g}_j = f_S \bmod \mathfrak{p}$.

By Hensel's lemma we may write $f_S = \prod_i g_i$ where each $g_i \in K_{\mathfrak{p}}[X]$ is normalized, integral with reduction $\bar{g}_i$. Via the substitution $X \mapsto \pi^{-h}X^e$, followed by multiplication with $\pi^{\deg(g_i)h}$, from g_i we get a normalized polynomial $f_m^{(i)} \in K_{\mathfrak{p}}[X]$ of degree $e \cdot \deg(g_i)$. Since $\sum_i \deg(g_i) = d = \deg(f_S)$ this yields a factorization

$$f_m = \prod_i f_m^{(i)}$$

over $K_{\mathfrak{p}}$. The Newton polygon of each $f_m^{(i)}$ must be a side with slope m and with associated polynomial g_i. Since $\bar{g}_i$ is irreducible over $k_{\mathfrak{p}}$, from Statement 2 it follows that $f_m^{(i)}$ must be irreducible over $K_{\mathfrak{p}}$. Separability of $f_S \bmod \mathfrak{p}$ implies that f_m is separable.

Replacing f by some $f^{(j)}$, if necessary, we therefore may assume that f is irreducible over K. Then, if we let $N = K(\theta)$ for some root θ of f, Statement 4 applies. We obtain the prime factorization

$$\widehat{f}_m = \prod_{\wp \in \mathcal{M}} \widehat{f}_{\wp}$$

over $K_{\mathfrak{p}}$ indexed by the set $\mathcal{M}$ of primes of N belonging to S_m. By Statements 3 and 2 (and separability of $\widehat{f_S} \bmod \mathfrak{p}$) the Newton polygon of any $\widehat{f}_{\wp}$ is a side with slope m and irreducible associated polynomial $\bar{g}_{\wp} \bmod \mathfrak{p}$, which must be one of the $\bar{g}_i$. In this manner we get a 1-1 correspondence $\wp \leftrightarrow i$ which we use to re-write $\bar{g}_{\wp} = \bar{g}_i$ and $f_{\wp} = f_m^{(i)}$. Thus $f_m = \prod_{\wp \in \mathcal{M}} f_{\wp}$ likewise.

Recall that $\deg(f_{\wp}) = e \cdot \deg(\bar{g}_{\wp})$ and $\deg(\widehat{f}_{\wp}) = e_{\wp} \cdot r_{\wp}$ (Statement 4), and that e is a divisor of $e_{\wp}$ for all $\wp \in \mathcal{M}$. From Statement 3 we know that $\deg(\bar{g}_{\wp})$ divides $r(\widehat{N}|K_{\mathfrak{p}})$ where $\widehat{N} = K_{\mathfrak{p}}(\theta^{\sigma})$ for some root θ^{σ} of $\widehat{f}_{\wp}$ in $L_{\mathfrak{P}}$ (with $\sigma \in G$). Then $\mathfrak{P} \mid \wp^{\sigma}$ and $\widehat{N} = (N^{\sigma})_{\wp^{\sigma}}$. It follows that $r(\widehat{N}|K_{\mathfrak{p}}) = r_{\wp}$ $(= r_{\wp^{\sigma}})$. From

$$\sum_{\wp} e \cdot \deg(\bar{g}_{\wp}) = \deg(f_m) = \deg(\widehat{f}_m) = \sum_{\wp} e_{\wp} \cdot r_{\wp}$$

we may conclude that $e_{\wp} = e$ and $\deg(\bar{g}_{\wp}) = r_{\wp}$ for all $\wp \in \mathcal{M}$. This completes the proof. ■

5. Tame ramification. Let φ and ψ be normalized, irreducible polynomials of the same degree over $K_{\mathfrak{p}}$ having the same Newton polygon, a side Σ with slope m (with $m = h/e$ as usual).

Proposition 3. *Assume that φ and ψ have the same associated polynomial $\bar{g}$ and that it is irreducible over $k_{\mathfrak{p}}$. If $\mathfrak{p}$ does not divide e, then to every root θ of φ there is a root β of ψ such that $K_{\mathfrak{p}}(\theta) = K_{\mathfrak{p}}(\beta)$, and vice versa.*

Proof. By symmetry it suffices to show that, for a fixed root θ of φ, there exists a root β of ψ with the required property. In place of $v_{\mathfrak{p}}$ we use a multiplicative (discrete) valuation $|\cdot|$ on $\overline{K}_{\mathfrak{p}}$, somehow normalized ($|\pi| < 1$).

By Statement 1 all the roots of φ and of ψ have $v_{\mathfrak{p}}$-value $m = h/e$. Hence $|\theta|^e = |\pi|^h = |\beta|^e$ for each root β of ψ. It follows that

$$\theta^e = \pi^h u_\theta, \qquad \beta^e = \pi^h u_\beta$$

for some units u_θ, u_β ($|u_\theta| = |u_\beta| = 1$).

Let $\widehat{T}$ be the unramified (cyclic) extension field of $K_{\mathfrak{p}}$ of degree $\deg(\bar{g})$ (within $\overline{K}_{\mathfrak{p}}$). Note that π is a prime element of $\widehat{T}$. Over the residue class field of $\widehat{T}$ the polynomial $\bar{g}$ decomposes into a product of Galois conjugate linear polynomials, and φ and ψ decompose correspondingly over $\widehat{T}$ (in view of Statement 3). Replace φ by the minimum polynomial of θ over $\widehat{T}$, and replace ψ by the appropriate prime factor over $\widehat{T}$. The polynomials thus obtained will have the same Newton polygon, consisting of one side with slope m, length e and height h, and with the same associated (linear) polynomial mod $\mathfrak{p}$ (Statement 2).

Since $K_{\mathfrak{p}}(\theta) = \widehat{T}(\theta)$ and $K_{\mathfrak{p}}(\beta) = \widehat{T}(\beta)$ for every root β of ψ, without loss of generality we may assume that $K_{\mathfrak{p}} = \widehat{T}$. Then $K_{\mathfrak{p}}(\theta)$ is a totally (and tamely) ramified extension of $K_{\mathfrak{p}}$ of degree $e = \deg(\varphi)$. A similar statement holds for $K_{\mathfrak{p}}(\beta)$ and any root β of ψ. The polynomial $\bar{g}$ being linear (with $\bar{g}(0) \neq 0$) the factors of φ and ψ for the side Σ are pure polynomials

$$X^e - \pi^h u, \qquad X^e - \pi^h \widehat{u},$$

respectively, where u and $\widehat{u}$ are units in $K_{\mathfrak{p}}$ satisfying $u \equiv \widehat{u} \pmod{\mathfrak{p}}$. Thus $|u - \widehat{u}| < 1$. Clearly we may assume that $e > 1$ ($m \neq 0$).

Suppose $\psi = X^e + c_1 X^{e-1} + \cdots + c_{e-1} X + c_e$. Then $c_e = -\pi^h \widehat{u}$ and $v_{\mathfrak{p}}(c_i) > im$ for all $i = 1, \ldots, e-1$. Hence if β is a root of ψ then

$$|c_i \beta^{e-i}| = |c_i| \cdot |\pi|^{(h/e)\cdot(e-i)} < |\pi|^h$$

for $i = 1, \ldots, e-1$. It follows that

$$|\beta^e - \pi^h \widehat{u}| = |c_1 \beta^{e-1} + \cdots + c_{e-1}\beta| < |\pi|^h.$$

Thus $|u_\beta - \widehat{u}| < 1$ for each root β of ψ. By considering φ in place of ψ we get $|u_\theta - u| < 1$ analogously. We infer that

$$|u_\theta - \widehat{u}| \leq \max\{|u_\theta - u|, |u - \widehat{u}|, |\widehat{u} - u_\beta|\} < 1.$$

This yields $|\theta^e - \pi^h\widehat{u}| = |\pi|^h|u_\theta - \widehat{u}| < |\pi|^h$ and so

$$\begin{aligned}|\psi(\theta)| &= |(\theta^e - \pi^h\widehat{u}) + (c_1\theta^{e-1} + \cdots + c_{e-1}\theta)|\\ &\le \max\{|\theta^e - \pi^h\widehat{u}|, \max_{1\le k\le e-1} |c_k\theta^{e-k}|\} < |\pi|^h.\end{aligned}$$

Suppose $\beta_1, \ldots, \beta_e$ are the roots of ψ. We have shown that

$$\prod_{j=1}^{e} |\theta - \beta_j| = |\psi(\theta)| < |\pi|^h.$$

Since $|\theta - \beta_j| \le \max\{|\theta|, |\beta_j|\} = |\pi|^{h/e}$ for all j, there must be some root, say $\beta = \beta_1$, such that $|\theta - \beta| < |\pi|^{h/e}$. We assert that $K_{\mathfrak{p}}(\beta) = K_{\mathfrak{p}}(\theta)$ for this choice of β.

We consider the derivative of ψ at β. Since $\mathfrak{p}$ does not divide e by hypothesis, we have $|e| = 1$. We obtain

$$|\psi'(\beta)| = \frac{1}{|\beta|} \cdot |e\beta^e + (e-1)c_1\beta^{e-1} + \cdots + c_{e-1}\beta| = |\beta|^{e-1} = |\pi|^{(e-1)\cdot h/e}.$$

On the other hand, $|\psi'(\beta)| = \prod_{j=2}^{e} |\beta - \beta_j|$ and $|\beta - \beta_j| \le |\pi|^{h/e}$ for each j. Consequently, $|\beta - \beta_j| = |\pi|^{h/e}$ for all $j = 2, \ldots, e$. But this implies that $|\theta - \beta| < |\beta - \beta_j|$ for all $j \ne 1$. By the lemma of Krasner ([9, p. 159]) this gives $K_{\mathfrak{p}}(\beta) \subseteq K_{\mathfrak{p}}(\theta)$. We must have equality since φ and ψ are irreducible over $K_{\mathfrak{p}}$ of the same degree. ∎

6. The Galois group for a regular side. We are going to prove the Theorem stated in the introduction. Suppose S_m is regular. Without assuming that S_m is tame ($\mathfrak{p}\nmid e$) we can describe the constituent $I_{\mathfrak{P}}^{Z_{f,m}}$ and the quotient $G_{\mathfrak{P}}^{Z_{f,m}}/I_{\mathfrak{P}}^{Z_{f,m}}$ as follows.

PROPOSITION 4. *Suppose* $\bar{f}_S = f_S \bmod \mathfrak{p}$ *is separable. Then* $I_{\mathfrak{P}}^{Z_{f,m}}$ *has exactly* d *orbits, each of size* e, *and is the stabilizer in* $G_{\mathfrak{P}}^{Z_{f,m}}$ *of these orbits. This implies that* $G_{\mathfrak{P}}^{Z_{f,m}}/I_{\mathfrak{P}}^{Z_{f,m}} \cong \mathrm{Gal}_{k_{\mathfrak{p}}}(\bar{f}_S)$ *as permutation groups.*

Proof. By Propositions 1 and 2 both f_m and $\widehat{f}_m$ are separable of degree de, and $\bar{f}_S = \widehat{f}_S \bmod \mathfrak{p}$. From Statement 1 it follows that $Z_{f,m}$ is a block for $G_{\mathfrak{P}}$ and that

$$G_{\mathfrak{P}}^{Z_{f,m}} = \mathrm{Gal}_{K_{\mathfrak{p}}}(\widehat{f}_m).$$

Now let $\widehat{L}$ be the splitting field of $\widehat{f}_m$ over $K_{\mathfrak{p}}$ (with $\widehat{L} \subseteq L_{\mathfrak{P}}$), and let $\widehat{T}|K_{\mathfrak{p}}$ be the maximal unramified subextension. Observe that $I_{\mathfrak{P}}$ maps onto $\mathrm{Gal}(\widehat{L}|\widehat{T})$ under the restriction map. The residue class field of $\widehat{T}$ is "the" splitting field of $\bar{f}_S$ by Statement 3.

By Proposition 2 and Statement 4 the $G_{\mathfrak{p}}$-orbits of $Z_{f,m}$ have length $d_i e$, where d_i denotes the degree of a prime factor of $\bar{f}_S$ ($\sum_i d_i = d$). Each such orbit decomposes under $I_{\mathfrak{P}}$ into d_i (conjugate) orbits of length e. We infer that $I_{\mathfrak{P}}^{Z_{f,m}}$ is the kernel of the action of $G_{\mathfrak{P}}^{Z_{f,m}}$ onto these $I_{\mathfrak{P}}$-orbits. This yields the proposition. ■

Proof of the Theorem. Suppose S_m is regular and $\mathfrak{p}$ does not divide e. Then Proposition 3 applies. This gives assertion (i). It is now obvious that $\widehat{L}$ (notation as above) is also a splitting field for f_m. Furthermore $\mathrm{Gal}_{K_{\mathfrak{p}}}(f_m) \cong \mathrm{Gal}_{K_{\mathfrak{p}}}(\widehat{f}_m)$ as permutation groups, because both agree with $\mathrm{Gal}(\widehat{L}|K_{\mathfrak{p}})$ as groups and have the same degree and the same point stabilizers as permutation groups. This is (ii).

Recall that the compositum of tamely ramified extensions is tamely ramified ([9, II.7.9]). Thus from Proposition 2 we may deduce that $\widehat{L}|K_{\mathfrak{p}}$ is tamely ramified ($\mathfrak{p} \nmid e$). It follows that $\widehat{L}|\widehat{T}$ is cyclic ([9, II.9.15]). Now statements (iii), (iv) of the Theorem are immediate consequences of Proposition 4. ■

7. g-adic Newton polygons. Suppose S_m is *not* regular. Then there is a normalized $\mathfrak{p}$-integral polynomial $g \in K[X]$ whose reduction mod $\mathfrak{p}$ is irreducible and a multiple divisor of f_S mod $\mathfrak{p}$ ($g \nmid f$). Then, as a rule, we proceed by investigating the *g-adic Newton polygon* of f with respect to $\mathfrak{p}$. This is defined via the g-adic expansion $f = \sum_{i=0}^{\widetilde{n}} \alpha_i g^{\widetilde{n}-i}$, $\widetilde{n} = [n/\deg(g)]$, by letting $v_{\mathfrak{p}}(\alpha_i)$ be the minimum of the $v_{\mathfrak{p}}$-values of the coefficients of the polynomial $\alpha_i = \alpha_i(X) \in K[X]$ ($\deg(\alpha_i) < \deg(g)$).

There is a parallel theory for g-adic polygons (cf. [10] and [7]). However, after passage to the unramified extension of $K_{\mathfrak{p}}$ of degree $\deg(g)$ we are led to expansions with regard to linear polynomials. Of course, this is most convenient (also for computations) in case g itself is linear, that is, $g = X - u$ for some $\mathfrak{p}$-unit $u \in K$. Then we just have to examine the standard polygon of $\widetilde{f}(X) = f(X+u)$. Note that $\mathrm{Gal}_K(\widetilde{f}) \cong \mathrm{Gal}_K(f)$. We give some typical examples.

Example 1. Let f be the pth cyclotomic polynomial over $K = \mathbb{Q}$ and $\mathfrak{p} = p\mathbb{Z}$ ($n = p-1$). The standard Newton polygon of f with respect to $\mathfrak{p}$ is a side with slope 0. Here $f \equiv (X-1)^n \pmod{p}$ so that we should consider the standard polygon of $\widetilde{f}(X) = f(X+1)$. It consists of one side $S = S_m$ with slope $m = 1/n$. So $\widetilde{f}_S$ is linear and $\widetilde{f}_m = X^n + p$. From the Theorem we deduce the (known) result that $\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p(\sqrt[p-1]{-p})$ is the pth cyclotomic field over the p-adics.

Example 2. Let p be an odd prime and let $h \in \mathbb{Z}[X]$ be a normalized polynomial of degree p which is Eisenstein with respect to p. Then h is irreducible over $\mathbb{Q}_p$. Let π be a root of h and $K = \mathbb{Q}(\pi)$. Then $K_{\mathfrak{p}}|\mathbb{Q}_p$ is totally and wildly ramified and $v_{\mathfrak{p}}(\pi) = 1$, $\mathfrak{p}$ being the unique prime of K above p. Now suppose that p^2 does not divide $a = h'(0)$ (like $h(0)$).

Let $f(X) = h(X)/(X-\pi)$, and let $\widetilde{f}(X) = f(X+\pi)$. This $\widetilde{f}$ is normalized of degree $n = p-1$ with $\widetilde{f}(0) = h'(\pi) = au$ for some principal unit u of $K_{\mathfrak{p}}$. Use the fact that p divides $\binom{p}{k}$ for $1 \leq k < p$. This also implies that the (standard) Newton polygon of $\widetilde{f}$ is a side of length $p-1$ and height $p = v_{\mathfrak{p}}(\widetilde{f}(0))$. Hence the Theorem applies (Corollary 2). In this case the Newton polygon of f itself would not give any useful information. Since u is a $(p-1)$th power in $K_{\mathfrak{p}}$ we infer that $\widehat{L} = K_{\mathfrak{p}}(\sqrt[p-1]{-a})$ is a root field for $\widetilde{f}$ and f and has degree $p-1$ over $K_{\mathfrak{p}}$. In particular $[\widehat{L} : \mathbb{Q}_p] = p(p-1)$. Since $\mathrm{Gal}_{\mathbb{Q}_p}(h)$ is a solvable subgroup of the symmetric group of degree p, a theorem of Galois now ensures that it must be the full affine group $\mathrm{AGL}_1(p)$ (Corollary 3.5B in [3]). It follows that $\widehat{L} = \mathbb{Q}_p(\pi, \sqrt[p-1]{-a})$ is the splitting field of h over $\mathbb{Q}_p$.

It follows from the classification of the finite simple groups that, for $p \geq 5$, the affine group $\mathrm{AGL}_1(p)$ is a maximal subgroup of the symmetric group $\mathrm{Sym}(p)$ (see [3, p. 99 and Sect. 7.7]). Hence $\mathrm{Gal}_{\mathbb{Q}}(h)$ is either the affine group or the symmetric group.

Example 3. Let $n \geq 5$ be a rational prime and b a rational integer not divisible by n. Let $f = X^n + aX + a$ over $K = \mathbb{Q}$ where $a = bn$. This Eisenstein trinomial has been studied by several authors. From Example 2 we know that $G = \mathrm{Gal}_{\mathbb{Q}}(f)$ is either the affine group or the symmetric group. By examining the discriminant of a root field defined by f (computed in [5]) the Wegener–Hasse theorem [4] shows that $G = \mathrm{AGL}_1(p)$ if and only if the splitting field L of f contains the nth roots of unity (see also Movahhedi [8] for an alternative approach). Let p be a prime dividing

$$D = n^{n-1} + b(n-1)^{n-1}.$$

This D is a divisor of the discriminant of f, but we do not use that. Note that $D \equiv b \pmod n$ and that p does not divide $2bn(n-1)$. The standard polygon of f with respect to $\mathfrak{p} = p\mathbb{Z}$ is a side with slope 0.

We have $f' = nX^{n-1} + a$ and so $nf(X) - Xf'(X) = a(n-1)X + na$. Hence the greatest common divisor of f and f' mod p is either 1 or $X - u \bmod p$, where $u = -n/(n-1)$ is a rational p-adic unit. We check that $v_p(f(u)) = v_p(f'(u)) = v_p(D)$ (> 0) and $v_p(f''(u)) = 0$. This implies (directly) that $f \bmod p$ is inseparable. We have all the necessary information about the standard Newton polygon of $\widetilde{f}(X) = f(X+u)$ with respect to $\mathfrak{p}$ (Taylor). It consists of a side with slope 0 and length $n-2$, and a side S_m with slope $m = v_p(D)/2$ and length 2. For the side S_m we get $\widetilde{f}_m = X^2 - c$ where

$$c = 4uD/(n^{(n-1)/2}(n-1))^2.$$

Note that $v_p(c) = v_p(D)$. The associated polynomial (picking $\pi = p$) is either $\widetilde{f}_S = X - c/p^{v_p(D)}$ or $\widetilde{f}_S = X^2 - c/p^{v_p(D)}$, depending on whether $v_p(D)$ is odd or even. In any case, $\widetilde{f}_S$ is separable mod p, and the Theorem applies. The polynomial associated to the side with slope 0, which agrees with its factor, must be separable mod p as well.

If $v_p(D)$ is odd, c is not a square in $\mathbb{Q}_p$. We conclude that $I_{\mathfrak{P}}$ is generated by a transposition on $Z_{\widetilde{f}}$. Since $G \cong \mathrm{Gal}_{\mathbb{Q}}(\widetilde{f})$ is a primitive permutation group (of prime degree), $G = \mathrm{Sym}(n)$ is the symmetric group by a theorem of Jordan ([3, Theorem 3.3A]).

So let $v_p(D)$ be even. Then $I_{\mathfrak{P}} = 1$ and $G_{\mathfrak{P}}$ has either two fixed points or an orbit of length 2 on $Z_{\widetilde{f}}$, depending on whether c, that is, uD, is a square in $\mathbb{Q}_p$ or not. Assume G is the affine group (so that $\mathbb{Q}(\zeta_n) \subseteq L$). In the first case we then must have $G_{\mathfrak{P}} = 1$, because G is a Frobenius group. In this case p splits completely in $\mathbb{Q}(\zeta_n) \subseteq L$ and so $p \equiv 1 \pmod{n}$. In the second case $G_{\mathfrak{P}}$ is generated by a product of $(n-1)/2$ disjoint transpositions on $Z_{\widetilde{f}}$, hence has order 2 even when restricted to $\mathbb{Q}(\zeta_n)$. This implies that $p \equiv -1 \pmod{n}$.

Remark. It is conjectured that $G = \mathrm{Gal}_{\mathbb{Q}}(X^n + aX + a)$ is always the full symmetric group ($n \geq 5$ a prime dividing the integer a exactly to the first power). We have just shown that this is true if $|D|$ is not a rational square or if D has a prime divisor $p \not\equiv \pm 1 \pmod{n}$. Such a prime divisor is, for instance, $p = 3$ if $n \equiv 2 \pmod{3}$ and $a \equiv 1 \pmod{3}$. We also have $G = \mathrm{Sym}(n)$ if a is odd or if $a \equiv 2 \pmod{3}$. To see this use the fact that $X^n + aX + a$ mod 2 is separable and has no root in $\mathbb{F}_2$ if a is odd, and that the analogous statement holds mod 3 in the other case. Thus from $G = \mathrm{AGL}_1(n)$ it would follow that the polynomial is even irreducible mod 2 resp. 3. This would imply that $G_{\mathfrak{P}}$, for $\mathfrak{P}$ over $p = 2$ resp. 3, is the (cyclic) normal subgroup of order n in G and that 2 or 3 split completely in $\mathbb{Q}(\zeta_n) \subseteq L$, which is impossible.

One also knows that $G = \mathrm{Sym}(n)$ if $D < 0$ or, more generally, if $a < n^2$. No example is known so far where $G \neq \mathrm{Sym}(n)$.

References

[1] E. Brieskorn und H. Knörrer, *Ebene algebraische Kurven*, Birkhäuser, Basel, 1981.

[2] S. D. Cohen, A. Movahhedi and A. Salinier, *Double transitivity of Galois groups of trinomials*, Acta Arith. 82 (1997), 1–15.

[3] J. D. Dixon and B. Mortimer, *Permutation Groups*, Springer, Berlin, 1996.

[4] H. Hasse, *Über die Diskriminante auflösbarer Körper von Primzahlgrad*, J. Reine Angew. Math. 176 (1936), 12–17.

[5] P. Llorente, E. Nart and N. Vila, *Discriminants of number fields defined by trinomials*, Acta Arith. 43 (1984), 367–373.

[6] B. H. Matzat, *Konstruktive Galoistheorie*, Lecture Notes in Math. 1284, Springer, 1987.

[7] J. Montes and E. Nart, *On a theorem of Ore*, J. Algebra 146 (1992), 318–334.

[8] A. Movahhedi, *Galois group of $X^p + aX + a$*, ibid. 180 (1996), 966–975.

[9] J. Neukirch, *Algebraische Zahlentheorie*, Springer, Berlin, 1992.

[10] Ö. Ore, *Newtonsche Polygone in der Theorie der algebraischen Körper*, Math. Ann. 99 (1928), 84–117.

[11] B. L. van der Waerden, *Die Zerlegungs- und Trägheitsgruppe als Permutationsgruppen*, ibid. 111 (1937), 731–733.

Mathematisches Institut
Universität Tübingen
Auf der Morgenstelle 10
D-72076 Tübingen, Germany
E-mail: peter.schmid@uni-tuebingen.de

Received on 24.9.2003 (4628)