ACTA ARITHMETICA
140.1 (2009)

Correction to "Computing Galois groups by means of Newton polygons"

(Acta Arith. 115 (2004), 71–84)

by

Michael Kölle and Peter Schmid (Tübingen)

The last statement of the (main) theorem in the above joint paper, cited as [KS], is not stated correctly. The error comes from Proposition 4 in [KS], because the residue class field of $\widehat{T}$ merely *contains* the splitting field of the *associated polynomial* $\bar{f}_S$ (page 80). We use the notations and conventions introduced in [KS]. In particular, we assume that the side $S = S_m$ with slope $m = h/e$ of the Newton polygon of the normalized polynomial $f \in K[X]$ with respect to the finite prime $\mathfrak{p}$ of the number field K is *regular* ($\bar{f}_S$ separable over the residue class field $k_{\mathfrak{p}}$) and *tame* ($\mathfrak{p} \nmid e$). Let then $\omega = \mathrm{o}(\mathrm{N}\mathfrak{p} \bmod e)$ be the order of the absolute norm $\mathrm{N}\mathfrak{p} = |k_{\mathfrak{p}}|$ of $\mathfrak{p}$ in $(\mathbb{Z}/e\mathbb{Z})^*$, and let the distinct normalized prime factors of $\bar{f}_S$ over $k_{\mathfrak{p}}$ have degrees $d_1, \ldots, d_r$ (so that $\sum_{i=1}^{r} d_i = d = \deg(\bar{f}_S)$).

Recall that by part (iii) of the theorem in [KS] the inertia group $I_{\mathfrak{P}}^{Z_{f,m}}$ equals $\langle\tau\rangle$ where τ is the product of d disjoint e-cycles on the roots $Z_{f,m}$. Part (iv) should read as follows:

(iv) *The constituent* $G_{\mathfrak{P}}^{Z_{f,m}} = \langle\sigma, \tau\rangle$ *has just* r *orbits of sizes* $d_1 e, \ldots, d_r e$ *and is a metacyclic group, with* $\sigma^{-1}\tau\sigma = \tau^{\mathrm{N}\mathfrak{p}}$. *The order of the* (*cyclic*) *group* $G_{\mathfrak{P}}^{Z_{f,m}}/I_{\mathfrak{P}}^{Z_{f,m}}$ *is divisible by* $\mu = \mathrm{lcm}(\omega, d_1, \ldots, d_r)$, *and it is a divisor of* $\mu \cdot e$. *This order is equal to* μ *if* $e = 1$ *and* $d = 1$, *and if* $r = 1$ *and* $\gcd(\omega, d) = 1$.

The first assertion follows from Proposition 2 in [KS] (essentially due to Ore). By parts (i), (ii) of the theorem $\widehat{f}_m$, having the set $Z_{f,m}$ of zeros, and the *factor* f_m to the side S have the same splitting field $\widehat{L}_m \subseteq \overline{K}_{\mathfrak{p}}$, and we may identify $G_{\mathfrak{P}}^{Z_{f,m}}$ with the Galois group $G_m = \mathrm{Gal}(\widehat{L}_m|K_{\mathfrak{p}})$ acting on

2010 *Mathematics Subject Classification*: 11R32, 20B25.
Key words and phrases: Galois groups, Newton polygons.

DOI: 10.4064/aa140-1-7

the roots of f_m. Let $\widehat{T}$ be the maximal subfield of $\widehat{L}_m$ unramified over $K_{\mathfrak{p}}$. We identify $I_{\mathfrak{P}}^{Z_{f,m}}$ with $I_m = \mathrm{Gal}(\widehat{L}_m|\widehat{T})$ (acting on the roots of f_m). By assumption $\widehat{L}_m|K_{\mathfrak{p}}$ is a tame extension. It is well known that $G_m/I_m \cong \mathrm{Gal}(\widehat{T}|K_{\mathfrak{p}})$ is cyclic, generated by the inverse image $I_m\sigma$ of the Frobenius automorphism over $k_{\mathfrak{p}}$, and that $\sigma^{-1}\tau\sigma = \tau^{\mathrm{N}\mathfrak{p}}$.

Observe that $\omega = [K_{\mathfrak{p}}(\varepsilon) : K_{\mathfrak{p}}]$ where ε is a primitive eth root of unity. We assert that $\varepsilon \in \widehat{T}$. Of course $K_{\mathfrak{p}}(\varepsilon)|K_{\mathfrak{p}}$ is unramified ($\mathfrak{p} \nmid e$). Recall that $\deg(f_m) = \ell = de$ equals the length of S and that f_m is a polynomial in X^e. Indeed, by construction, or in view of Hensel's lemma, there is a unique normalized lift $f_S \in K_{\mathfrak{p}}[X]$ of $\bar{f}_S$ such that

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

where π is the fixed element of K with order 1 at $\mathfrak{p}$. Hence if θ is a root of f_m (in $\widehat{L}_m$) so is $\varepsilon^i\theta$ for each integer i, giving the assertion. Moreover, $\pi^{-h}\theta^e$ is then a root of f_S. If $\pi^{-h}\theta^e = \pi^{-h}\beta^e$ for some other root β of f_m, then β/θ is an eth root of unity and so $\beta = \varepsilon^i\theta$ for some integer i. For $\tau \in I_m$ we have $(\theta^\tau)^e = (\theta^e)^\tau = \theta^e$. We conclude that $\{\varepsilon^i\theta : 1 \le i \le e\}$ is the orbit of θ under I_m. Since there are just $d = \deg(f_S)$ such orbits, we deduce that each root of f_S is of the form $\pi^{-h}\theta^e$ for some root θ of f_m. It follows that $[\widehat{T} : K_{\mathfrak{p}}]$ is divisible by μ.

Let T be the (unique) subfield of $\widehat{T}$ such that $[T : K_{\mathfrak{p}}] = \mu$. We know that $\varepsilon \in T$ and that, for each root θ of f_m, we have $\theta^e = \pi^h u_\theta$ for some unit $u_\theta \in U_T$ in T, which is a root of f_S in T. By separability of $\bar{f}_S = f_S \bmod \mathfrak{p}$ these u_θ belong to d distinct elements in k_T^*, where k_T is the residue class field of T. From $\mathfrak{p} \nmid e$ we infer that $U_T/U_T^e \cong k_T^*/k_T^{*e}$ is cyclic (of order e). Observe that π is a prime in T and that $\gcd(e,h) = 1$. Combining Proposition 2 in [KS] with Abhyankar's lemma and (abelian) Kummer theory we see that, for any root θ of f_m, the polynomial $X^e - \pi^h u_\theta$ is irreducible over T and that $T(\theta)|T$ is a cyclic totally ramified extension of degree e with $T(\theta)\widehat{T} = \widehat{L}_m$. In this manner we recover part (iii) of the theorem in [KS]. Now $\widehat{L}_m|T(\theta)$ is cyclic of degree $[\widehat{T} : T]$, and $\widehat{L}_m$ is the compositum of all these $T(\theta)$. We conclude that the degree $[\widehat{T} : T]$ is a divisor of e. Hence $|G_m/I_m| = [\widehat{T} : K_{\mathfrak{p}}]$ divides $\mu \cdot e$.

It is obvious that $T = \widehat{T}$ if $e = 1$ or $d = 1$. Suppose that $r = 1$ and $\gcd(\omega, d) = 1$. Then $\bar{f}_S$ is (even) irreducible over the residue class field of $K_{\mathfrak{p}}(\varepsilon)$, which has order $(\mathrm{N}\mathfrak{p})^\omega \equiv 1 \pmod{e}$. Hence the roots $u_\theta = \pi^{-h}\theta^e$ of f_S are conjugate over $K_{\mathfrak{p}}(\varepsilon)$ and so belong to the same class in U_T/U_T^e. Apply Kummer theory.

Whereas Corollary 1 to the theorem in [KS] is true as it stands ($e = 1$), Corollary 2 has to be modified. Here we have $d = 1$ ($\ell = e$), so that G_m/I_m

is cyclic of order $\omega = \mathrm{o}(\mathrm{N}\mathfrak{p} \bmod e)$. For $e \neq 1 \neq d$ it can happen that $|G_m/I_m| > \mu$; an example with $e = 2 = d$ (and $m = 1/2$) is provided by $f_m = X^4 - 2 \cdot 7^2$ over $\mathbb{Q}_7$ ($\pi = 7$).

NOTE. Let us say that two normalized polynomials φ, ψ in $K_\mathfrak{p}[X]$ (of the same degree) belong to the same *Ore class* provided their Newton polygon (with respect to $v_\mathfrak{p}$) is the same and consists of one straight line S such that the associated polynomials $\overline{\varphi}_S = \overline{\psi}_S$ agree. This means that the points on the line S resulting from φ, ψ are the same and that the corresponding coefficients only differ by principal units in $K_\mathfrak{p}$. The statements of the theorem, for regular and tame S, only depend on the Ore class of the polynomials.

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

Received on 26.3.2009
and in revised form on 16.6.2009 (5983)