,

DETERMINATION OF THE NUMBER OF ISOMORPHISM CLASSES OF EXTENSIONS OF A $\mathfrak{p}$-ADIC FIELD

MAURIZIO MONGE

Abstract. We deduce a formula enumerating the isomorphism classes of extensions of a $\mathfrak{p}$-adic field K with given ramification e and inertia f. The formula follows from a simple group-theoretic lemma, plus the Krasner formula and an elementary class field theory computation. It shows that the number of classes only depends on the ramification and inertia of the extensions $K/\mathbb{Q}_p$, and $K(\zeta_{p^m})/K$ obtained adding the p^m-th roots of 1, for all p^m dividing e.

Résumé

Calcul du nombre des classes d'isomorphisme des extensions d'un corps $\mathfrak{p}$-adique. On donne une formule pour l'énumeration des classes d'isomorphisme des extensions d'un corps $\mathfrak{p}$-adique K à ramification e et inertie f. La formule est obtenue par un lemme de théorie des groupes, plus une formule de Krasner et un simple calcul de théorie des corps de classe. Elle preuve que le nombre des classes dépends seulement de la ramification et de l'inertie des extensions $K/\mathbb{Q}_p$, et $K(\zeta_{p^m})/K$ obtenues en ajoutant à K les racines de l'unité d'ordre p^m, pour p^m divisant e.

Let K be a finite extension of $\mathbb{Q}_p$ with residue field $\bar{K}$. Let $n_0 = [K : \mathbb{Q}_p]$, and let respectively $e_0 = e(K/\mathbb{Q}_p)$ and $f_0 = f(K/\mathbb{Q}_p)$ be the absolute ramification index and inertia degree. Formulas for the total number of extensions with given degree in a fixed algebraic closure were computed by Krasner and Serre [1, 3], as well as formulas counting all totally ramified extensions and totally ramified extension with given valuation of the discriminant.

We will show how it is possible to modify such formulas to enumerate the isomorphism classes of extensions with fixed ramification and inertia, with some help from class field theory. We intend to show in a forthcoming paper the application of this method to the determination of the number classes of totally ramified extensions with given discriminant, when possible.

The problem of enumerating isomorphism classes of $\mathfrak{p}$-adic field had been solved in a special case by Hou-Keating [5] for extensions with ramification e satisfying $p^2 \nmid e$, with a partial result when $p^2 \parallel e$.

1. Group theoretic preliminaries

For $k \geq 1$, let $C_k \cong \mathbb{Z}/k\mathbb{Z}$ be the cyclic group of order k. For natural n and a group G having a finite number of subgroups with index n, let $\mathfrak{I}_n$ denote the number of conjugacy classes of subgroups of G with index n, possibly restricting to subgroups satisfying some fixed conjugation-independent property. For a finite group Q, let $\mathfrak{T}_n(Q)$ denote the number of two-steps chains of subgroups $H \lhd J \leq G$ such that $(G : H) = n$, H is normal in J with $J/H \cong Q$ and satisfies the same restrictions imposed above.

Lemma 1.1. *For a group G with a finite number of subgroups of index n we have*

$$\mathfrak{I}_n = \frac{1}{n} \sum_{d|n} \phi(d) \mathfrak{T}_n(C_d). \tag{1}$$

2000 *Mathematics Subject Classification.* 11S15, 12B25.

Proof: For fixed $H \leq G$ with $(G : H) = n$, let's compute the contribute of the chains of the form $H \lhd J \leq G$. All the admissible J are contained in the normalizer $N_G(H)$, and the number of subgroups in $N_G(H)/H$ isomorphic to C_d multiplied by $\phi(d)$ counts the number of elements of $N_G(H)/H$ with order precisely equal to d. The contribute for all possible d is hence equal to $(N_G(H) : H)$, and having H precisely $(G : N_G(H))$ conjugates its conjugacy class contributes n to the sum, i.e. 1 to the full expression. □

The absolute Galois group of a $\mathfrak{p}$-adic field has only a finite number of closed subgroups with fixed index, and by Galois theory the formula (1) can be interpreted denoting with $\mathfrak{I}_n$ the number of isomorphism classes of extensions L/K of degree n over a fixed field K, and with $\mathfrak{T}_n(Q)$ the number of all towers $L/F/K$ such that $[L : K] = n$, and L/F is Galois with group isomorphic to Q. Similarly, the above formula can be used to count, say, extensions with prescribed ramification and inertia, all the extensions of given degree, or totally ramified extensions with prescribed valuation of the different, applying the same restriction when enumerating the towers.

The above formula can be applied to local fields with great effectiveness because the number of cyclic extension with prescribed ramification and inertia (which will be carried over in the next section) has little dependence on the particular field taken into account, and only depends on the absolute degree over $\mathbb{Q}_p$, the absolute inertia, and the p-part of the group of the roots of the unity.

2. On the number of cyclic extensions

In this section we briefly deduce via class field theory the number $\mathfrak{C}(F, e, f)$ of cyclic extensions of a $\mathfrak{p}$-adic field F with prescribed ramification e, inertia f and degree $d = ef$, and the number $\mathfrak{C}(F, d)$ of all cyclic extension of degree d, for any d.

By class field theory (see [2, 4]), the maximal abelian extension with exponent d has Galois group isomorphic to the biggest quotient of $F^\times$ which has exponent d, and consequently its Galois group is isomorphic to $F^\times/(F^\times)^d$. Furthermore, the upper numbering ramification groups are the images of the principal units $U_0, U_1, \ldots$ under this isomorphism.

The choice of a uniformizer π provides a factorization $F = \langle \pi \rangle \times U_0$, and as is well known [4, see (3) of Cor. 6.5, and also Prop. 5.4 and Cor. 7.3], U_0 is isomorphic to the direct product of the group of the roots of the unity μ_F and a free $\mathbb{Z}_p$ module with rank $m = [F : \mathbb{Q}_p]$. Consequently calling G the Galois group of the maximal abelian extension with exponent d we have

$$G \cong C_d \times C_z \times C_{p^r}^m \times C_{p^{\min\{\xi,r\}}}, \qquad G^0 \cong \{1\} \times C_z \times C_{p^r}^m \times C_{p^{\min\{\xi,r\}}}$$

where $d = p^r k$ with $(d, k) = 1$, z is the g.c.d. of k and the order $|\bar{F}^\times| = p^{f(F/\mathbb{Q}_p)} - 1$ of the group of the roots of the unity with order prime with p, and ξ is the integer such that p^ξ is the order of the group of the roots of the unity with p-power order.

The number of subgroups $H \subseteq G$ such that $G/H \cong C_d$ and $G/(HG^0) \cong C_f$ will be computed using the duality theory of finite abelian groups. Let $\hat{G} = Hom(G, \mathbb{Q}/\mathbb{Z})$, and for each subgroup H of G put $H^\perp = \{\phi \in \hat{G} : \phi(x) = 0, \text{ for } x \in H\} \cong \widehat{G/H}$.

The conditions on H amounts to having $H^\perp \cong C_d$, and $(HG^0)^\perp = H^\perp \cap (G^0)^\perp \cong C_f$. Since we have (non-canonically) that

$$(G^0)^\perp \cong C_d \times \{1\} \times \{1\} \times \{1\} \subseteq C_d \times C_z \times C_{p^r}^m \times C_{p^{\min\{\xi,r\}}} \cong \hat{G},$$

we must count the number of subgroups isomorphic to C_d, generated by an element of the form (x, y) with $x \in C_d$ and $y \in C_z \times C_{p^r}^m \times C_{p^{\min\{\xi,r\}}}$ say, such that the intersection with $(G^0)^\perp$ is isomorphic to C_f. Since $e \cdot x$ needs to have order f, writing $C_d \cong C_{f(f,e)} \times C_{e/(e,f)}$ we see that the component in the first factor can be chosen in $\phi(f \cdot (f,e))$ ways, while the second component can be chosen arbitrarily in $e/(e,f)$ ways, so we have $e\phi(f)$ possibilities.

The y coordinate on the other hand should have order precisely equal to e, which we write $e = p^s h$ with $(h,p) = 1$, and this is impossible if $h \nmid z$, while if $h \mid z$ we have

$$\phi(h) \cdot \Pi_p(m, s, \xi)$$

possibilities for y, where for all p, m, s, ξ we define for convenience

$$\Pi_p(m,s,\xi) = \begin{cases} 1 & \text{if } s = 0, \\ p^{ms+\min\{\xi,s\}} - p^{m(s-1)+\min\{\xi,s-1\}} & \text{if } s > 0, \end{cases} \tag{2}$$

which counts the number of elements of order p^s in a group for the form $C_{p^r}^m \times C_{p^{\min\{\xi,r\}}}$ (for any $r \geq s$).

Since we counted the number of good generators, to obtain the number of good groups we must divide by $\phi(ef)$ obtaining

$$\mathfrak{C}(F,e,f) = \frac{e\phi(h)\phi(f)}{\phi(ef)} \cdot \Pi_p(m,s,\xi) \tag{3}$$

if $h \mid (p^{f(F/\mathbb{Q}_p)} - 1)$, while $\mathfrak{C}(F,e,f) = 0$ if $h \nmid (p^{f(F/\mathbb{Q}_p)} - 1)$.

The total number of cyclic extensions of degree $d = p^r k$ can be deduced similarly, considering that

$$G \cong C_k \times C_z \times C_{p^r}^{m+1} \times C_{\min\{\xi,r\}}.$$

Let's consider the function $\psi(u,v)$ which for natural u,v counts the number of elements with order u in the group $C_u \times C_v$, and can be expressed as

$$\psi(u,v) = u \cdot (u,v) \cdot \prod_{\substack{\ell \text{ prime} \\ \ell \mid u/(u,v)}} \left(1 - \frac{1}{\ell}\right) \cdot \prod_{\substack{\ell \text{ prime} \\ \ell \mid u,\ \ell \nmid u/(u,v)}} \left(1 - \frac{1}{\ell^2}\right). \tag{4}$$

A computation similar to what done above tells us that the total number of C_d-extensions is

$$\mathfrak{C}(F,d) = \frac{\psi(k, p^{f(K/\mathbb{Q}_p)} - 1)}{\phi(d)} \cdot \Pi_p(m+1, r, \xi). \tag{5}$$

3. The formula for the number of isomorphism classes of extensions

Let's recall Krasner formula for the number $\mathfrak{N}(K,e,f)$ of extensions of K with ramification $e = p^s h$ (with $(p,h) = 1$) and inertia f, which can be written as

$$\mathfrak{N}(K,e,f) = eR_p(s, n_0 hf),$$

where for natural m, s the quantity $R_p(m,s)$ is defined as

$$R_p(m,s) = \begin{cases} 1 & \text{if } s = 0, \\ p^{mp^{s-1}+1} R_p(m, s-1) - p + 1 & \text{if } s > 0. \end{cases} \tag{6}$$

If we ignore for a moment the dependence of $\mathfrak{C}(F,e,f)$ on the group of p-power roots of the unit, we can count the number of isomorphism classes of extensions iterating on all the towers $L/F/K$ with F/K having ramification e' and inertia f', and L/F Galois cyclic with ramification e'' and inertia f'', with $e'e'' = e$ and $f'f'' = f$. Indicating with $F^{e',f'}$ a generic extension with ramification e' and inertia

f' over K, we obtain

$$\begin{aligned}\mathfrak{I}(K,e,f) &= \frac{1}{n}\sum_{\substack{f'f''=f\\ e'e''=e}} \phi(e''f'')\cdot\mathfrak{N}(K,e',f')\cdot\mathfrak{C}(F^{e',f'},e'',f'')\\ &= \frac{1}{f}\sum_{\substack{f'f''=f\\ e'e''=e\\ h''\left|\left(p^{f_0 f'}-1\right)\right.}} \phi(h'')\phi(f'')\cdot R_p(n_0h'f',s')\cdot\Pi_p(n_0e'f',s'',\xi),\end{aligned}$$

where in all the sum we always put $e'=p^{s'}h'$, $e''=p^{s''}h''$ with $(p,h')=(p,h'')=1$.

But unluckily the ξ is not well defined (and depends on the particular extension F/K), and if we start putting $\xi=0$ while counting all the towers $L/F/K$, each factor $\Pi_p(\cdot,\cdot,0)$ should be corrected by a term $\Pi_p(\cdot,\cdot,1)-\Pi_p(\cdot,\cdot,0)$ for all towers with $F\supseteq K(\zeta_p)$, another correction term $\Pi_p(\cdot,\cdot,2)-\Pi_p(\cdot,\cdot,1)$ is required for all $F\supseteq K(\zeta_{p^2})$, and so on.

Consequently, if we define for convenience

$$\Delta_p(m,s,i)=\begin{cases}\Pi_p(m,s,0) & \text{if } i=0,\\ \Pi_p(m,s,i)-\Pi_p(m,s,i-1) & \text{if } i>0,\end{cases} \tag{7}$$

where Π_p is defined in (2), we have

Theorem 3.1. *The number of isomorphism classes of extensions with ramification e and inertia f of a field K of absolute degree $n_0=[K:\mathbb{Q}_p]$ and absolute inertia $f_0=f(K/\mathbb{Q}_p)$ is*

$$\mathfrak{I}(K,e,f)=\frac{1}{f}\sum_{\substack{0\le i\le s\\ f'f''f^{(i)}=f\\ e'e''e^{(i)}=e\\ h''\left|\left(p^{f_0f^{(i)}f'}-1\right)\right.}} \frac{\phi(h'')\phi(f'')}{e^{(i)}}\cdot R_p(n_0h'f',s')\cdot\Delta_p(n_0n^{(i)}e'f',s'',i),$$

where R_p and Δ_p are respectively defined in the (6) *and* (7)*, we have put*

$$e^{(i)}=e(K(\zeta_{p^i})/K),\quad f^{(i)}=f(K(\zeta_{p^i})/K),\quad n^{(i)}=e^{(i)}f^{(i)},$$

and where throughout the sum we have put

$$e=p^sh,\quad e'=p^{s'}h',\quad e''=p^{s''}h''$$

with h,h',h'' all prime with p.

Remark 1. *When $s=0$ (i.e. $p\nmid e$) the formula has the much simpler form*

$$\begin{aligned}\mathfrak{I}(K,e,f) &= \frac{1}{f}\sum_{\substack{f'f''=f\\ e'e''=e\\ e''\left|\left(p^{f_0f'}-1\right)\right.}} \phi(f'')\cdot\phi(e'')\\ &= \frac{1}{f}\sum_{f'f''=f}\phi(f'')\cdot\left(e,p^{f_0f'}-1\right)=\frac{1}{f}\sum_{i=0}^{f-1}\left(e,p^{f_0(f',i)}-1\right),\end{aligned}$$

which is precisely the formula obtained in [5, Remark 4.2, pag. 27].

With a computation similar to what done for Theorem 3.1, we obtain

Theorem 3.2. *The total number of isomorphism classes of extensions with degree n of a field K of absolute degree $n_0 = [K : \mathbb{Q}_p]$ and absolute inertia $f_0 = f(K/\mathbb{Q}_p)$ is*

$$\mathfrak{I}(K,n) = \frac{1}{n} \sum_{\substack{0 \le i \le t \\ de'f'n^{(i)}=n}} e'\psi(k, p^{f_0 f^{(i)} f'} - 1) \cdot R_p(n_0 n^{(i)} h' f', s') \cdot \Delta_p(n_0 n^{(i)} e' f' + 1, r, i),$$

where we are keeping the same notation as in Theorem 3.1, $\psi(u,v)$ is defined in the (4), p^t is the biggest power of p dividing n, and moreover throughout the sum we have written $d = p^r k$ with $(k,p) = 1$.

Acknowledgements

We wish to thank Sara Checcoli, Roberto Dvornicich, Vincenzo Mantova and Dajano Tossici for helpful discussions and help while writing this note.

References

[1] M. Krasner, *Nombre des extensions d'un degré donné d'un corps p-adique*, CR Acad. Sc. Paris **254** (1962), 3470–3472, *ibidem* **255** (1962), 224–226, 1682–1684, 2342–2344, 3095–3097.

[2] J.P. Serre, *Local fields*, Springer, 1979.

[3] J.P. Serre, *Une formule de masse pour les extensions totalement ramifiées de degré donné dun corps local*, CR Acad. Sci. Paris AB **286** (1978).

[4] I.B. Fesenko and SV Vostokov, *Local fields and their extensions*, American Mathematical Society, 2002.

[5] X. Hou and K. Keating, *Enumeration of isomorphism classes of extensions of p-adic fields*, Journal of Number Theory **104** (2004), no. 1, 14–61.

E-mail address: maurizio.monge@gmail.com

Scuola Normale Superiore di Pisa - Piazza dei Cavalieri, 7 - 56126 Pisa