Local discriminants, kummerian extensions, and elliptic curves

Chandan Singh Dalawat

Harish-Chandra Research Institute
Chhatnag Road, Jhunsi, Allahabad 211019, India
Email : dalawat@gmail.com

Abstract. Starting from Stickelberger’s congruence for the absolute discriminant of a number field, we ask a series of natural questions which ultimately lead to an orthogonality relation for the ramification filtration on \( K(\sqrt{K^\times}) \), where \( K \) is any finite extension of \( \mathbb{Q}_p \) containing a primitive \( p \)-th root of \( 1 \). An extensive historical survey of discriminants and primary numbers is included. Among other things, we give a direct proof of Serre’s mass formula in the case of quadratic extensions. Incidentally, it is shown that every unit in a local field is the discriminant of some elliptic curve.

Keywords : Stickelberger’s congruence, discriminants, primary numbers, local fields, ramification filtration, cyclic extensions, Serre’s mass formula, Kummer pairing, elliptic curves.

Die hier charakterisierte neue Theorie der algebraischen Zahlen […] scheint mir auch aus dem Grunde ein brauchbares Hilfsmittel für arithmetische Untersuchungen zu sein, weil mit ihrer Hilfe Fragen der Zahlentheorie vollständig und einfach gelöst werden können, deren Beantwortung mit den bisherigen Methoden entweder überhaupt nicht gelang, oder doch bedeutende Schwierigkeiten bereitete. — Kurt Hensel [24, p. 70].

Stickelberger showed that if the discriminant \( D \) of a degree-\( n \) number field \( \Omega \) is not divisible by an odd prime \( p \), then \( D \) becomes a square in \( \mathbb{F}_p^\times \) if and only if \( n - m_p \) is even, where \( m_p \) is the number of places of \( \Omega \) above \( p \). If 2 does not divide \( D \), then \( D \equiv 1 \pmod{8} \) if \( n - m_2 \) is even, \( \equiv 5 \pmod{8} \) if \( n - m_2 \) is odd.

Hensel showed that these global results are immediate consequences of purely local ones. We give the relative versions of Hensel’s local results : the base field is no longer \( \mathbb{Q}_p \), but a finite extension \( K \) thereof (prop. 15). Along the way, we also specify the \( \mathbb{F}_l \)-line in \( K^\times / K^\times l \) which corresponds, via Kummer theory, to the unramified degree-\( l \) extension of \( K \) when \( K^\times \) has an element of prime order \( l \) (prop. 16). Prop. 15 turns out to be a somewhat sharper version of a theorem of Fröhlich (th. 14), which we had
indeed set out to sharpen. In the presence of prop. 30 and 45, prop. 16 becomes the local version of theorems of Hecke (th. 53 and 54), which are immediate corollaries, and which generalise a part of Hilbert’s results (cf. th. 56 and 58).

The other part of Hilbert’s results deals with the valuation of the discriminant; a generalisation of this part can be deduced from results in Hasse’s *Klassenkörperbericht* (cf. th. 60 and 63). Stickelberger, Hilbert, Hecke and Hasse all four deal with number fields, but the questions are purely local, and deserve a purely local proof, a proof which Hensel could have given and which he did indeed give for Stickelberger’s theorem. (Hensel did more; read on to find out.) This is what we do for the other theorems.

An interesting local consequence of prop. 16 is an explicit formula (prop. 17) for the pairing $G \times D \to \mu_p$, where $D \subset \overline{K^\times/K^\times_p}$ is the $\mathbb{F}_p$-line which corresponds to the unramified degree-$p$ extension $L$ of $K$, and $G = \text{Gal}(L|K)$.

An interesting global consequence of these theorems, apart from the decomposition law in prime-degree kummerian extensions of number fields, is a theoretical procedure for computing the relative discriminant of any extension of number fields. This also provides a test for an order in a number field to be the maximal order. Everything boils down to the computation of the relative discriminant of a local kummerian extension of degree equal to the residual characteristic, which is achieved in terms of the ramification filtration and its relation to the natural filtration on the multiplicative group; see the final remark in Part VII.

Our proofs require no more than a study of the filtration on the $\mathbb{Z}_p$-module $U_1$ of principal units or Einseinheiten of $K$, especially of the endomorphism $(\cdot)^p$ of raising to the exponent $p$, which goes back to Hensel. Thus they have the appearance of a piece of late-nineteenth- or early-twentieth-century arithmetic which fell into the twenty-first.

The paper consists of nine Parts, two of them of an historical nature. Part I is a brief chronology of the work of Pellet, Brill, Stickelberger, Voronoï, Hensel, Schur, Herbrand and Fröhlich on discriminants, interspersed with a series of questions which lead to later developments.

Part II contains the statements of our results about discriminants of unramified extensions, about unramified kummerian extensions of prime degree, about the explicit $p$-tic (quadratic, cubic, quintic, ...) character, about the filtration on $K^\times/K^\times_p$, about rings of integers, about discriminants of elliptic curves and about the orthogonality relation.
Part VI is a brief review of the work of Fröhlich, Hasse, Hecke and Hilbert on primary numbers. After the proof of prop. 16, it was natural to try to extend Fröhlich’s results about rings of integers from quadratic extensions to prime-degree kummerian extensions. It was in seeking to do so that we became aware of Hecke’s global results, and, somewhat later, of those of Hilbert. Hecke’s Sätze 118 (th. 53) and 119 (th. 54), which constitute a generalisation of Hilbert’s Satz 96 (th. 58) and a part of Satz 148 (th. 56), follow from our local prop. 16. Hensel makes a reentry on the scene at the end of this Part, closely followed by Eisenstein.

The mathematical Parts can be read independently of the historical ones; a more detailed listing of the contents can be found in Part II.

Part III determines the structure of the multiplicative group $K^\times$ of a local field $K$, following chapter 15 of Hasse’s Zahlentheorie, itself based upon Hensel’s results. Our treatment is more intrinsic, and some of our proofs differ from theirs. Using this, general properties of the discriminant, and the compatibility with Artin-Schreier theory, we prove our results about discriminants and $p$-primary numbers in Part IV.

In Part V, we take a closer look at the filtration on $K^\times/K^{\times p}$, which leads to an understanding of the precise relationship of our results with the theorems of Fröhlich and Hecke. We also give a few examples to show that some disparate results in the literature follow from a systematic theory.

Part VII deals with the computation of the discriminant of ramified prime-degree cyclic extensions of local fields and the determination of their rings of integers (cor. 61). We determine the number of such extensions in the kummerian case and, as a consequence, give a direct elementary proof, in the case of quadratic extensions, of Serre’s mass formula (lemma 67).

In Part VIII, we introduce the discriminant of an elliptic curve $E$ over a local field $K$ as an element of $K^\times/o^{\times 12}$; this definition was anticipated by J. Silverman. We show that — in contrast to the Stickelberger-Hensel condition (th. 6) and to our prop. 15 — every element of $o^\times/o^{\times 12}$ occurs as the discriminant of a good-reduction elliptic curve (cor. 71).

Part IX contains a few words about the genesis of these notes, and determines the ramification filtration on $\text{Gal}(M|K)$, where $M = K(\sqrt[p]{K^\times})$ (the maximal abelian extension of exponent dividing $p$) and $K|Q_p$ is a finite extension containing a primitive $p$-th root of 1, in terms of the filtration on $K^\times/K^{\times p}$. The question was natural in the light of prop. 16, which can be interpreted as saying that $\text{Gal}(M|K)^n = \hat{\bigwedge}_{p^e_1-n+1}$ for $n = 1$, where the orthogonal is with respect to the Kummer pairing, and where
$\bar{U}_{p^n} \subset K^\times/K^\times_p$ is the "deepest" $F_p$-line; the statement of orthogonality for $n > 1$ is taken from [13], where the special case $K = F(\sqrt[n]{F^\times})$ for some (finite) extension $F|Q_p$ is treated. Our proof in the general case is simpler and more conceptual.

***

I. A brief history of discriminants

**Stickelberger (1897).** At the first international Congress of mathematicians, held at Zürich, L. Stickelberger proved some new properties of the discriminant ($Grundzahl$) of an algebraic number field $\Omega$ of degree $n$. We quote the two theorems relevant to us.

**Theorem 1** ([50, p. 186]). — Die Diskriminante des Körpers $\Omega$ ist durch die Primzahl $p$ nicht teilbar, wenn $p$ ein Produkt von lauter verschiedenen Primidealen in $\Omega$ ist; zugleich ist sie, wenn $p$ ungerade, quadratischer Rest oder Nichtrest von $p$, je nachdem die Anzahl der in $p$ aufgehenden Primideale von geradem Grade eine gerade oder ungerade ist, oder je nachdem die Anzahl aller Primfaktoren von $p$ dem Grade des Körpers kongruent ist nach dem Modul Zwei oder nicht.

(If a prime $p$ is unramified in $\Omega$, then it does not divide the discriminant $D$ of $\Omega$; if such a $p$ is odd, then $D$ is a quadratic residue (mod $p$) or not according as the number of even-degree places above $p$ is even or odd.)

The *etwas mühsamer* prime 2 is treated in the last result of the paper.

**Theorem 2** ([50, p. 192]). — Die Diskriminante des Zahlkörpers $\Omega$, in dem 2 ein Produkt von $m$ verschiedenen Primidealen $p_1, p_2, \ldots, p_m$ der Grade $f_1, f_2, \ldots, f_m$ ist, ist von der Form $8q + 1$ oder $8q + 5$, je nachdem unter jenen Primfaktoren solche geraden Grades in gerader oder ungerader Zahl vorkommen; in Zeichen ist

$$\frac{D - 1}{4} \equiv \sum (f - 1) = n - m \pmod{2}$$

oder

$$(-1)^{\frac{D-1}{4}} = (-1)^{n-m}.$$  

(If the prime 2 is unramified in $\Omega$, then the discriminant of $\Omega$ is $\equiv 1$ (mod 8) or $\equiv 5$ (mod 8) according as the number of even-degree places above 2 is even or odd.)
Voronoï (1905). G. Voronoï, unaware of Stickelberger’s results, redisCOVERS th. 1 and gives a different proof at the third international Congress at Heidelberg in 1904. He takes an irreducible polynomial \( F(x) \in \mathbb{Z}[x] \) of degree \( n \) whose discriminant is not divisible by a prime \( p \) and factors it as \( F = \varphi_1 \varphi_2 \cdots \varphi_\nu \) into irreducible polynomials in \( \mathbb{F}_p[x] \). Implicitly assuming that \( p \) is odd, his version of th. 1 is the following.

**Theorem 3** ([53, p. 186]). — *Le nombre \( \nu \) des facteurs irréductibles de la fonction \( F(x) \) par rapport au module \( p \) vérifie l’équation*

\[
\left( \frac{D}{p} \right) = (-1)^{n-\nu},
\]

* où \( \left( \frac{D}{p} \right) \) est le symbole de Legendre.*

(The number \( \nu \) of irreducible factors of \( F \) modulo \( p \) satisfies the displayed equation involving the Legendre symbol.)

Th. 1 was subsequently rediscovered by Th. Skolem [49] and R. Swan [51]. Indeed, it had been anticipated by A. Pellet:

**Theorem 4** ([41, p. 1071]). — *Soit \( \Delta \) le produit des carrés des différences des racines d’une congruence \( f(x) \equiv 0 \) (mod. \( p \)) n’ayant pas de racines égales; \( \Delta \) est non-résidu quadratique (mod. \( p \)), si \( f(x) \) admet un nombre impair de facteurs irréductibles de degré pair; \( \Delta \) est, au contraire, résidu quadratique, si \( f(x) \) n’admet pas de facteurs irréductibles de degré pair ou en admet un nombre pair.*

(The discriminant \( \Delta \) of a separable polynomial \( f \in \mathbb{F}_p[x] \) is in \( \mathbb{F}_p^{\times 2} \) if and only if the number of even-degree irreducible factors of \( f \) is even.)

***

With these beginnings, we shall ask a series of questions which lead naturally to many twentieth-century results about discriminants and related topics. The idea is thus to see the new results in an old light.

Our first questions is : *Aren’t these theorems global manifestations of purely local results?*

**Hensel (1905).** This was first realised by K. Hensel, who proved the local result at the finite places.

**Theorem 5** ([24, p. 78]). — *Ist \( f(x) \) für den Bereich von \( p \) irreduktibel, und ist \( p \) kein Diskriminantenanteiler des zugehörigen Körpers \( K(x) \), so ist die*
Diskriminante einer jeden Gleichung dieses Körpers quadratischer Rest oder Nichtrest zu \( p \), je nachdem \( n \) ungerade oder gerade ist; es ist also stets:

\[
\left( \frac{D}{p} \right) = (-1)^{n-1}.
\]

(If \( f \in \mathbb{Q}_p[x] \) is irreducible, and if the odd prime \( p \) does not divide the discriminant \( D \) of \( \mathbb{Q}_p[x]/f \), then \( D \) is a quadratic residue \((\text{mod} \ p)\) or not according as \( n \) is odd or even.)

He says that this formula remains valid for \( p = 2 \) if we define the Legendre symbol in this case as

\[
\left( \frac{D}{2} \right) = i^{\frac{D-1}{2}} = (-1)^{\frac{D-3}{4}}.
\]

**Theorem 6** ([24, p. 79]). — Ist \( f(x) \) für den Bereich der Primzahl \( 2 \) irreduktibel und ist \( 2 \) nicht in der Körperdiskriminante enthalten, so ist jede Diskriminante dieses Körpers von der Form \( 8\nu + 1 \) oder \( 8\nu + 5 \), je nachdem der Grad jenes Körpers ungerade oder gerade ist. Est gibt keine Diskriminante von der Form \( 8\nu + 3 \) oder \( 8\nu + 7 \).

(If \( f \in \mathbb{Q}_2[x] \) is irreducible, and if 2 does not divide the discriminant \( D \) of \( \mathbb{Q}_2[x]/f \), then \( D \) is \( \equiv 1 \) or \( \equiv 5 \) \((\text{mod} \ 8)\) according as \( n \) is odd or even. No discriminant is \( \equiv 3 \) or \( \equiv 7 \) \((\text{mod} \ 8)\).)

Pellet, Hensel-Mirimanoff, Laskar, Swan, and Barrucand-Laubie have used these theorems to give a new proof of the law of quadratic reciprocity; they continue to inspire current research: see, for example, [36].

To these results about the reduction of the discriminant (modulo an odd prime \( p \), or modulo 8) must be added information about its sign, which goes back to A. Brill. He is working with polynomials with real coefficients and finds that (cf. prop. 9):

**Theorem 7** ([5, p. 87]). — Das Vorzeichen der Discriminante einer Gleichung — lauter verschiedene Wurzeln vorausgesetzt — ist negativ, wenn die Anzahl der complexen Wurzelpaaren eine Ungerade ist, positiv, wenn diese Zahl gerade ist.

(The sign of the discriminant of a separable real polynomial is negative if the number of pairs of complex conjugate roots is odd, positive if this number is even.)

Unaware of Brill’s local th. 7, Hensel considers the number field \( \mathbb{K}(x) \) obtained by adjoining a root \( x \) of an irreducible polynomial \( f \in \mathbb{Q}[x] \) of
degree $n$, with factorisation $f = f_1 f_2 \cdots f_h$ into irreducible polynomials in $\mathbb{R}[x]$ (necessarily linear or quadratic by a theorem of C. Gauss, as he reminds us: *Gauß hat zuerst streng bewiesen,...*).

**Theorem 8** ([24, p. 70]). — *Die Basisdiskriminanten eines Körpers $K(x)$ sind sämtlich positiv oder sämtlich negativ, je nachdem $n - h$ gerade oder ungerade ist, d. h. es ist*

$$\text{sgn } D = (-1)^{n-h}.$$  

(The sign of the discriminant $D$ of $K(x)$ is given by the above equation.)

By multiplicativity, Brill’s th. 7 comes down to the following prop., which also implies Hensel’s global th. 8:

**Proposition 9.** — *The discriminant of a finite extension $K | \mathbb{R}$ is $(-1)^{n-1}$ in $\mathbb{R}^x/\mathbb{R}^{x^2}$, where $n = [K : \mathbb{R}]$.*

**Proof:** Only the case $K = \mathbb{C}$ needs to be considered. Computing the discriminant $d_{\mathbb{C}|\mathbb{R}}$ using the standard basis $1, i$, we get $d_{\mathbb{C}|\mathbb{R}} = -4$, which is the same as $-1$ in $\mathbb{R}^x/\mathbb{R}^{x^2}$. We could have equally well computed the discriminant (“$b^2 - 4ac$”) of $T^2 + 1$.

Our next question is: *What is the valuation of the discriminant when the extension $K | \mathbb{Q}_p$ is ramified?*

This leads to a host of results due to R. Dedekind, D. Hilbert, E. Artin, J. Herbrand, etc., some of which are taken up in Part VII. Let us content ourselves here with a modest corollary of a result (1) of Dedekind.

**Theorem 10** ([12, p. 54]). — *Ist aber $p = 2$, also der Exponent $e$ theilbar durch $p$, so ist $d$ mindestens durch $p^2$, und folglich $D$ mindestens durch 4 theilbar.*

(If $p = 2$ and the ramification index $e$ is even, then $p^2$ divides the different $d$ and consequently 4 divides the discriminant $D$.)

---

(1) *Ist $p$ ein beliebiges Primideal, $p$ der durch $p$ theilbare rationale Primzahl, und $p^e$ die höchste in $p$ aufgehende Potenz von $p$, so ist das Grundideal $d$ allemal theilbar durch $p^{e-1}$; ist ferner der Exponent $e$ nicht theilbar durch $p$, so ist $d$ nicht theilbar durch $p^e$; ist aber $e$ theilbar durch $p$, so ist $d$ theilbar durch $p^e$ und vielleicht durch noch höheren Potenzen von $p$. [12, p. 52] (If $p$ is a prime ideal, $p$ the rational prime divisible by $p$ and $p^e$ the highest power of $p$ dividing $p$, then the different $d$ is divisible by $p^{e-1}$; if $p$ does not divide $e$, then $p^e$ does not divide $d$; if $p$ divides $e$, then $p^e$ and possibly a higher power of $p$ divides $d$).*
Schur (1929). A simple proof of the conjunction of this fact and of a somewhat less precise form of th. 2 was given by I. Schur; regrettably, this is the version most commonly cited these days.

Theorem 11 ([44, p. 29]). — Die Diskriminante $D$ eines algebraischen Zahlkörpers is stets kongruent 0 oder 1 nach dem Modul 4.

(The discriminant $D$ of a number field is always $\equiv 0$ or $\equiv 1 \pmod{4}$.)

Our next question is: What are the relative versions of these results?

Herbrand (1932). Indeed, J. Herbrand asked himself this question before his tragic death in a mountaineering accident at the young age of 23. In a paper which he could write only partially, and which was completed by C. Chevalley based upon his rough notes (brouillons), he proves the following theorem.

Theorem 12 ([30, p. 105]). — $\vartheta$ étant le discriminant par rapport au corps $k$ d’un sous-corps relativement metacyclique $K$ de degré relatif $N$, on a $\vartheta = a^2(\alpha)$, où $\alpha$ est un nombre tel que :

\begin{enumerate}
\item $\alpha \equiv 1 \pmod{b}$, $b$ étant le plus grand idéal divisant 4 et premier à $\vartheta$.
\item Le conjugué de $\alpha$ dans un corps réel conjugué de $k$ n’est négatif que si le conjugué correspondant de $K$ est imaginaire et si $N \equiv 2 \pmod{4}$.
\end{enumerate}

($\vartheta$ being the discriminant of a metacyclic extension $K|k$ of degree $N$, one has $\vartheta = a^2(\alpha)$, where $\alpha$ is a number such that $\alpha \equiv 1 \pmod{b}$, $b$ being the greatest ideal dividing 4 and prime to $\vartheta$. Moreover, the conjugate of $\alpha$ in a real field is not negative unless the corresponding conjugate of $K$ is imaginary and $N \equiv 2 \pmod{4}$.)

As a corollary, he gets a theorem of Hecke:

Le discriminant d’un corps algébrique, par rapport à un sous-corps, est le dans carré d’une classe de ce sous-corps (The discriminant of a number field, with respect to a subfield, is the square of a class in that subfield),

and, taking $k = \mathbb{Q}$, the theorem of Stickelberger-Schur:

Le discriminant d’un corps algébrique est congru à 0 ou à 1 (mod. 4) (The discriminant of a number field is always $\equiv 0$ or $\equiv 1 \pmod{4}$),

in the case of metacyclic extensions (resp. number fields). He says that as these two theorems are true without restriction to the metacyclic — or even to the galoisian — case, it is probable that his theorem is also true without the hypothesis that the extension $K|k$ be metacyclic.
Fröhlich (1960). This conjecture was proved some thirty years later by A. Fröhlich when he introduced the idelic discriminant. For an extension \( \Lambda|K \) of number fields, the discriminant \( \mathfrak{d}_{\Lambda|K} \) is an element of the restricted direct product of the various \( K_p^\times/\mathfrak{o}_p^\times \), where \( p \) runs through the places of \( K \). The classical discriminant of \( \Lambda|K \) becomes the (integral) ideal \( (\mathfrak{d}_{\Lambda|K}) \) associated to the idelic discriminant.

**Theorem 13** ([17, p. 28]). — The ideal \( (\mathfrak{d}_{\Lambda|K}) \) (\( \Lambda|K \) normal) can be written in the form \( a^2(\alpha), \alpha \in K^\times \) where

(i) \( \alpha \equiv 1 \pmod{b} \), \( b \) the greatest divisor of 4 prime to \( (\mathfrak{d}_{\Lambda|K}) \).

(ii) \( \alpha_p > 0 \) for each real prime divisor \( p \), except when \( \Lambda_p \) is a direct sum of copies of the field of complex numbers and \( (\Lambda : K) \equiv 2 \pmod{4} \).

He remarks that (i) is also true when \( \Lambda|K \) is not normal, while in the place of the congruence in (ii) we have \( r_2 \equiv 1 \pmod{2} \). His relative version of the Stickelberger-Schur theorem (th. 11) is the following.

**Theorem 14** ([17, p. 23]). — *Every discriminant is a quadratic residue mod 4.*

The proof is by reduction to the local case, where Schur’s proof applies almost without change. (This result was anticipated by K. Dalen [11, p. 125] and rediscovered by R. Swan [51, p. 1100].)

But in the formulation “*Every discriminant is a quadratic residue mod 4*”, the local version is contentless for odd residual characteristics, because \( \mathfrak{o}/4\mathfrak{o} = 0 \) : one does not recover Hensel’s th. 6. When the residual characteristic is 2, it leaves open the question as to which squares in \( \mathfrak{o}/4\mathfrak{o} \) are discriminants, and which units the discriminants of even-degree unramified extensions; in the absolute case \( K = \mathbb{Q}_2 \), th. 6 gives precise answers to these questions. Moreover, it is not very aesthetic to lift elements (of positive valuation) of the multiplicative group \( K^\times/\mathfrak{o}^\times \) to the additive group \( \mathfrak{o} \) with the purpose of going modulo \( 4\mathfrak{o} \).

In the next section, we give our formulation of the relative version and show how it can be interpreted as a characterisation of “2-primary” numbers, leading to the question of a characterisation of “\( p \)-primary” numbers — to use a piece of terminology we learnt much later — for every prime \( p \), answered in prop. 16.

**II. The main propositions**

**The relative version.** The correct relative version in the local case is not far to seek. The discriminant \( d_{L|K} \) is an element of \( K^\times/\mathfrak{o}^\times \), a group
which comes equipped with a filtration

(1) \[ \cdots \subset \bar{U}_n \subset \cdots \subset \bar{U}_1 \subset o^\times/o^{\times 2} \subset K^\times/o^{\times 2} \]

by vector \( F_2 \)-spaces, deduced from the filtration

(2) \[ \cdots \subset U_n \subset \cdots \subset U_1 \subset o^\times \subset K^\times, \]

where \( U_n = \text{Ker}(o^\times \to (o/p^n)^\times) \) \((n > 0)\). The filtration (1) is finite; indeed \( \bar{U}_{2e+1} = \{1\} \), and \( \bar{U}_{2e} = \{1, u\} \) is an \( F_2 \)-line, where \( e \) is the (absolute) ramification index of \( K \) if \( p = 2 \), and \( e = 0 \) if \( p \neq 2 \) (cf. prop. 33).

We have adopted the convention that \( U_0 = o^\times \).

**Proposition 15.** — Let \( K \) be a finite extension of \( \mathbb{Q}_p \) (\( p \) prime) and let \( L \) be a finite unramified extension of \( K \), of degree \( r = [L : K] \). Then the discriminant \( d_{L|K} \) belongs to the \( F_2 \)-line \( \bar{U}_{2e} = \{1, u\} \); one has \( d_{L|K} = 1 \) if \( r \) is odd, \( d_{L|K} = u \) if \( r \) is even. When \( p = 2 \), none of the other \( 2^{d+1} - 2 \) \((d = [K : \mathbb{Q}_p])\) elements of \( o^\times/o^{\times 2} \) is a discriminant.

The proof is given in Part III. Hensel could have easily proved prop. 15, because all we need for the proof are Hensel’s results on the structure of the multiplicative group of \( K \), and general properties of the discriminant in a tower of extensions, which go back to Hilbert. We wish to argue that if he had done it, and if this version had become established instead of the Schur-Fröhlich version (th. 11, th. 14), the history of mathematics would have been different in a few respects.

The first thing to notice is that, when \( p \neq 2 \), the discriminant of the residual extension of \( L|K \) is the reduction of the discriminant via the isomorphism \( \bar{U}_{2e} \ra k^\times/k^{\times 2} \). What about the case \( p = 2 \)? In this case, there is an isomorphism \( \bar{U}_{2e} \ra k/\varphi(k) \), where \( \varphi \) is the \( F_2 \)-linear endomorphism \( x \mapsto x^2 - x \) of \( k \).

Our next question therefore is: *Is there a way of defining discriminants — with values in \( k/\varphi(k) \) — when \( k \) is an extension of \( \mathbb{F}_2 \)?*

**Discriminants in characteristic 2.** There is indeed one: it was found by E. Berlekamp [3] in 1976, who seems to have been motivated by coding theory. He does notice (p. 326) the analogy between his definition and Stickelberger’s th. 1, but fails to mention the even stronger analogy with th. 2, or its substantial identity with Hensel’s th. 6, which can be construed as implying that the discriminant of a finite extension of \( \mathbb{F}_2 \) is 0 (trivial) if the degree is odd, 1 (not trivial) if the degree is even. When the base field \( \mathbb{F}_2 \) is replaced by any finite extension \( k \) thereof, prop. 15 implies the
The analogous result: the discriminant of an odd-degree (resp. even-degree) extension of \( k \) is 0 (resp. 1) in the additive 2-element group \( k/\varphi(k) = F_2 \).

The interpretation of the characteristic-2 discriminant as the reduction of a characteristic-0 discriminant was found by A. Wardsworth [55] in 1985, eighty years after Hensel’s absolute local versions (th. 5, th. 6).

**Unramified kummerian extensions.** There is another reading of prop. 15. It can be viewed as specifying the \( F_2 \)-line in \( K^x/K^{x^2} \) which gives us the unramified quadratic extension of \( K \) upon adjoining square roots.

If the local field \( K \) contains a primitive \( l \)-th root of 1 for some prime \( l \), then degree-\( l \) cyclic extensions of \( K \) correspond to \( F_l \)-lines in \( K^x/K^{x^l} \) (“Kummer theory”).

Our next question is: *Which line in the \( F_l \)-space \( K^x/K^{x^l} \) gives us the unramified \( (\mathbb{Z}/l\mathbb{Z}) \)-extension of \( K \)?*

If \( l = p \), let \( e_1 \) stand for the ramification index of \( K|Q_p \) divided by \( p - 1 \) (the quotient \( e_1 \) is an integer; cf. prop. 25); if \( l \neq p \), put \( e_1 = 0 \).

It can be shown that the induced filtration on \( K^x/K^{x^l} \) by \( F_l \)-spaces

\[
\cdots \subset \bar{U}_n \subset \cdots \subset \bar{U}_1 \subset o^x/o^{x^l} \subset K^x/K^{x^l}
\]

has \( \bar{U}_{pe_1+1} = \{1\} \), and that \( \dim_{F_l} \bar{U}_{pe_1} = 1 \) (see Part III).

**Proposition 16.** — *The \( F_l \)-line in \( K^x/K^{x^l} \) which gives the unramified \( (\mathbb{Z}/l\mathbb{Z}) \)-extension of \( K \) upon adjoining \( l \)-th roots is \( \bar{U}_{pe_1} \).*

The proof is to be found in Part III. Notice that \( \bar{U}_{pe_1} = \bar{U}_{le_1} \) even when \( l \neq p \), for then \( e_1 = 0 \).

**Degree-\( p \) cyclic extensions in characteristic \( p \).** When \( l = p \), the choice of an element \( \zeta \in K^x \) of order \( p \) gives us an isomorphism \( \bar{U}_{pe_1} \rightarrow k/\varphi(k) \), where \( \varphi: k \rightarrow k \) is the \( F_p \)-linear map \( x \mapsto x^p - x \) (cf. the discussion after prop. 33). This leads us to the next question.

We ask: Do \( (\mathbb{Z}/p\mathbb{Z}) \)-extensions of a characteristic-\( p \) field \( k \) correspond to \( F_p \)-lines in \( k/\varphi(k) \)?

They indeed do, as was discovered by E. Artin and O. Schreier [2], who were led to their result by an entirely different route (maximally ordered fields). Neither they, nor E. Witt [58], make any connection\(^{(2)}\)

\(^{(2)}\) According to Prof. Peter Roquette [43], Artin made this connection
with Hensel’s determination of the filtration on $K^\times/K^{\times p}$, which preceded their results by more than twenty years. The connection between the two theories was fully understood only in the eighties, in the works of T. Sekiguchi, F. Oort & N. Suwa [45] and W. Waterhouse [56]. It is no accident that last-named author published a paper [57] on the cohomological interpretation of the discriminant in the same year; as we have seen, the two topics are not unrelated. As it happens, we shall make a modest use of Artin-Schreier theory in our proofs.

The Kummer pairing. Recall that Kummer theory provides not only a bijection between the set of $F_p$-lines $D \subset K^\times/K^{\times p}$ and the set of degree-$p$ cyclic extensions $L$ of $K$, but also a pairing $\text{Gal}(L|K) \times D \to \mu_p$ when $D$ and $L$ correspond to each other:

$$L = K(\sqrt[p]{D}), \quad D = \ker(K^{\times}/K^{\times p} \to L^{\times}/L^{\times p}).$$

Our next question is: Can we give an explicit description of the pairing $\langle , \rangle : G \times \hat{U}_{pe1} \to \mu_p$, where $G = \text{Gal}(L|K)$ and $L$ is the degree-$p$ unramified extension of $K$?

The group $G$ has a canonical generator $\phi$ (“Frobenius”) : the unique element $\phi$ such that $\phi(\alpha) \equiv \alpha^q \pmod{p}$ for every $\alpha \in \mathfrak{o}_L$, where $q = \text{Card } k$ and $k$ is the residue field of $K$. We shall see in Part III that the choice of a generator $\zeta \in \mu_p$ leads to a specific isomorphism $\eta \mapsto \hat{c} : \hat{U}_{pe1} \to k/\wp(k)$, where $c = (\eta - 1)/p(\zeta - 1)$, which belongs to $\mathfrak{o}$, and $\hat{c}$ is its image in $k/\wp(k)$. This can be composed with the trace map $S_{k|F_p} : k/\wp(k) \to F_p$, which is also an isomorphism.

**Proposition 17.** Choose and fix a generator $\zeta \in \mu_p$. For $a \in \mathbb{Z}/p\mathbb{Z}$ and $\eta \in U_{pe1}$, we have $\langle \varphi^a, \eta \rangle = \zeta^{a \cdot S_{k|F_p}(\hat{c})}$.

in a letter to Hasse in 1927, with the words *Ich entdeckte, daß hier ein alter Bekannter von mir vorlag…*; see [16]. This connection also appears independently and implicitly in Hasse [21, p. 234] as

$$\left(\frac{\alpha}{T}\right)_l = \zeta_0^{S_{l\left(\frac{a-1}{\lambda_0}\right)}},$$

which is essentially the case $a = 1$ of our (purely local) prop. 17. See also his *Klassenkörperbericht*, Teil II, §17, 3, IV, to which we don’t have access. Hasse derives (13) from Artin’s general reciprocity law; not even its local version is needed for the proof of prop. 17.
The proof is to be found in Part IV (prop. 38), where the implication [46, p. 230] for the pairing \( K^\times \times \bar{U}_{p \xi} \rightarrow p \mu \) coming from the reciprocity map \( K^\times \rightarrow G \) is also mentioned.

Another interesting consequence of the characterisation of the unramified degree-\( p \) kummerian extension (prop. 16) is a generalisation of the Pellet-Voronoi theorem (th. 3 and 4) to arbitrary finite fields \( k \): the discriminant of a separable polynomial \( f \in k[T] \) is trivial precisely when the number of even-degree irreducible factors of \( f \) is even (cor. 41).

**The filtration on** \( K^\times/K^{\times p} \). In Part V, we will give three different characterisations of the filtration \( (\bar{U}_n)_{n>0} \) on \( K^\times/K^{\times p} \) for a finite extension \( K \) of \( Q_p \) and compute the \( F_p \)-dimension of the quotients \( \bar{U}_n/\bar{U}_{n+1} \). The main results are the following two propositions.

**Proposition 18.** Let \( \zeta \in \bar{K}^\times \) be an element of order \( p \). Then

\[
\dim_{F_p} \bar{U}_n/\bar{U}_{n+1} = \begin{cases} 
0 & \text{if } n > pe_1, \\
1 & \text{if } n = pe_1 \text{ and } \zeta \in K^\times, \\
0 & \text{if } n = pe_1 \text{ and } \zeta \notin K^\times, \\
0 & \text{if } n < pe_1 \text{ and } p | n, \\
f & \text{otherwise.}
\end{cases}
\]

**Proposition 19.** For \( x \in \mathfrak{o}^\times \) and \( n > 0 \), let \( \bar{x} \) be its image in \( \mathfrak{o}^\times/\mathfrak{o}^{\times p} \) and \( \hat{x} \) the image in \( (\mathfrak{o}/p^n)^\times \). Then

\[
\bar{x} \in \bar{U}_n \iff \hat{x} \in (\mathfrak{o}/p^n)^\times.
\]

It is this result which allows us to deduce the theorems of Hecke and Hilbert from our local results. In this Part, we also work out a number of explicit examples.

**Rings of integers in kummerian extensions.** In Part VII, we determine, following Hasse, the valuation \( v_K(d_{L|K}) \) of the discriminant \( d_{L|K} \) of cyclic degree-\( p \) extensions \( L|K \) of local fields (prop. 60). The proof allows us to determine the ring of integers \( \mathfrak{o}_L \) explicitly (prop. 61). One can also compute the number of such \( L \) with a given \( v_K(d_{L|K}) \) (prop. 66).

We also explain how this solves the global problem of determining the relative discriminant of an extension of number fields.
Discriminants of elliptic curves over local fields. In view of the definition of the discriminant  $d_{L|K}$ of a finite extension $L|K$ of local fields as an element of $K^\times /\mathfrak{o}^\times$, it is natural to define the discriminant of an elliptic curve $E|K$ as an element $d_{E|K} \in K^\times /\mathfrak{o}^{12}$ (see Part VIII).

We may ask: Suppose that $E|K$ has good reduction. Does $d_{E|K} \in \mathfrak{o}^\times /\mathfrak{o}^{12}$ have to satisfy some congruence?

In contrast to th. 6 and prop. 15, every element of $\mathfrak{o}^\times /\mathfrak{o}^{12}$ occurs as $d_{E|K}$ for some good-reduction elliptic curve $E|K$ (prop. 71). As corollary, every element of $k^\times /k^{12}$ occurs as the discriminant of some elliptic $k$-curve over any finite field $k$ (cor. 72).

The orthogonality relation. In Part IX, we derive the orthogonality relation $\text{Gal}(M|K)^n = U_{p_1-1-n+1}^\perp$ which can be thought of as a generalization of prop. 16. It determines the ramification filtration on the maximal exponent-$p$ kummerian extension $M = K(\sqrt[p]{K^\times})$ of a finite extension $K|\mathbb{Q}_p$ (containing a primitive $p$-th root $\zeta$ of 1). Upon taking $K = F(\zeta)$, it can be used to derive the ramification filtration on the maximal exponent-$p$ abelian extension of any finite extension $F$ of $\mathbb{Q}_p$.

III. The multiplicative group of a local field

In chapter 15 of his Zahlentheorie [22], H. Hasse studies the multiplicative group $K^\times$ of a finite extension $K$ of $\mathbb{Q}_p$ ($p$ prime), whose determination goes back to Hensel [25]. In this Part, we give a brief account of the results, not all of which are needed for what follows. Some of our proofs (for example in §1 and §4) are different from those of Hensel and Hasse. A part of §3 can be also be found in [15, I,§5].

We first study the analogous local field $k((T))$, where $k$ is a finite extension of $\mathbb{F}_p$. In both cases, the multiplicative group comes equipped with a decreasing sequence of subgroups $(U_n)_n$ which are $\mathbb{Z}_p$-modules for $n > 0$. The result for $k((T))$ states that the $\mathbb{Z}_p$-module $U_1$ of Einseinheiten is not finitely generated, so the filtration on $U_1/U_1^p$ is not of finite length.

By contrast, the group of 1-units $U_1$ in $K$ is finitely generated as a $\mathbb{Z}_p$-module (cor. 32) and the filtration on $K^\times/K^{\times p}$ is of finite length. There is a criterion for $K^\times$ to contain an element of order $p$ (prop. 25). For an element $\zeta$ of order $p^\alpha$, the precise level — the integer $n$ such that $\zeta \in U_n$ but $\zeta \notin U_{n+1}$ — is known (prop. 26). We study the raising-to-the-exponent-$p$ map $(\cdot)^p$ and show that $U_n^p \subset U_{\lambda(n)}$, where $\lambda(n) = \inf(pn, n + e)$, and $e = (v(K^\times) : v(Q_p^\times))$ is the ramification index (prop. 27). Next, we show that the induced map $\rho_n : U_n/U_{n+1} \to U_{\lambda(n)}/U_{\lambda(n)+1}$ is always an
isomorphism except when $K^\times$ has an element of order $p$ and $n = e/(p - 1)$, in which case both Ker $\rho_n$ and Coker $\rho_n$ are cyclic of order $p$; we determine these groups explicitly (prop. 33). Finally, we determine the structure of the $p$-groups $U_1/U_n$ for sufficiently large $n$ (prop. 34).

1. The multiplicative group $k((T))^\times$

Let $k$ be a finite extension of $\mathbb{F}_p$ and let $K = k((T))$. For every $n > 0$, let $U_n$ be the kernel of the reduction map from $k[[T]]^\times$ to $(k[[T]]/T^n k[[T]])^\times$; in particular, $U_1 = \text{Ker}(k[[T]]^\times \to k^\times)$. The $U_n$ are $\mathbb{Z}_p$-modules, because they are commutative pro-$p$-groups.

**Proposition 20. —** The $\mathbb{Z}_p$-module $U_1 = \text{Ker}(k[[T]]^\times \to k^\times)$ is not finitely generated.

It is sufficient to show that ($U_1 : U_n^p$) is not finite. Supposing that it is, we shall get a contradiction.

We have $U_n^p \subset U_{pn}$ for every $n$, because $(1 + aT^n)^p = 1 + a^pT^{pn}$ for every $a \in k[[T]]$. The inclusions $U_n^p \subset U_{pn} \subset U_n$ imply that

$$(U_n : U_n^p) \geq (U_n : U_{pn}) = q^{pn-n} \quad (q = \text{Card } k),$$

because $(U_i : U_{i+1}) = q$, as $(1 + aT^i) \mapsto a$ induces an isomorphism $U_i/U_{i+1} \to k$ for every $i > 0$.

We also have the inclusions $U_n^p \subset U_n \subset U_1$ and $U_n^p \subset U_n^p \subset U_1$ which allow us to compute the index $(U_1 : U_n^p)$ in two different ways. Comparing them, and using the fact that $(U_1 : U_n) = (U_1^p : U_n^p)$ (for which the absence of torsion — the only $p$-th root of 1 in a field of characteristic $p$ is 1 — is needed), we get the equality $(U_1 : U_1^p) = (U_n : U_n^p)$, which is larger than $q^{pn-n}$. But we can take $n$ as large as we please, so $(U_1 : U_1^p)$ cannot be finite!

**Corollary 21. —** The $\mathbb{F}_p$-space $K^\times/K^{\times p}$ is infinite.

***

We fix the notation for the rest of Part III : $K$ is a finite extension of $\mathbb{Q}_p$, $v : K^\times \to \mathbb{Z}$ is its surjective valuation, $\mathfrak{o} = v^{-1}([0, +\infty])$ is its ring of integers, with unique maximal ideal $\mathfrak{p} = v^{-1}([0, +\infty])$ and residue field $k = \mathfrak{o}/\mathfrak{p}$. The units $\mathfrak{o}^\times$ will also be denoted $U_0$; for $n > 0$, we put $U_n = 1 + \mathfrak{p}^n$. Denote by $d = [K : \mathbb{Q}_p]$ the degree of $K$, by $e = (v(K^\times) : v(\mathbb{Q}_p^\times))$ the ramification index, and by $f = [k : \mathbb{F}_p]$ the residual degree; we have $d = ef$ and $q = p^f$, where $q = \text{Card } k$. 

15
We put \( e_1 = e/(p - 1) \). For \( n > 0 \), define \( \lambda(n) = \inf(pn, n + e) \), so that \( \lambda(n) = pn \) if \( n \leq e_1 \) and \( \lambda(n) = n + e \) if \( n \geq e_1 \).

We identify \( k^\times \) with a subgroup of \( \sigma^\times \) by the section \( x \mapsto \lim_{n \to +\infty} y q^n \) (“Teichmüller”), where \( y \in \sigma^\times \) is any preimage of \( x \in k^\times \); it is the subgroup of solutions of \( z^{q-1} = 1 \). We have \( \sigma^\times = k^\times U_1 \) and \( k^\times \cap U_1 = \{1\} \).

Fix an algebraic closure \( \bar{K} \) of \( K \).

2. Roots of 1

In this section, we study cyclotomic extensions of \( K \), give a criterion for \( K^\times \) to contain an element of order \( p \), and determine the level of an element of order \( p^\alpha \).

**Proposition 22.** — Let \( \zeta \in \bar{K}^\times \) be an element of order \( n \) prime to \( p \). Then the extension \( K(\zeta) \mid K \) is unramified of degree \( g \), where \( g \) is the order of \( q \) in \( (\mathbb{Z}/n\mathbb{Z})^\times \).

Recall that, for each \( m > 0 \), \( K \) has a unique unramified extension \( K_m \) in \( \bar{K} \) of degree \( m \), that \( K_m^\times \) contains an element of order \( (q^m - 1) \), and that “\( m' \mid m \)” is equivalent to \( K_{m'} \subset K_m \). If \( K_m \) has an element of order \( l \) prime to \( p \), then \( l \mid q^m - 1 \) (and conversely).

As \( n \mid q^g - 1 \), we have \( K(\zeta) \subset K_g \). Therefore \( K(\zeta) \) is unramified over \( K \), and hence \( K(\zeta) = K_{g'} \) for some \( g' \mid g \). As \( K_{g'}^\times \) contains an element — \( \zeta \), for example — of order \( n \) prime to \( p \), we have \( n \mid q^{g'} - 1 \), which means that \( q^{g'} \equiv 1 \mod{n} \) and \( g \mid g' \), because \( g \) is the order of \( q \) in \( (\mathbb{Z}/n\mathbb{Z})^\times \). Thus \( g' = g \).

From now on, let \( K_0 \) be the maximal unramified subextension of \( K \).

**Proposition 23.** — Let \( \zeta \in \bar{K}^\times \) be an element of order \( p^n \) \((n > 0)\). Then the extension \( K_0(\zeta) \mid K_0 \) is totally ramified of degree \( \varphi(p^n) = p^{n-1}(p - 1) \), and \( 1 - \zeta \) is a uniformiser of \( K_0(\zeta) \).

The proof proceeds by induction on \( n \). Put \( \xi_n = \zeta, \xi_{n-1} = \xi_n^p, \ldots, \xi_1 = \xi_2^p \). Also put \( K_i = K_0(\xi_i) \) and \( \pi_i = 1 - \xi_i \).

Let us show that \( \pi_1 \) is a uniformiser of \( K_1 \), which is totally ramified of degree \( p - 1 \) over \( K_0 \). As \( \xi_1 \in K_1^\times \) is an element of order \( p \), we have

\[
\frac{1 - \xi_1^p}{1 - \xi_1} = 1 + \xi_1 + \xi_1^2 + \cdots + \xi_1^{p-1} = 0,
\]

which, in terms of \( \pi_1 = 1 - \xi_1 \), means that

\[
\frac{1 - (1 - \pi_1)^p}{\pi_1} = p - \left(\frac{p}{2}\right) \pi_1 + \cdots + (-1)^{p-1} \pi_1^{p-1} = 0.
\]
Thus $\pi_1$ is a root of a degree-$(p - 1)$ Eisenstein polynomial over $K_0$, and hence $K_1 \mid K_0$ is totally ramified of degree $p - 1$, and $\pi_1$ is a uniformiser of $K_1$.

Assume now that $K_{n-1} \mid K_0$ is totally ramified of degree $\varphi(p^{n-1})$ with $\pi_{n-1} = 1 - \xi_{n-1}$ as a uniformiser. From $\xi_n^p - \xi_{n-1} = 0$ it follows that

$$(1 - \pi_n)^p - (1 - \pi_{n-1}) = \pi_{n-1} - \left(\begin{pmatrix} p \\ 1 \end{pmatrix}\pi_n + \left(\begin{pmatrix} p \\ 2 \end{pmatrix}\pi_n^2 - + \cdots + (-1)^{p}\pi_{n}^p = 0,$$

which means that $\pi_n$ is a root of a degree-$p$ Eisenstein polynomial with coefficients in $K_{n-1}$. Therefore $\pi_n$ is a uniformiser of $K_n$, which is totally ramified of degree $p$ over $K_{n-1}$; in other words, $K_n \mid K_0$ is totally ramified of degree $\varphi(p^n)$. This completes the proof by induction.

(By contrast, for an arbitrary finite extension $K$ of $\mathbb{Q}_p$, the extension $K(\zeta) \mid K$ may be unramified. Hasse notes that if $p = 2$ and $n = 2$, then $K(\sqrt{-1})$ is an unramified quadratic extension of the ramified extension $K = \mathbb{Q}_2(\sqrt{3})$. Cf. ex. 50.)

**Proposition 24.** — The two extensions $\mathbb{Q}_p(\omega)$ ($\omega^{p-1} + p = 0$) and $\mathbb{Q}_p(\zeta)$ ($\zeta^{p-1} + \zeta^{p-2} + \cdots + 1 = 0$) are isomorphic to each other.

We know that $\pi = 1 - \zeta$ is a uniformiser of $\mathbb{Q}_p(\zeta)$ and that $p$ is the norm of $\pi$:

$$p = (1 - \zeta)(1 - \zeta^2) \cdots (1 - \zeta^{p-1}).$$

Putting

$$u_r = \frac{1 - \zeta^r}{1 - \zeta} = 1 + \zeta + \cdots + \zeta^{r-1} \equiv r \pmod{\pi} \quad (0 < r < p)$$

we have $p = (1 - \zeta)^{p-1} u_1 u_2 \cdots u_{p-1}$. But we all know that $u_1 u_2 \cdots u_{p-1} \equiv 1.2 \cdots (p-1) \equiv -1$ in $\mathbb{F}_p^\times$ (“Wilson’s theorem”). So $-p = u \pi^{p-1}$ with $u \in U_1$ depending on $\zeta$.

But $U_1$ is a $\mathbb{Z}_p$-module, and $p - 1$ is invertible in $\mathbb{Z}_p$, so there is a unique $\eta \in U_1$ such that $\eta^{p-1} = u$. Therefore we have $-p = (\eta \pi)^{p-1}$, and thus $\eta \pi$ is a root of $T^{p-1} + p$ in $\mathbb{Q}_p(\zeta_p)$.

Hence, there is an embedding $\mathbb{Q}_p(\omega) \to \mathbb{Q}_p(\zeta_p)$; it is an isomorphism because the two extensions have the same degree over $\mathbb{Q}_p$.

(Prop. 24 answers a question similar to the one answered by prop. 16. Knowing that $\mathbb{Q}_p^\times$ has an element of order $p - 1$, and that the extension $\mathbb{Q}_p(\zeta)$ is cyclic of degree $p - 1$, which cyclic subgroup of order $p - 1$ in $\mathbb{Q}_p^\times/\mathbb{Q}_p^\times(p-1)$ does it correspond to? Answer: the subgroup generated by the image of $-p$.)
Proposition 25. — For the group $K^\times$ to contain an element of order $p$, it is necessary and sufficient that $p - 1$ divide $e$ and, upon writing $-p = u\pi^e$ ($u \in o^\times$ and $\pi$ uniformiser of $K$), to have $\bar{u} \in k^{\times(p-1)}$.

The first thing to ask is: Is this independent of the choice of the uniformiser? If $\pi'$ is another uniformiser and we write $-p = u'\pi'^e$, does one also have $\bar{u}' \in k^{\times(p-1)}$? Well, we then have

$$u' = u\pi^e\pi'^{-e} = u((\pi/\pi')^{e_1})^{p-1}$$

and therefore $\bar{u}' \in k^{\times(p-1)}$, because $\bar{u} \in k^{\times(p-1)}$.

Let us prove the proposition. Suppose first that $K^\times$ has an element $\zeta$ of order $p$ and consider the tower of extensions $K | Q_p(\zeta) | Q_p$. The absolute ramification index $e$ is divisible by the absolute ramification index $p - 1$ of $Q_p(\zeta)$, so $e_1 = e/(p - 1)$ is an integer. The maximal unramified subextension $K_0$ of $K | Q_p$ is linearly disjoint from $Q_p(\zeta)$ because the latter is totally ramified; the extension $K | K_0(\zeta)$ is totally ramified of degree $e_1$.

There is a root $\omega$ of $T^{p-1} + p$ in $K_0(\zeta)$ (prop. 24). Further, $\omega$ is a uniformiser of $K_0(\zeta)$ and, if $\pi$ is a uniformiser of $K$, then $\omega = \varepsilon\pi^{e_1}$, for some $\varepsilon \in o^\times$. Now observe that $-p = \omega^{p-1} = \varepsilon^{p-1}\pi^e$, and the unit $\varepsilon^{p-1}$ clearly reduces modulo $\pi$ to an element of $k^{\times(p-1)}$.

Conversely, suppose that $p - 1|e$ and that, writing $-p = u\pi^e$, we have $\bar{u} \in k^{\times(p-1)}$. Write $u = \varepsilon u_1$, where $\varepsilon \in k^\times$ and $u_1 \in U_1$. By hypothesis, $\varepsilon = \eta^{p-1}$ for some $\eta \in k^\times$ and, as we have observed earlier, $u_1 = \eta_1^{p-1}$ for a unique $\eta_1 \in U_1$. Then $\eta_1 \pi^{e_1}$ is a root of $T^{p-1} + p$ in $K$ so, by prop. 24, $K$ contains $Q_p(\zeta)$.

*La proposition 25 est grossièrement fausse.*

— Anonyme [1, p. 1].

Proposition 26. — Suppose that $K^\times$ has an element $\zeta$ of order $p^n$ ($n > 0$). Then $\zeta \in U_a$ but $\zeta \notin U_{a+1}$, where $a = e/\varphi(p^n)$ and $\varphi(p^n) = p^{n-1}(p - 1)$.

Note that $a$ is an integer by prop. 23. By the same prop., $1 - \zeta$ is a uniformiser of $K_0(\zeta)$, of which $K$ is a totally ramified extension of degree $a$. For any uniformiser $\pi$ of $K$, writing $1 - \zeta = u\pi^a$ ($u \in o^\times$), we see that $\zeta \in U_a$ but $\zeta \notin U_{a+1}$.

### 3. Raising to the exponent $p$

In this section we study the “homothetie of ratio $p$” in the $\mathbb{Z}_p$-modules $U_n$. We show that this raising to the exponent $p$ maps $U_n$ into $U_{\lambda(n)}$.
(recall that \( \lambda(n) = \inf(pn, n + e) \)) for every \( n > 0 \). The induced map \( \rho_n : U_n/U_{n+1} \to U_{\lambda(n)}/U_{\lambda(n)+1} \) is an isomorphism in all cases except when \( K^\times \) has an element of order \( p \) and \( n = e_1 \), in which case \( \text{Ker}(\rho_n) \) and \( \text{Coker}(\rho_n) \) are cyclic of order \( p \). We also specify these two groups.

**Proposition 27.** — For every \( \eta \in U_n \) \((n > 0)\), one has \( \eta^p \in U_{\lambda(n)} \).

Let \( \pi \) be a uniformiser of \( K \) and write \( \eta = 1 + a\pi^n \) \((a \in \mathfrak{o})\). We have

\[
(1 + a\pi^n)^p = 1 + pa\pi^n + \cdots + a^p\pi^{pn}.
\]

It is sufficient to restrict to \( a \in \mathfrak{o}^\times \); then the valuation of the second (resp. last) term on the right is \( n + e \) (resp. \( pn \)) and the terms not displayed have valuation > \( \lambda(n) \), so \( (1 + a\pi^n)^p \equiv 1 + h(a)\pi^{\lambda(n)} \) \((\text{mod. } p^{\lambda(n)+1})\), with

\[
h(a) = \begin{cases} 
  a^p & \text{if } n < e_1, \\
  a^p - \varepsilon a & \text{if } n = e_1, \\
  -\varepsilon a & \text{if } n > e_1.
\end{cases}
\]

where \( \varepsilon \in \mathfrak{o}^\times \) is such that \(-p = \varepsilon \pi^e \). Hence \( \eta^p \in U_{\lambda(n)} \), as claimed.

**Corollary 28.** — Let \( \pi \) be a uniformiser of \( K \) and write \(-p = \varepsilon \pi^e \) \((\varepsilon \in \mathfrak{o}^\times)\). The following diagram commutes :

\[
\begin{array}{ccc}
U_n/U_{n+1} & \xrightarrow{(\_)^p} & U_{\lambda(n)}/U_{\lambda(n)+1} \\
\downarrow & & \downarrow \\
k & \xrightarrow{h} & k,
\end{array}
\]

where the vertical maps are the isomorphisms \( U_i/U_{i+1} \to k, 1 + a\pi^i \mapsto \bar{a} \) \((a \in \mathfrak{o})\) and the the bottom arrow \( h \) is given by \( (5) \).

**Proposition 29.** — The map \( \rho_n : U_n/U_{n+1} \to U_{\lambda(n)}/U_{\lambda(n)+1} \) is an isomorphism for all \( n > 0 \) except when \( K^\times \) has an element of order \( p \) and \( n = e_1 \), in which case \( \text{Ker}(\rho_n) \) and \( \text{Coker}(\rho_n) \) are cyclic of order \( p \).

The \( \mathbf{F}_p \)-linear map \( (5) \) from \( k \) to \( k \) is an isomorphism in all cases except when \( n = e_1 \) and \( \varepsilon \in k^{(p-1)} \), which happens precisely when \( K^\times \) has an element of order \( p \) (prop. 25). In this case, the kernel has at least two (for if \( \varepsilon = b^{p-1} \) for some \( b \in k^\times \), then \( 0, b \in \text{Ker}(\rho_n) \)) and at most \( p \) elements (because the polynomial \( T^p - \varepsilon T \) can have at most \( p \) roots), hence it has exactly \( p \) elements. Consequently, \( \text{Coker}(\rho_n) \) is also cyclic of order \( p \).
PROPOSITION 30. — For every \( n > e_1 \), the map \( (\cdot)^p : U_n \to U_{n+e} \) is bijective.

Let \( \pi \) be a uniformiser of \( K \) and write \( -p = \varepsilon \pi^e \) (\( \varepsilon \in \mathfrak{o}^\times \)). Let \( y \in U_{n+e} \) and write \( y = 1 + b\pi^{n+e} \) (with \( b \in \mathfrak{o} \)). We seek a root of \( x^p = y \) such that \( x = 1 + a\pi^n \) for some \( a \in \mathfrak{o} \). This leads to the equation
\[
1 + b\pi^{n+e} = 1 + pa\pi^n + \cdots + a^p\pi^{np}.
\]
As we have seen, all the terms on the right, except the first two, have valuation \( > n + e \), in view of \( n > e_1 \). The equation can therefore be rewritten
\[
b = -\varepsilon a + \pi f(a)
\]
for some polynomial \( f \in \mathfrak{o}[T] \). Reducing modulo \( \pi \) yields \( \bar{b} = -\bar{\varepsilon}\bar{a} \), and since \( \bar{\varepsilon} \neq 0 \), this equation has a unique root. By Hensel’s lemma, the same holds for \( x^p = y \). (The injectivity also follows from prop. 26). Cf. [46] (pp. 212–3).

PROPOSITION 31. — For every \( n > e_1 \), the \( \mathbb{Z}_p \)-module \( U_n \) is free of rank \( d = [K : \mathbb{Q}_p] \).

We have seen that \( U_n \) has no element of order \( p \) (prop. 26), so it is sufficient to show that the \( \mathbb{F}_p \)-space \( U_n/U_n^p \) is of dimension \( d \). This is the case because \( U_n^p = U_{n+e} \) (prop. 30) is of index \( q^e = p^f e = p^d \) in \( U_n \).

COROLLARY 32. — The \( \mathbb{Z}_p \)-module \( U_1 \) is finitely generated of rank \( d \).

Suppose that \( K^\times \) has an element of order \( p \), and let \( p\mu \) be the \( p \)-torsion of \( K^\times \). We have seen (prop. 26) that
\[
p\mu \subset U_{e_1}, \quad p\mu \cap U_{e_1+1} = \{1\}.
\]
We also know (prop. 30) that \( U_{pe_1+1} \subset (U_{pe_1} \cap U_1^p) \). So we get a sequence
\[
1 \to p\mu \to U_{e_1}/U_{e_1+1} \xrightarrow{(\cdot)^p} U_{pe_1}/U_{pe_1+1} \to \bar{U}_{pe_1} \to 1.
\]
in which \( \bar{U}_{pe_1} = U_{pe_1}/(U_{pe_1} \cap U_1^p) \).

PROPOSITION 33. — Suppose that \( K^\times \) has an element of order \( p \). The sequence (6) is then exact.

It is clear that \( p\mu \subset \text{Ker}(\cdot)^p \); as the latter group has \( p \) elements (prop. 29), the inclusion is an equality. It is also clear that \( U_{pe_1}^p \subset (U_{pe_1} \cap U_1^p) \); let us show equality here too. If \( \eta \in U_r \) but \( \eta \notin U_{r+1} \) for some \( r < e_1 \), then \( \eta^p \in U_{pr} \) and \( \eta^p \notin U_{pr+1} \) (cor. 28). As \( pr + 1 < pe_1 \),
we have \( \eta^p \notin U_{pe_1} \), which was to be shown. Remark that the proof also
gives the exactness of the sequence
\[
1 \to p^\mu \to \mathbb{U}_{e_1} \xrightarrow{(\cdot)^p} \mathbb{U}_{pe_1} \to \overline{\mathbb{U}}_{pe_1} \to 1.
\]
Therefore the kernel and cokernel of \((\cdot)^p : \mathbb{U}_{e_1} \to \mathbb{U}_{pe_1}\) are trivial when \(K^\times\)
doesn’t have an element of order \(p\); when it does, \(\text{Ker}(\cdot)^p\) and \(\text{Coker}(\cdot)^p\)
are both of order \(p\).

Upon choosing a uniformiser \(\pi\). Let \(\pi\) be an \(\mathfrak{a}\)-basis of \(p\) and write
\(-p = \varepsilon \pi^e\, (\varepsilon \in \mathfrak{o}^\times)\). Consider the following diagram, in which the two
middle vertical arrows are induced by the \(\mathfrak{o}\)-bases \(\pi^e_1, \pi^{pe_1}\) of \(p^{e_1}, p^{pe_1}\), in
which \(\varphi_\varepsilon(a) = a^p - \varepsilon a\), and where we have put \(t = e_1\) to save space. We
have seen (cor. 28, prop. 33) that with these choices, it is commutative.

\[
\begin{array}{ccccccccc}
1 & \to & p^\mu & \to & \mathbb{U}_{e_1}/\mathbb{U}_{e_1+1} & \xrightarrow{(\cdot)^p} & \mathbb{U}_{pe_1}/\mathbb{U}_{pe_1+1} & \to & \mathbb{U}_{pt} & \to & 1 \\
& & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \to & \text{Ker} \varphi_\varepsilon & \to & k & \xrightarrow{\varphi_\varepsilon} & k & \to & k/\varphi_\varepsilon(k) & \to & 0 \\
\end{array}
\]

Upon choosing a primitive \(p\)-th root of \(1\). If we choose such a root \(\zeta\),
then \(\pi_1 = 1 - \zeta\) is an \(\mathfrak{o}\)-basis of \(p^{e_1}\) (prop. 23), and 
\(-p\pi_1 = p(\zeta - 1)\) a
basis of \(p^{pe_1}\). These bases lead to the commutative diagram

\[
\begin{array}{ccccccccc}
1 & \to & p^\mu & \to & \mathbb{U}_{e_1}/\mathbb{U}_{e_1+1} & \xrightarrow{(\cdot)^p} & \mathbb{U}_{pe_1}/\mathbb{U}_{pe_1+1} & \to & \overline{\mathbb{U}}_{pe_1} & \to & 1 \\
& & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \mathbb{F}_p & \to & k & \xrightarrow{\varphi} & k & \xrightarrow{\text{S}_k|\mathbb{F}_p} & \mathbb{F}_p & \to & 0, \\
\end{array}
\]

in which the vertical maps are isomorphisms, with \(\varphi(x) = x^p - x\) and
\(\text{S}_k|\mathbb{F}_p\) the trace map. Here we have \(\varphi\) instead of \(\varphi_\varepsilon\) because 
\(-p\pi_1/\pi_1^p\) is a
1-unit ("Wilson’s theorem", cf. proof of prop. 24).

Explicitly, the isomorphism \(\overline{\mathbb{U}}_{pe_1} \to \mathbb{F}_p\) — induced by the choice \(\zeta \in p^\mu\)
of a generator — sends \(\bar{\eta}\) to \(\text{S}_k|\mathbb{F}_p(\hat{c})\), where \(\eta \in U_{pe_1}, \ c = (1 - \eta)/p(1 - \zeta)\)
and \(\hat{c}\) denotes its image in \(k/\varphi(k)\). (\(^3\)) In particular, when \(k = \mathbb{F}_p\), we have

(\(^3\)) Hasse’s convention in [21, p. 233] amounts to taking \(p\pi_1\) as an \(\mathfrak{o}\)-basis
for \(p^{pe_1}\); one would then have to replace \(\varphi\) by \(\varphi\) in the displayed diagram. Compare the exponent \(S_1(\frac{\alpha-1}{p\lambda_0})\) in formula (13) in footnote (\(^2\)) with our
\(\text{S}_k|\mathbb{F}_p\left(\frac{1-\eta}{p(1-\zeta)}\right)\).
\[ \varphi = 0 \text{ (Fermat’s “little” theorem), and } k/\varphi(k) = k = F_p. \]
The isomorphism is then simply \( \bar{\eta} \mapsto (1 - \eta)/p(1 - \zeta) \text{ (mod. } p) \).

Upon choosing a \((p - 1)\)-th root of \(-p\). Equivalently, as we discovered recently in [28, p. 211], one can choose a \((p - 1)\)-th root \( \Pi \) of \(-p\) in \( K \) (cf. prop. 24); then \( \Pi \) is an \( \alpha \)-basis of \( p^{e_1} \) and \( \Pi^p \) a basis of \( p^{pe_1} \); with these choices for the two middle vertical arrows, the above diagram is commutative.

Notice that if we fix \( \Pi \) and \( \zeta \), there is a unique “natural” bijection, sending \( \Pi \) to \( \zeta \), between the set \( R \) of \((p - 1)\)-th roots of \(-p\) and the set \( P \) of \( p \)-th roots of 1. Indeed, \( R \) is a \((p-1)\)-torsor, and \( P \) a \((\mathbb{Z}/p\mathbb{Z})^\times\)-torsor. But we have a natural isomorphism \( \varphi \mapsto \varphi : p^{-1}\mu \to (\mathbb{Z}/p\mathbb{Z})^\times \) of groups (over \( \mathbb{Z}_p \), so to speak), induced by the passage to the quotient \( \mathbb{Z}_p \to F_p \). The bijection \( R \to P \) in question is \( \varphi \mapsto \varphi^r \) (for every \( \varphi \in p^{-1}\mu \)).

All this would be true for any two torsors under the “same” group \( p^{-1}\mu = (\mathbb{Z}/p\mathbb{Z})^\times \). But more is true here : there is a unique bijection \( \zeta \mapsto \Pi : P \to R \) such that \( \Pi(1 - \zeta) \) is a 1-unit for every \( \zeta \in P \). Indeed, as we saw during the proof of prop. 24, \( u = -p/(1 - \zeta)^{p-1} \) is a 1-unit for every \( \zeta \in P \); denoting by \( \eta \in U_1 \) the unique \((p - 1)\)-th root of \( u \), take \( \Pi = \eta(1 - \zeta) \). Moreover, this bijection is “equivariant” : \( \Pi(1 - \zeta) = \chi(r) \Pi \) for every \( r \in (\mathbb{Z}/p\mathbb{Z})^\times \), where \( \chi(r) \) is the “Teichmüller” lift of \( r : \chi(r) = r \).

The case \( p = 2 \). The choice \( \zeta = -1 \) (or \( \Pi = -2 \)) is forced upon us. Consequently, the isomorphisms are canonical. Thus, when \( k = F_2 \), the isomorphism \( \overline{U}_2 \to F_2 \) is \( \bar{\eta} \mapsto (1 - \bar{\eta})/4 \text{ (mod. } p) \), which is the same as the more familiar \( \eta \mapsto (\eta - 1)/4 \text{ (mod. } p) \) because \( p \) is even.

4. The multiplicative group \((\mathfrak{a}/p^n)^\times\)

**Proposition 34.** — The group \((\mathfrak{a}/p^n)^\times\) is the direct product of its subgroups \( k^\times \) and \( U_1/U_n \). For \( n > e_1 \), the restriction of \( U_1 \to U_1/U_n \) to the torsion subgroup \( W \subset U_1 \) is injective, and the image of \( W \) is a direct factor of \( U_1/U_n \). For \( n > e_1 + e \), the group \( U_1/U_n \) is the direct product of the image of \( W \) with \( d \) cyclic \( p \)-groups (of order \( >1 \)).

The exact sequence \( 1 \to U_1/U_n \to \mathfrak{a}^\times/U_n \to k^\times \to 1 \) has a canonical splitting for every \( n > 0 \), because \( U_1/U_n \) is a \( p \)-group and the order of \( k^\times \) is prime to \( p \).

For \( n > e_1 \), we have \( W \cap U_n = \{1\} \) (prop. 26), so the restriction of the projection \( U_1 \to U_1/U_n \) is injective on \( W \) and the restriction of \( U_1 \to U_1/W \) injective on \( U_n \). Choosing a section \( s : U_1/W \to U_1 \), which
is possible because the $\mathbb{Z}_p$-module $U_1/W$ is free (of rank $d$, prop. 31), write $U_1 = W \times (U_1/W)$; then, quotienting modulo the sub-$\mathbb{Z}_p$-module $U_n \subset U_1/W$, we still get a direct product decomposition $U_1/U_n = W \times (U_1/WU_n)$.

Let us show that for $n > e_1 + e$, the (finite) $\mathbb{Z}_p$-module $M = U_1/WU_n$ is a direct product of $d$ cyclic $p$-groups (of order $> 1$). As it can be generated by $d$ elements (take the image of any $\mathbb{Z}_p$-basis of $U_1/W$), it is sufficient to show that it cannot be generated by $< d$ elements. It is in fact sufficient to exhibit one subgroup which cannot be generated by $< d$ elements. Now, the $\mathbb{Z}_p$-module $U_{n-e}$ is free of rank $d$ (prop. 31), and $U_{n-e} = U_n$. Thus the subgroup $U_{n-e}/U_n \subset U_1/WU_n$, a $d$-dimensional vector $\mathbb{F}_p$-space, cannot be generated by $< d$ elements. Note that $U_{n-e}/U_n$ is a subgroup of $U_1/WU_n$ because $W \cap U_{n-e} = \{1\}$ (prop. 26).

Information about the groups $U_1/U_n$ for small $n$ can be found in [38].

The methods of ideal theory had not succeeded in determining the structure of the groups $(A/a)^\times$, where $A$ is the ring of integers in a number field and $a \subset A$ an ideal. As a curiosity, let us mention that Wilson’s theorem, which we have had to invoke a certain number of times, and which was generalised by Gauss in his Disquisitiones (§78) from $(\mathbb{Z}/p\mathbb{Z})^\times$ to $(\mathbb{Z}/a\mathbb{Z})^\times$ for any $a > 0$, can be further generalised by local means to all $(A/a)^\times$. There are four possibilities for the product of all elements in this group, and precise conditions for each of these possibilities to occur have been given [10].

IV. Unramified kummerian extensions

This Part and the next contain the proofs of our main propositions about discriminants of unramified extensions, unramified kummerian extensions, their rings of integers, the $p$-tic character (prop. 38), and the filtration on $K^{\times}/K^{\times l}$. But before proving prop. 16 and deriving a few corollaries, among them prop. 15, let us compute the greatest $n$ such that the $\mathbb{F}_l$-dimension of $U_n$ is $\neq 0$.

Recall the notation in vigour: $K$ is a finite extension of $\mathbb{Q}_p$, $\mathfrak{o}$ is its ring of integers, with residue field $k$ having $q$ elements. The units $\mathfrak{o}^{\times}$ will also be denoted $U_0$; we denote by $U_{n+1}$ the 1-units of level $> n$ (cf. Part II).

Let $l$ be a prime number such that $K^{\times}$ has an element of order $l$. We define $e_1 = e/(p - 1)$, where $e$ is the absolute ramification index of $K$ if $l = p$, and $e = 0$ if $l \neq p$. The filtration $(U_n)_n$ on $K^{\times}$ induces the filtration $(\bar{U}_n)_n$ on $K^{\times}/K^{\times l}$.

Thus, in both cases ($l \neq p$ and $l = p$), we have $\dim_{\mathbb{F}_l} \bar{U}_{pe_1} = 1$ and
dim\(F_l\), \(\hat{U}_n = 0\) for \(n > pe_1\): the case \(l \neq p\) follows from the fact that \(U_1\) is a \(\mathbb{Z}_p\)-module and \(k^\times\) a cyclic group of order divisible by \(l\); for the case \(l = p\), see prop. 29 and 33.

***

Prop. 16 says that the \(F_l\)-line in \(K^\times/K^\times_l\) which corresponds to the unramified degree-\(l\) extension of \(K\) is the one which lies the deepest in the induced filtration, namely the line \(\hat{U}_{pe_1}\).

**Proof of prop. 16.** Suppose first that \(l \neq p\); then \(l \mid q - 1\), as \(k^\times\) has an element of order \(l\). Let \(M\) be the unramified degree-\(l\) extension of \(K\); its residue field \(m\) is the degree-\(l\) extension of \(k\). To show that \(M\) is associated to the \(F_l\)-line \(U_{pe_1} = \hat{U}_0 = o^\times/o^\times_l = k^\times/k^\times_l\), it is sufficient to show that \(k^\times \subset m^\times_l\).

As the group \(m^\times\) is cyclic of order \(q^l - 1\), and as the subgroup \(k^\times\) is of order \(q - 1\), we have \(k^\times = m^\times a\), where \(a = (q^l - 1)/(q - 1)\). But, as \(a \equiv 1 \pmod{l}\), we have \(1 + q + q^2 + \cdots + q^{l-1} \equiv 0 \pmod{l}\), so \(a\) is a multiple of \(l\), and hence \(k^\times \subset m^\times_l\). It would have also sufficed to remark that the map \(k^\times/k^\times_l \to m^\times/m^\times_l\) is trivial, by Kummer theory.

Let us remark that it is not so much the primality of \(l\), but the fact that \(l\) divides \(q - 1\) (and hence is prime to \(p\)) which has been used in the proof. Thus, for every divisor \(s \mid q - 1\), the degree-\(s\) unramified extension of \(K\) is the kummerian extension obtained by adjoining \(\sqrt[n]{\sigma^\times}\) to \(K\).

Let us come to the case \(l = p\). Let \(M\) now be the degree-\(p\) unramified extension of \(K\); its absolute ramification index is the same as that of \(K\), namely \(e\). We have to show that every element of \(U_{pe_1}\) has a \(p\)-th root in \(M\). Denoting by \((V_n)_{n>0}\) the filtration on the 1-units of \(M\), this amounts to showing that the map \(\hat{U}_{pe_1} \to \hat{V}_{pe_1}\) (induced by the inclusions \(U_i \subset V_i\)) is trivial.

The map \(\hat{U}_{pe_1} \to \hat{V}_{pe_1}\), whose triviality is in question, and which is therefore denoted by \(1?\) in the multiplicative notation in use, is part of the following commutative diagram:

\[
\begin{array}{cccccc}
1 & \to & \mu_p & \to & V_{e_1}/V_{e_1+1} & \to & V_{pe_1}/V_{pe_1+1} & \to & \hat{V}_{pe_1} & \to & 1 \\
= & & & & & & & & \uparrow & & \uparrow 1? \\
1 & \to & \mu_p & \to & U_{e_1}/U_{e_1+1} & \to & U_{pe_1}/U_{pe_1+1} & \to & \hat{U}_{pe_1} & \to & 1.
\end{array}
\]

Upon choosing a generator \(\zeta\) of \(\mu_p\), or, equivalently, a \((p-1)\)-th root of \(-p\),
— cf. the discussion after prop. 33 — the above diagram gets identified with

\[
\begin{array}{ccccccc}
0 & \rightarrow & F_p & \rightarrow & m & \rightarrow & m \\
& & & & \phi \rightarrow & m & \rightarrow \ F_p \\
& & & & & S_m \rightarrow F_p & \rightarrow 0,
\end{array}
\]

in which \(m\) is the residue field of \(M\) and the first three vertical arrows are inclusions. We have to show that the last arrow \(0 \rightarrow F_p \rightarrow F_p\) is indeed 0. But this is the case because \(m\) is the degree-\(p\) extension of \(k\): we have \(k \subset \phi(m)\).

The following corollaries are immediate.

**Corollary 35.** — Let \(\tilde{K}\) be the maximal unramified extension of \(K\). The kernel of the map \(K^x/K^{xl} \rightarrow \tilde{K}^x/\tilde{K}^{xl}\) is \(\tilde{U}_{pe_1}\).

**Corollary 36.** — Let \(\tilde{K}\) be the maximal tamely ramified extension of \(K\). The map \(K^x/K^{xl} \rightarrow \tilde{K}^x/\tilde{K}^{xl}\) is trivial if \(l \neq p\); it has the kernel \(U_{pe_1}\) if \(l = p\).

When \(l = 2\) and \(K\) is the extension of \(\mathbb{Q}_2\) obtained by adjoining \(1\), or \(\sqrt{2}\), or \(\sqrt{3}\), or \(\sqrt{-1}\), A. Kraus [34, p. 376] does explicit calculations in each case to determine the units which become squares in the maximal unramified extension; cf. cor. 46. Cor. 35 and 36 give a criterion for an element of \(K\) to become an \(l\)-th power in \(\tilde{K}\) for any finite extension \(K\) of \(\mathbb{Q}_p\) having a primitive \(l\)-th root of 1, where the primes \(p\) and \(l\) are otherwise arbitrary.

In view of the discussion after prop. 33, things can be made more explicit. Let \(u \in \mathfrak{o}\) be such that its image generates \(k/\phi(k)\). Then the image of \(\eta = 1 - up(1 - \zeta)\) generates \(\tilde{U}_{pe_1}\). Let \(\sqrt[p]{\eta}\) be a root of \(T^p - \eta\); then \(\sqrt[p]{\eta} - 1\) is a root of

\[
T^p + pT^{p-1} + \cdots + pT + up(1 - \zeta),
\]

where the coefficients of the suppressed terms are all divisible by \(p\). Dividing throughout by \((1 - \zeta)^p\) and setting \(S = T/(1 - \zeta)\), we see that \(\rho = (\sqrt[p]{\eta} - 1)/(1 - \zeta)\) is a root of

\[
h(S) = S^p + \cdots + S^{p-1} + \frac{up}{(1 - \zeta)^{p-1}}.
\]
where the coefficients of the suppressed terms are divisible by \(\pi\) — any uniformiser of \(K\). Denoting by \(\hat{h}, \hat{u}\) the reductions modulo \(\pi\) and recalling that \(-p/(1 - \zeta)^{p-1}\) is a 1-unit ("Wilson’s theorem"), we see that
\[
\hat{h}(S) = S^p - S - \hat{u}.
\]
As we had chosen \(u \in \mathfrak{o}\) such that the image of \(\hat{u} \in k\) generates \(k/\wp(k)\), this shows that \(\mathfrak{o} \left[ \rho \right] / \pi\) is the degree-\(p\) extension of \(k\). (Cf. [19, p. 60]).

**Corollary 37.** — For \(\eta = 1 - up(1 - \zeta)\), with \(u \in \mathfrak{o}\) such that \(S_k|F_p(\hat{u}) \neq 0\), the ring of integers of \(K(\sqrt{\eta})\) is \(\mathfrak{o}\left[ (\sqrt{\eta} - 1)/(1 - \zeta) \right]\).

(If we had worked more generally with a characteristic-0 field \(K\) complete with respect to a discrete valuation whose residue field \(k\) is perfect of prime characteristic \(p\) and which contains a primitive \(p\)-th root of 1, the choice of such a root \(\zeta\) would still lead to an isomorphism \(\bar{U}_{pe1} \rightarrow k/\wp(k)\), but these \(F_p\)-spaces need no longer be 1-dimensional.)

Abbreviate \(D = \bar{U}_{pe1}, L = K(\sqrt{D})\) and \(G = \text{Gal}(L|K)\). We have seen that the choice of a generator \(\zeta \in p\mu\) allows us to identify \(D\) and \(p\mu\) with \(\mathbb{Z}/p\mathbb{Z}\). On the other hand, the group \(G\) has a canonical generator \(\varphi\) : the unique element such that \(\varphi(\alpha) \equiv \alpha^q (\mod. pL)\) for every \(\alpha \in \mathfrak{o}_L\), where \(q = \text{Card } k\); it can be used to identify \(G\) with \(\mathbb{Z}/p\mathbb{Z}\). Can the pairing
\[
G \times D \rightarrow p\mu, \quad \langle \sigma, \bar{\eta} \rangle = \frac{\sigma(\zeta)}{\zeta} (\zeta^p = \eta),
\]
which comes from Kummer theory, be made explicit in terms of these identifications?

**Proposition 38** ("Poor man’s explicit reciprocity law"). — Choose and fix a generator \(\zeta \in p\mu\). For \(a \in \mathbb{Z}/p\mathbb{Z}\) and \(\eta \in \bar{U}_{pe1}\), we have \(\langle \varphi^a, \bar{\eta} \rangle = \zeta^{aS_k|F_p(\hat{c})}\), where \(c = \frac{1 - \eta}{p(1 - \zeta)}\) and \(\hat{c}\) is its image in \(k/\wp(k)\).

(More prosaically, if we identify \(G\) (resp. \(\bar{U}_{pe1}\) and \(p\mu\)) with \(\mathbb{Z}/p\mathbb{Z}\) using \(\varphi\) (resp. \(\zeta\)), then the pairing (7) is just \(\langle a, b \rangle = ab\). Recall (cf. the discussion after prop. 33) that the isomorphism \(\bar{U}_{pe1} \rightarrow F_p\) is given by \(\bar{\eta} \mapsto S_k|F_p(\hat{c})\), with \(c = (1 - \eta)/p(1 - \zeta)\).) Note, in particular, that \(\langle \varphi, \bar{\eta} \rangle = \zeta\) if \(\bar{\eta} \in \bar{U}_{pe1}\) corresponds to \(1 \in \mathbb{F}_p\) under the isomorphism \(\bar{U}_{pe1} \rightarrow \mathbb{F}_p\) induced by a generator \(\zeta \in p\mu\).

It is sufficient to show that the choice of \(\zeta\) leads to an identification of the Kummer pairing \(G \times \bar{U}_{pe1} \rightarrow p\mu\) with the Artin-Schreier pairing \(\text{Gal}(l|k) \times k/\wp(k) \rightarrow \mathbb{Z}/p\mathbb{Z}\), where \(l\) denotes — not a prime number as
hitherto, but momentarily the residue field of \( L \); the prop. will follow from this because the Artin-Schreier pairing is just \( \langle \hat{\phi}^a, b \rangle = aS_{k|\mathbb{F}_p}(b) \), where \( \hat{\phi} \) — the image of \( \varphi \) — is the canonical generator of \( \text{Gal}(l|k) \).

(Recall that there is a reciprocity map \( K^\times \to G \), and hence a pairing \( (\ , \)_K : K^\times \times \hat{U}_{pe_1} \to p\mu \) deduced from the Kummer pairing. Remarking that the reciprocity map sends uniformisers of \( K \) to \( \varphi \), prop. 38 allows us to retrieve the last prop. of [46, p. 230].)

***

Let us come to the proof of prop. 15. For the time being, let \( l \) be any prime for which the finite extension \( K \) of \( \mathbb{Q}_p \) has a primitive \( l \)-th root of 1; for the application to discriminants, the case \( l = 2 \) is sufficient.

Let \( M \) be an unramified extension of \( K \); it has the same \( e \) as \( K : e = v_K(l) = v_M(l) \) (= 0 if \( p \neq l \)). We denote by \( (V_n)_{n>0} \) the filtration induced on \( M^\times /M^\times l \) by the canonical filtration of \( M^\times \). The residue field \( m \) of \( M \) is a finite extension of \( k \).

**Proposition 39.** — The norm map \( N_{M|K} : M^\times \to K^\times \) induces an isomorphism \( \hat{V}_{pe_1} \to \hat{U}_{pe_1} \).

If \( p \neq l \), then \( \hat{V}_{pe_1} = m^\times /m^\times l \) and \( \hat{U}_{pe_1} = k^\times /k^\times l \), and the map induced by \( N_{M|K} \) on these two spaces is the same as the isomorphism induced by \( N_{m|k} \) (which is surjective \( m^\times \to k^\times \); cf. also the proof of prop. 16).

Let us come to the case \( p = l \). We have a commutative diagram of horizontal isomorphisms

\[
\begin{array}{ccc}
\hat{V}_{pe_1} & \longrightarrow & m/\varphi(m) \\
\downarrow & & \downarrow S_{m|k} \\
\hat{U}_{pe_1} & \longrightarrow & k/\varphi(k)
\end{array}
\]

in which \( S_{m|k} \) is the trace map; it suffices to show that it is an isomorphism. This follows from the fact that \( S_{m|\mathbb{F}_p} = S_{k|\mathbb{F}_p} \circ S_{m|k} \), where \( S_{m|\mathbb{F}_p} : m/\varphi(m) \to \mathbb{F}_p \) and \( S_{k|\mathbb{F}_p} : k/\varphi(k) \to \mathbb{F}_p \) are the trace maps, which are isomorphisms. Therefore the norm map \( \hat{V}_{pe_1} \to \hat{U}_{pe_1} \) is an isomorphism, as claimed.

Remark that the isomorphism \( S_{m|k} \) sits in the commutative diagram of
\[ \begin{array}{cccccc}
0 & \to & \mathbb{F}_p & \longrightarrow & m & \varphi \to m \longrightarrow m/\varphi(m) \to 0 \\
0 & \downarrow & \downarrow & \downarrow & \downarrow & ~S_m|k \\
0 & \to & \mathbb{F}_p & \longrightarrow & k & \varphi \to k \longrightarrow k/\varphi(k) \to 0 
\end{array} \]

which should be contrasted with the diagram appearing before cor. 35.

The above diagram results from

\[ \begin{array}{cccccc}
1 & \to & p\mu & \to & \mathbf{V}_{e_1}/\mathbf{V}_{e_1+1} & \to & \mathbf{V}_{pe_1}/\mathbf{V}_{pe_1+1} & \to & \mathbf{V}_{pe_1} \to 1 \\
1 & \downarrow & & \downarrow & \downarrow & & \downarrow & & \downarrow \\
1 & \to & p\mu & \to & \mathbf{U}_{e_1}/\mathbf{U}_{e_1+1} & \to & \mathbf{U}_{pe_1}/\mathbf{U}_{pe_1+1} & \to & \mathbf{U}_{pe_1} \to 1 
\end{array} \]

in which the arrows are the norm maps, upon choosing a \( p \)-th root of unity.

Till the end of this Part III, take \( l = 2 \), which is allowed because \( K^\times \) has an element of order 2, namely \(-1\).

**Proposition 40.** — Let \( M|K \) be the unramified quadratic extension. Its discriminant \( d_{M|K} = u \) is the unique element \( \neq 1 \) in \( \mathbf{U}_{pe_1} \).

This is clear if \( p \neq 2 \), because the quadratic extension \( m \) of \( k \) is obtained by adjoining \( \sqrt{u} \). The discriminant of \( T^2 - u \) is \( 4u \), which is the same as \( u \) modulo squares (of units).

Suppose that \( p = 2 \). The quadratic extension \( m \) of \( k \) is obtained by adjoining a root of the polynomial \( T^2 - T - \alpha \), for some \( \alpha \not\in \varphi(k) \). Let \( \omega \in \mathfrak{o} \) be a lift of \( \alpha \); then \( M \) is obtained by adjoining a root \( t \) of \( T^2 - T - \omega \).

As the ring of integers of \( M \) is \( \mathfrak{o}[t] \), the discriminant \( d_{M|K} \) equals \( d = 1 + 4\omega \), modulo \( \mathfrak{o}^{\times 2} \). Because \( 4\mathfrak{o} = p^{2e} \), one has \( d \in \mathbf{U}_{2e} \); one also has \( d \not\in \mathfrak{o}^{\times 2} \), because \( K(\sqrt{d}) = M \). Thus \( d = u \) in \( \mathbf{U}_{2e} \), which was to be proved.

Prop. 15 says that the discriminant \( d_{L|K} \) of an unramified extension \( L|K \) lies in the \( \mathbf{F}_2 \)-line \( \mathbf{U}_{pe_1} = \{1, u\} \), and equals 1 if the degree \([L : K]\) is odd, \( u \) if the degree in question is even. Prop. 40 was the case \([L : K] = 2\).

(Recall that \( e_1 = 0 \) if \( p \neq 2 \).)

**Proof of prop. 15.** As \( L|K \) is galoisian, it contains \( K(\sqrt{d_{L|K}}) \), which is therefore an unramified extension of \( K \), and hence (prop. 16) \( d_{L|K} \in \mathbf{U}_{pe_1} \),

28
If \([L : K]\) is odd, necessarily \(K(\sqrt{d_{L|K}}) = K\), and therefore \(d_{L|K} = 1\).

If \([L : K] = 2g\) is even, \(L\) contains the quadratic unramified extension (prop. 16) \(M = K(\sqrt{u})\) of \(K\), and

\[
d_{L|K} = d_{M|K}^g N_{M|K}(d_{L|M}) \quad \text{(Schachtelungssatz)}
\]

according to [17, p. 19] or [6, p. 143] (or [22, Kap. 25], or [57, p. 213] or even Hilbert — \(D = d^r n(\mathfrak{d}) — \) [31, p. 22]), where \(N_{M|K}\) is the norm map \(M^\times \to K^\times\); it induces the isomorphism \(\bar{V}_{pe_1} \to \bar{U}_{pe_1}\) (prop. 39). The proof is now complete: if \(g\) is odd, the first factor on the right in (8) is 1 and the second \(u\) (prop. 40), whereas if \(g\) is even, the first factor is \(u\) (by the induction hypothesis and prop. 39), and the second is 1 (prop. 40).

Irrespective of the parity of \(g\), the product is always \(u\), which proves the proposition. Finally, it is clear that when \(p = 2\), none of the other \(2^{2d+1} - 2^d\) elements of \(\mathfrak{o}/\mathfrak{o}^{\times 2}\) can be a discriminant, for \(v(d_{L|K}) > 0\) if \(L|K\) is a ramified extension, so \(d_{L|K} \notin \mathfrak{o}^{\times}/\mathfrak{o}^{\times 2}\).

Notice that in the case \(K = \mathbb{Q}_p\), prop. 15 reduces to the Stickelberger-Hensel th. 5 if \(p \neq 2\), to their th. 6 if \(p = 2\). The analogy between prop. 15, which determines relative discriminants at the \(p\)-adic places, and prop. 9, which determines them at the archimedean places, is striking.

The Pellet-Voronoï theorem (th. 3 and 4) can now be extended from \(\mathbb{F}_p\) (\(p \neq 2\)) to any finite field \(k\).

**Corollary 41.** — *Let \(p\) be an odd prime (resp. \(p = 2\)), \(k\) a finite extension of \(\mathbb{F}_p\) and \(f \in k[T]\) a separable polynomial. The discriminant of \(k[T]/fk[T]\) is trivial in the 2-element multiplicative group \(k^\times/k^{\times 2}\) (resp. additive group \(k/\mathfrak{o}(k)\)) if and only if the number of even-degree irreducible factors of \(f\) is even.*

***

*Relative discriminants of ramified extensions.* Having found the correct relative analogue (prop. 15) of the Stickelberger-Hensel congruence (th. 5 and 6), what about the relative version of Dedekind’s th. 10, which says that the discriminant of a ramified extension of \(\mathbb{Q}_2\) is \(\equiv 0 \pmod{4}\)? Part VII is devoted to this problem, where the valuation of the relative discriminant of a prime-degree cyclic extension of local fields (of arbitrary residual characteristic) is computed.

**V. The filtration on \(K^\times/K^{\times p}\)**

In this Part, we make a finer study of the filtration on \(K^\times/K^{\times p}\), which helps us see the precise relationship between th. 14 and prop. 15. In fact,
we shall give three equivalent ways of looking at this filtration. Then we compute a number of examples which illustrate some of our results and explain the theoretical underpinnings of some results in the literature.

When the $\mathbb{Z}_p$-module $U_1$ of Einseinheiten is free, a basis can be found in [15, I, §6]. One can also find there and in VI, §5 a basis for the $(\mathbb{Z}/p\mathbb{Z})$-module $U_1/U_1^p$ when the torsion subgroup of $U_1$ has order $p^r$.

The first definition of the filtration on $K^\times/K^\times p$. Let us put $U_0 = \overline{1}$ and $\bar{U}_n = U_n/(U_n \cap U_0^p)$. We thus get a filtration on $K^\times/K^\times p$ by sub-$\mathbb{F}_p$-spaces

$$
\cdots \subset \bar{U}_n \subset \cdots \subset \bar{U}_1 \subset \bar{U}_0 \subset K^\times/K^\times p.
$$

We have seen that $\bar{U}_n = \{\bar{1}\}$ if $n > pe_1$ (prop. 30; note that $pe_1 = e_1 + e$) and that $\bar{U}_{pe_1}$ is an $\mathbb{F}_p$-line if $K^\times$ has an element of order $p$ (prop. 33), otherwise $\bar{U}_{pe_1} = \{\bar{1}\}$. Let us show that the other inclusions $\bar{U}_{n+1} \subset \bar{U}_n$ are an equality if $p|n$ and of codimension $f$ otherwise.

**Proposition 42.** — Let $\zeta \in \bar{K}^\times$ be an element of order $p$. Then

$$
\dim_{\mathbb{F}_p} \bar{U}_n/\bar{U}_{n+1} = \begin{cases} 
0 & \text{if } n > pe_1, \\
1 & \text{if } n = pe_1 \text{ and } \zeta \in K^\times, \\
0 & \text{if } n = pe_1 \text{ and } \zeta \notin K^\times, \\
0 & \text{if } n < pe_1 \text{ and } p|n, \\
f & \text{otherwise}.
\end{cases}
$$

(Note that the condition " $\zeta \in K^\times$ " just means that $K^\times$ has an element of order $p$).

We have already seen the cases $n > pe_1$ (prop. 30) and $n = pe_1$ (prop. 29). Suppose next that $n = ps$ for some $s < e_1$. Then, $U_{ps} \cap U_0^p = U_p^s$, whereas $U_{ps+1} \cap U_0^p = U_{ps+1}^p$, as follows from prop. 29 (cf. the proof of prop. 33). Thus we have a commutative diagram

$$
\begin{array}{c}
1 \\
\downarrow \\
1 \rightarrow U_{s+1} \rightarrow U_s \rightarrow U_s/U_{s+1} \rightarrow 1 \\
(\)p \downarrow \quad (\)p \downarrow \quad (\)p \\
1 \rightarrow U_{ps+1} \rightarrow U_{ps} \rightarrow U_{ps}/U_{ps+1} \rightarrow 1 \\
\downarrow \quad \downarrow \quad \downarrow \\
\bar{U}_{ps+1} \rightarrow \bar{U}_{ps} \rightarrow 1
\end{array}
$$
both whose rows are exact, as are the columns (prop. 29). Hence the inclusion \( \bar{U}_{ps+1} \to \bar{U}_{ps} \) is an isomorphism by the serpent lemma. Consider finally the case when \( n = ps + g \) (\( s < e_1, 0 < g < p \)) is \( < pe_1 \) and prime to \( p \). Then \( U_n \cap U_0^p = U_{s+1}^p \) and \( U_{n+1} \cap U_0^p = U_{s+1}^p \), as follows from prop. 29 by considerations similar to the ones above. The inclusions \( U_{s+1}^p \subset U_{n+1} \subset U_n \) induce the short exact sequence

\[
1 \to \bar{U}_{n+1} \to \bar{U}_n \to U_n/U_{n+1} \to 1
\]

which proves the proposition because we know that the last \( F_p \)-space is of dimension \( f \).

As a check, the dimension of \( \bar{U}_0 = \bar{U}_1 \), according to prop. 42, turns out to be \( e_1(p - 1)f = ef = d \) if \( \zeta \not\in K^\times \), which is what it is according to cor. 32.

**Corollary 43.** — Suppose that \( K^\times \) has an element \( \zeta \) of order \( p \). Then \( \dim_{F_p} K^\times/K^{\times p} = 2 + d = 2 + ef \) and, for \( m = pe_1 - t \) with \( t \in [0, pe_1[ \),

\[
\dim_{F_p} \bar{U}_m = 1 + \left( t - \left\lfloor \frac{t}{p} \right\rfloor \right) f.
\]

When \( K^\times \) has no element of order \( p \), subtract 1 from these dimensions.

Concretely, let \( pe_1 - 1 = m_1 > \cdots > m_e = 1 \) be the \( e = (p - 1)e_1 \) numbers in \( [1, pe_1] \) which are prime to \( p \). When \( \zeta \in K \), we have

\[
\dim_{F_p} \bar{U}_{m_i} = 1 + if \quad (i \in [1, e]).
\]

The second definition of the filtration on \( K^\times/K^{\times p} \). Because \( U_{pe_1+1} \subset U_0^p \) (prop. 30), the \( F_p \)-spaces \( \bar{U}_n \) can be described entirely in terms of the ring \( \mathcal{O}/p^{pe_1+1} \), or rather its group of units \( W_0 = (\mathcal{O}/p^{pe_1+1})^\times \), which comes equipped with the filtration

\[
W_n = U_n/U_{pe_1+1} = \text{Ker}((\mathcal{O}/p^{pe_1+1})^\times \to (\mathcal{O}/p^n)^\times) \quad (n \in [0, pe_1 + 1]).
\]

**Proposition 44.** — We have \( \bar{U}_n = W_n/(W_n \cap W_0^p) \) for \( n \in [0, pe_1 + 1] \).

This follows from the fact that the image of \( (U_n \cap U_0^p) \subset U_n \), modulo \( U_{pe_1+1} \), is \( (W_n \cap W_0^p) \subset W_n \). Indeed, the inclusion \( (U_n \cap U_0^p)/U_{pe_1+1} \subset (W_n \cap W_0^p) \) is clear. Conversely, suppose that \( \bar{y} \in W_0^p \) for some \( y \in U_n \); we have to show that \( y \in U_0^p \). Let \( x \in U_0 \) be such that \( \bar{y} = \bar{x}^p \). Then \( y/x^p \in U_{pe_1+1} \), hence there is a (unique) \( \gamma \in U_{e_1+1} \) such that \( y/x^p = \gamma^p \). Consequently, \( y \in U_0^p \). An equivalent way of saying it : \( W_0^p = U_0^p/U_{pe_1+1} \) (prop. 30).
The third definition of the filtration on $K^\times/K^{\times p}$. Let us come to the definition most commonly used in the literature. The following proposition is also true for $l \neq p$, but it is then trivial.

**Proposition 45.** — For $x \in \mathfrak{o}^\times$ and $n > 0$, let $\bar{x}$ be its image in $\mathfrak{o}^\times/\mathfrak{o}^{\times p}$ and $\hat{x}$ the image in $(\mathfrak{o}/\mathfrak{p}^n)^\times$. Then

$$\bar{x} \in \bar{U}_n \iff \hat{x} \in (\mathfrak{o}/\mathfrak{p}^n)^{\times p}.$$ 

Suppose first that $\bar{x} \in \bar{U}_n$. Then there is a $y \in \mathfrak{o}^\times$ such that $xy^p \in U_n$. But then $\hat{x} = \hat{y}^p$, hence $\hat{x} \in (\mathfrak{o}/\mathfrak{p}^n)^{\times p}$. Conversely, suppose that $\hat{x} \in (\mathfrak{o}/\mathfrak{p}^n)^{\times p}$, and write $\hat{x} = \hat{y}^p$ for some $y \in \mathfrak{o}^\times$. Then $xy^p$ belongs to $U_n$ and hence $\bar{x} \in \bar{U}_n$.

Prop. 45 says that $\bar{U}_n = \text{Ker}(\mathfrak{o}^\times/\mathfrak{o}^{\times p} \to G_n/G_p^n)$, where $G_n = (\mathfrak{o}/\mathfrak{p}^n)^\times$. In the light of the case $p = 2$ of this prop., th. 14 is equivalent to “$d_{L|K} \in \bar{U}_{2e}$”, whereas prop. 15 says, writing $\bar{U}_{2e} = \{1, u\}$, that $d_{L|K} = 1$ for $[L : K]$ odd and $d_{L|K} = u$ for $[L : K]$ even. The difference is already clear for $K = \mathbb{Q}_2$, where Hensel’s th. 6 is more precise, in that it specifies when $D \equiv 1 \pmod{\pi}$ and when $D \equiv 5 \pmod{\pi}$, than Schur’s th. 11 ($D \equiv 1 \pmod{4}$).

Let us make the criterion of cor. 35 explicit for $l = p$, in terms of reduction modulo $\mathfrak{p}^{pe_1}$.

**Corollary 46.** — A unit $x \in \mathfrak{o}^\times$ becomes a $p$-th power in the maximal unramified extension, or in the maximal tamely ramified extension, if and only if it is a $p$-th power modulo $\mathfrak{p}^{pe_1}$.

**Example 47 ([34, p. 376]).** — Let $K = \mathbb{Q}_2(\pi)$, $\pi^3 = 2$, so that $e = 3$ and $\mathfrak{p}^{pe_1} = 4\mathfrak{o}$. A unit becomes a square in the maximal unramified extension of $K$ if and only if it is congruent to one of

$$1, 1 + \pi^2 + \pi^4, 1 + \pi^2 + \pi^5, 1 + \pi^4 + \pi^5 \pmod{\pi}. $$

By cor. 46, we have to determine the squares in $(\mathfrak{o}/4\mathfrak{o})^\times = U_1/U_6$ or (prop. 29) the image of the map $(\mathfrak{o}/4\mathfrak{o})^\times : U_1/U_3 \to U_1/U_6$. As the above list consists of the squares of $1, 1 + \pi, 1 + \pi^2, 1 + \pi + \pi^2$, we are done.

**Example 48.** — A unit in $K = \mathbb{Q}_2(\pi)$, $\pi^3 = 2$, is the discriminant of an odd-degree (resp. even-degree) unramified extension if and only if, up to squares in $(\mathfrak{o}/\pi^7\mathfrak{o})^\times$, it is

$$\equiv 1 \pmod{\pi^7}.$$
Indeed, by the second definition of the filtration on \( \mathfrak{o}^\times/\mathfrak{o}^\times^2 \), the group \( \bar{U}_6 \) can be identified with \( \{1, 1 + \pi^6\} \). which, in the notation of that definition, is the kernel \( W_6 = \{1, 1 + \pi^6\} \) of \( U_1/U_7 \to U_1/U_6 \) modulo its intersection \( \{1\} \) with the subgroup of squares in \( U_1/U_7 \).

\[ \text{Example 49.} \quad \text{Let } \zeta \in \bar{Q}_p^\times \text{ be an element of order } p. \text{ A unit of } K = Q_p(\zeta) \text{ becomes a } p\text{-th power in the maximal tamely ramified extension of } K \text{ if, and only if, it is } \equiv 1 \pmod{p^e}, \text{ where } p \text{ is the maximal ideal of the ring of integers of } K. \]

Here \( e = p - 1 \) and \( e_1 = 1 \). By cor. 35, we have to determine the \( p \)-th powers in \( U_1/U_p \). But the raising-to-the-exponent-\( p \) map \( (\ )^p \) takes \( U_1 \) to \( U_p \) (prop. 27), so the only \( p \)-th power in \( U_1/U_p \) is 1.

\[ \text{Example 50 [22, Kap. 15].} \quad K(\sqrt{-1}) \text{ is the unramified quadratic extension of } K = Q_2(\sqrt{3}). \]

It suffices (prop. 16, prop. 45) to show that \(-1\) is a square \( \pmod{\pi^4} \), where \( \pi = \sqrt{3} - 1 \) is a uniformiser of \( K \). Indeed, we have \(-1 = (\sqrt{3})^2 - 4\), which implies that \(-1 \equiv (1 + \pi)^2 \pmod{\pi^4} \).

More generally, the compositum \( L_1L_2 \) of two linearly disjoint degree-\( p \) ramified kummerian extensions \( L_1 = K(\sqrt{D_1}), L_2 = K(\sqrt{D_2}) \) is unramified over \( L_1, L_2 \) precisely when the \( F_p \)-plane \( D_1D_2 \) contains the line \( \bar{U}_{pe_1} \):

\[ \text{Example 51.} \quad \text{Let } K \text{ be a finite extension of } Q_p(\zeta) \text{ (}\zeta^p = 1 \text{ but } \zeta \neq 1\text{) and let } D_1, D_2 \text{ be two distinct } F_p \text{-lines in } K^\times/K^\times, \text{ distinct from } \bar{U}_{pe_1}, \text{ such that the plane } D_1D_2 \text{ contains } \bar{U}_{pe_1}. \text{ Then the compositum } L_1L_2 \text{ is the unramified degree-} p \text{ extension of } L_1 = K(\sqrt{D_1}) \text{ and of } L_2 = K(\sqrt{D_2}). \]

This results from the computation of the relative ramification index and residual degree of the degree-\( p^2 \) extension \( L_1L_2|K \) by multiplicativity in three different ways, the intermediate extensions being respectively \( L_1, L_2, \) and the degree-\( p \) unramified extension \( L \) of \( K \), which is contained in \( L_1L_2 \) because the plane \( D_1D_2 \) contains the line \( \bar{U}_{pe_1} \). The only possibility for the said relative ramification index and residual degree is \( p \) and \( p \), which forces the conclusion.

Specifically, for \( K = Q_p(\zeta) \), take \( D_1 \) to be the \( F_p \)-line generated by \( \bar{\zeta} \) in \( K^\times/K^\times, \) and \( D_2 \) to be any line in the plane \( D_1\bar{U}_p \) distinct from the lines \( D_1, \bar{U}_p \). Then \( L_2(\sqrt{\zeta}) \) is the unramified degree-\( p \) extension of \( L_2 = K(\sqrt{D_2}) \). Ex. 50 illustrates this observation for \( p = 2 \).

(\text{Abhyankar’s lemma asserts that if } K|Q_p, L_1|K, L_2|K \text{ are finite extensions with } L_1|K \text{ tame of ramification index dividing the degree of } L_2|K, \text{ then the extension } L_1L_2|L_2 \text{ is unramified, cf. [39, p. 236]. One can see} \]
that the requirement of tameness cannot be dispensed with: take $K$ containing $\zeta$, and $L_1 = K(\sqrt[n]{D_1})$, $L_2 = K(\sqrt[n]{D_2})$, where the $F_p$-lines $D_1, D_2$ in $K^\times/K^{\times p}$ are chosen to be different and such that the plane $D_1D_2$ does not contain the line $\bar{U}_{pe_1}$, where $(p - 1)e_1$ is the absolute ramification index of $K$.)

VI. A brief history of primary numbers

We pass in review the problem of characterising, among prime-degree kummerian extensions of local fields, the unramified one, and of computing the valuation of the discriminant for the ramified ones.

As in Part I, there is no pretence at exhaustiveness. These two Parts have been added merely to share with the reader some of the wonderful theorems which we have discovered in the classical literature. They are presented roughly in the order in which we came across them; this explains the chronological zigzag.

Fröhlich (1960). After the proof of prop. 16, we wanted to generalise, from quadratic extensions to prime-degree kummerian extensions, results of Fröhlich on the valuation of the discriminant. We quote the result without explaining his peculiar notation; a translation into our notation is therefore provided.

**Theorem 52** [17, p. 24]. — Let $p$ be a prime lying above 2.

(i) If $\alpha \equiv 0 \pmod{p}$ then $\delta_p = 4_p \alpha_p$.

(ii) If $\alpha_p \in U_p$ and if $s$ is the greatest positive integer such that firstly

$$4 \equiv 0 \pmod{p^{2s}}$$

and in the second place

$$\exists \gamma_p \in U_p \quad \text{with} \quad \alpha_p \equiv \gamma_p^2 \pmod{p^{2s}},$$

then

$$\delta_p = (2_p \pi^{-1})^2 \alpha_p, \quad \text{where} \quad \pi \in \mathfrak{o}_p^\times, \quad (\pi) = p^s.$$ 

(Let $K$ be a finite extension of $\mathbb{Q}_2$ and let $L = K(\sqrt{\alpha})$ for some $\alpha \in K^\times$. If $\alpha \in \bar{U}_m$ but $\alpha \not\in \bar{U}_{m+1}$ for some $m < 2e$ (with the convention that $\bar{U}_0 = K^\times/K^{\times 2}$), then $v_K(d_{L|K}) = 1 + 2e - m$. If $\alpha \in \bar{U}_{2e}$ but $\alpha \not\in \bar{U}_{2e+1}$, then $v_K(d_{L|K}) = 0.$)
Hecke (1923). A search in the literature revealed Sätze 118–120 in Hecke’s Vorlesungen, which crown his treatment of Allgemeine Arithmetik der Zahlkörper. He is studying the behaviour of primes in a degree-$l$ kummerian extension $K = k(\sqrt[l]{\mu})$ of a number field $k$ ($l$ being a prime for which $k^\times$ has an element $\zeta$ of order $l$) : when does a prime $p$ of $k$ remain a prime, or become the $l$-th power of a prime, or split as a product of $l$ (distinct) primes in $K$? Satz 118 says:

**Theorem 53 ([23, p. 150]).** — Es gehe das Primideal $p$ in der Zahl $\mu$ genau in der Potenz $p^a$ auf. Wenn dann $a$ nicht durch $l$ teilbar ist, so wird $p$ die $l$te Potenz eines Primideals in $K : p = \mathfrak{P}^l$. Wenn aber $a = 0$ ist und $p$ nicht in $\mu$ aufgeht, so wird $p$ in $K$ das Produkt von $l$ verschiedenen Primidealen, falls die Kongruenz

$$\mu \equiv \xi^l \pmod{p}$$

durch eine ganze Zahl $\xi$ in $k$ lösbar ist, dagegen bleibt $p$ ein Primideal in $K$, falls diese Kongruenz unlösbar ist.

(Let $a$ be the $p$-adic valuation of $\mu$. If $l$ does not divide $a$, then $p$ becomes the $l$-th power of a prime $\mathfrak{P}$ in $K$. When $a = 0$ but $p$ does not divide $l$, then $p$ splits in $K$ as a product of $l$ distinct prime ideals if the displayed congruence is solvable by an integer $\xi$ of $k$, otherwise $p$ remains a prime in $K$.)

The first part of the corresponding local statement — for $k|\mathbb{Q}_p$ a finite extension and $l$ a prime for which $k^\times$ has an element of order $l$ — would say that if $\mu \in k^\times/k^\times_l$ but $\mu \not\in \mathfrak{o}^\times/\mathfrak{o}^\times_l$, then the extension $k(\sqrt[l]{\mu})$ is totally ramified. This is easy, because $\mu$ can be taken to have valuation 1, and the polynomial $T^l - \mu$ is then Eisenstein.

The second part would say that if $l \neq p$ and if $\mu \in \mathfrak{o}^\times$, then $\mu \in \mathfrak{o}^\times_l$ if $\mu$ is an $l$-th power in the residue field : this follows from Hensel’s lemma. However, if $\mu \not\in \mathfrak{o}^\times_l$, then the extension $k(\sqrt[l]{\mu})$ is unramified : this is precisely the content of the case $l \neq p$ of prop. 16.

Hecke had the global result for $p = l$ as well; Satz 119 says:

**Theorem 54 ([23, p. 152]).** — Es sei $l$ ein primfaktor von $1 - \zeta$, die darin genau zur $a$ten Potenz aufgeht : $1 - \zeta = l^a1_l$ ; es gehe $l$ nicht in $\mu$ auf. Dann zerfällt $l$ in $l$ voneinander verschiedene Faktoren in $K(\sqrt[l]{\mu}; k)$, falls die Kongruenz

$$\mu \equiv \xi^l \pmod{l^{al+1}}$$

durch eine Zahl $\xi$ in $k$ lösbar ist. Es bleibt $l$ auch in $K$ Primideal, wenn zwar die Kongruenz

$$\mu \equiv \xi^l \pmod{l^{al}}$$

35
aber nicht (82) lösbar ist. Endlich wird l die l-te Potenz eines Primideals in K, wenn auch diese Kongruenz (83) unlösbar ist.

(Let l be a prime of k dividing 1 − ζ and let a be the l-adic valuation of 1 − ζ; suppose that l does not divide µ. Then l splits as a product of l distinct primes in K = k(√µ) if the congruence (82) can be solved by an integer ξ of k. If the congruence (83) can be solved, but not (82), then l remains a prime in K. Finally, l becomes the l-th power of a prime in K if the congruence (83) cannot be solved.)

Even Hasse’s formulation (Ist ζ0 eine primitive l-te Einheitswurzel, l0 = λ0 = 1 − ζ0 der Primteiler von l im Körper der l-ten Einheitswurzeln, und sind lε0 und lε = lε0(l−1) die Beiträge von l zu l0 und l = l0−1, so ist die Bedingung
\[ \alpha ≡ \alpha_0^l \pmod{lεlε_0} \]
notwendig und hinreichend dafür, daß l nicht im Führer von k(√α) aufgeht.) [21, p. 232] is global, as is clear from the context.

The local version (for k|Q, finite, containing an l-th root of 1) would say that for µ ≠ 1 in o×/o×l, the extension k(√µ) is totally ramified, unless µ ∈ ℤe1, in which case it is unramified: this is the case l = p of prop. 16. The local version of the first part of th. 54 would say that for µ ∈ o×, the condition “µ ∈ o×l” is equivalent to “µ = (a/pεlε+1)×l” : this follows from props. 29 and 44, in view of the fact that a = e1 (prop. 23).

In view of prop. 30 and 45, we see that prop. 16 is the precise local counterpart of the global th. 53 and 54, which are its immediate corollaries. Let us mention that th. 53 and 54 were first proved by Furtwängler [18] respectively as his Sätze 3 and 4; the results go back in part to Kummer. Hecke singles out the following consequence (Satz 120) :

**Theorem 55** ([23, p. 154]). — Die Relativdiskriminante von K(√µ; k) in bezug auf k ist dann und nur dann gleich 1, wenn µ die l-te Potenz eines Ideals in k ist, und gleichzeitig, sofern dann µ zu l teilerfremd gewählt wird, die Kongruenz \[ µ ≡ ξ^l \pmod{(1 − ξ)^l} \] durch eine Zahl ξ in k lösbar ist.

(The relative discriminant of K = k(√µ) over k equals 1 precisely when µ is the l-th power of an ideal in k and moreover, when µ is prime to l, the congruence \[ µ ≡ ξ^l \pmod{(1 − ξ)^l} \] admits a solution ξ in k.)

**Hilbert (1897).** Somewhat later we found that the case l ≠ 2 of Hecke’s theorems is a generalisation of a part of Satz 148 in Hilbert’s Zahlbericht, which treats the case k = Q(ζ); the other part computes the valuation of the discriminant for ramified prime-degree kummerian
extensions, again for this special base field. Hilbert’s notation for \( \mathbb{Q}(\zeta) \) is \( k(\zeta) \); he takes an integer \( \mu \) in this field which is not an \( l \)-th power.

*Satz* 148 says:

**Theorem 56 ([32, p. 251]).** — *Es werde* \( \lambda = 1 - \zeta \) und \( l = (\lambda) \) *gesetzt. Geht ein von \( l \) verschiedene Primideal \( p \) des Kreiskörpers \( k(\zeta) \) in der Zahl \( \mu \) genau zur \( e \)-ten Potenz auf, so enthält, wenn der Exponent \( e \) zu \( l \) prim ist, die Relativdiskriminante des durch \( M = \sqrt[p]{\mu} \) und \( \zeta \) bestimmten Kummerschen Körpers in bezug auf \( k(\zeta) \) genau die Potenz \( p^{l-1} \) von \( p \) als Faktor. Ist dagegen der Exponent \( e \) ein vielfaches von \( l \), so fällt diese Relativdiskriminante prim zu \( p \) aus.

Was das Primideal \( l \) betrifft, so können wir zunächst den Umstand ausschließen, daß die Zahl \( \mu \) durch \( l \) teilbar ist und dabei \( l \) genau in einer solchen Potenz enthält, deren Exponent ein Vielfaches von \( l \) ist; denn alsdann könnte der Zahl \( \mu \) sofort durch eine zu \( l \) prime Zahl \( \mu^* \) ersetzt werden, so daß \( k(\sqrt[p]{\mu^*}, \zeta) \) derselbe Körper wie \( k(\sqrt[p]{\mu}, \zeta) \) ist. Unter Ausschluß des genannten Umstandes haben wir die zwei möglichen Fälle, daß \( \mu \) genau eine Potenz von \( l \) enthält, deren Exponent zu \( l \) prim ist, oder daß \( \mu \) nicht durch \( l \) teilbar ist. Im ersteren Falle ist die Relativdiskriminante von \( k(\sqrt[p]{\mu}, \zeta) \) in bezug auf \( k(\zeta) \) genau durch die Potenz \( l^{l^2-1} \) teilbar. Im zweiten Falle sei \( m \) der höchste Exponent \( \leq l \), für den es eine Zahl \( \alpha \) in \( k(\zeta) \) gibt, so daß \( \mu \equiv \alpha^l \) nach \( l^m \) ausfällt. Jene Relativdiskriminante ist dann im Falle \( m = l \) zu \( l \) prim; sie ist dann im Falle \( m < l \) genau durch die Potenz \( l^{(l-1)(l-m+1)} \) von \( l \) teilbar.

(Put \( l = (1 - \zeta) \). If for some prime \( p \neq l \) of \( k(\zeta) \), the number \( \mu \) is divisible precisely by the \( e \)-th power of \( p \), and if \( e \) is prime to \( l \), then the relative discriminant of \( k(\sqrt[p]{\mu}, \zeta) \) over \( k(\zeta) \) is divisible precisely by \( p^{l-1} \). If, however, \( l \) divides \( e \), then the relative discriminant is prime to \( p \).

As for the prime \( l \), we may exclude the case in which \( \mu \) is divisible by a power of \( l \) whose exponent is a multiple of \( l \), for in this case we can replace \( \mu \) by \( \mu^* \) which is prime to \( l \) and such that \( k(\sqrt[p]{\mu^*}, \zeta) = k(\sqrt[p]{\mu}, \zeta) \).

Leaving aside this case, there are two possibilities: either \( \mu \) is divisible by a power of \( l \) whose exponent is prime to \( l \), or \( \mu \) is prime to \( l \). In the first case, the relative discriminant of \( k(\sqrt[p]{\mu}, \zeta) \) over \( k(\zeta) \) is divisible precisely by \( l^{l^2-1} \). In the second case, let \( m \leq l \) be the highest exponent for which there is an integer \( \alpha \) in \( k(\zeta) \) such that \( \mu \equiv \alpha^l \) (mod. \( l^m \)). The relative discriminant is then prime to \( l \) if \( m = l \), and divisible precisely by \( l^{(l-1)(1+l-m)} \) if \( m < l \).

The proof in the *Zahlbericht* needs tiefliegende Sätze mit schwierigen Beweisen, in Hensel’s words [27, p. 200]. Observe that in the first case
(\(v_l(\mu)\) is prime to \(l\)) Hilbert could have defined \(m = 0\).

***

But Stickelberger’s th. 1 is more closely related to Satz 96, which treats the prime 2 missing from Satz 148 (th. 56). Hilbert is working with the quadratic field \(k = \mathbb{Q}(\sqrt{m})\) for some squarefree integer \(m \neq 1\). Following Dedekind (cf. th. 10), he first determines the ring of integers of \(k\) and its discriminant. Satz 95 says:

**Theorem 57 ([32, p. 157]).** — Eine Basis der quadratischen Körpers \(k\) bilden die Zahlen 1, \(\omega\), wenn

\[
\omega = \frac{1 + \sqrt{m}}{2}, \text{ bzw. } \omega = \sqrt{m}
\]

genommen wird, je nachdem die Zahl \(m \equiv 1\) nach 4 oder nicht. Die Diskriminante von \(k\) ist, entsprechend diesen zwei Fällen,

\[d = m, \text{ bzw. } d = 4m.\]

(\(\omega\) being defined as above according as \(m \equiv 1\) (mod 4) or not, 1, \(\omega\) is a \(\mathbb{Z}\)-basis of the ring of integers of \(k\), and the discriminant of \(k\) is \(m\) or \(4m\) respectively.)

The splitting in \(k\) of rational primes is treated in Satz 96, which says:

**Theorem 58 ([32, p. 158]).** — Jede in \(d\) aufgehende rationale Primzahl \(l\) ist gleich dem Quadrat eines Primideals in \(k\). Jede ungerade, in \(d\) nicht aufgehende rationale Primzahl \(p\) zerfällt in \(k\) entweder in das Produkt zweier verschiedener, zu einander konjugierter Primideale ersten Grades \(p\) und \(p'\) oder stellt selbst ein Primideal zweiten Grades vor, je nachdem \(d\) quadratischer Rest oder Nichtrest für \(p\) ist. Die Primzahl 2 ist im Falle \(m \equiv 1\) nach 4 in \(k\) ein Produkt zweier voneinander verschiedener konjugierter Primideale zerlegbar oder selber Primideal, je nachdem \(m \equiv 1\) oder \(\equiv 5\) nach 8 ausfällt.

(If a prime number \(l\) divides \(d\), then it becomes the square of a prime ideal in \(k\). An odd prime number \(p\) which does not divide \(d\) splits as the product of two distinct degree-1 mutually conjugate prime ideals or becomes a degree-2 prime ideal in \(k\) according as \(d\) is a quadratic residue or not (mod \(p\)). In the case \(m \equiv 1\) (mod 4), the prime 2 splits into the product of two distinct conjugate prime ideals or remains a prime in \(k\) according as \(m \equiv 1\) or \(\equiv 5\) (mod 8).)
Notice that, except for the determination of the ring of integers, Hilbert could have made these two theorems a part of his *Satz* 148 if he had allowed the prime \( l \) there to equal 2.

**Hasse (1927).** Thus Hecke’s *Sätze* 118 and 119 generalise a part of Hilbert’s *Sätze* 95, 96 and 148, but leave out the computation of the discriminant for ramified Kummerian extensions of degree equal to the residual characteristic. Our conjectural answer, which amounted to the equality \( t + m = le_1 \) involving the “level” of a line \( D \neq \bar{U}_{le_1} \) in \( K^\times/K^\times l \) (the integer \( m \) such that \( D \subset \bar{U}_m \) but \( D \not\subset \bar{U}_{m+1} \)) and the break \( t \) in the filtration of \( \text{Gal}(L|K) \), \( L = K(\sqrt[l]{D}) \), by higher ramification groups as explained below, was found proved in *Satz* 10 (p. 266) of Hasse’s *Klassenkörperbericht* [20], in the form of the equality \( u + v = e_0 l \). He is working with number fields, but the question is purely local, so we formulate it for local fields. See Part VII.

***

**Hensel (1921).** Our most recent find, and the one most relevant to our proof of prop. 16, are three related papers [26], [27], [28] of Hensel. We merely reproduce his arguments in the \((l, l)\)-case, leaving the problem of interpretation to the reader. In the first one (pp. 117–8), he denotes by \( \zeta \) a primitive \( l \)-th root of 1, where \( l \) is a prime \( \neq 2 \), and considers an irreducible equation \( x^l - A = 0 \) over the cyclotomic field \( K(\zeta) \), which we would denote by \( Q(\zeta) \), and in which \( l \sim l^{l-1} \), with \( l \) the prime ideal generated by \( \lambda = 1 - \zeta \). In \( K(l) = Q_l(\zeta) \), or rather in its multiplicative group modulo \( l \)-th powers, he writes

(16.a) \[ A = \lambda^a (1 - \lambda)^{c_1} (1 - \lambda^2)^{c_2} \cdots (1 - \lambda^l)^{c_l} \quad (a, c_i < l), \]

meaning \((a, c_1, c_2, \ldots, c_l) \in (\mathbb{Z}/l\mathbb{Z})^{1+l} \). If \((a, c_1, c_2, \ldots, c_l) = 0\), then \( A \) is an \( l \)-th power in \( Q_l(\zeta) \) and therefore

(18.) \[ l \sim \mathfrak{L}_1 \mathfrak{L}_2 \cdots \mathfrak{L}_l \]

is a product of \( l \) distinct prime ideals in \( K(x) = Q(\zeta, x) \). Secondly, if \( a > 0 \) (i.e. if \( a \neq 0 \)), then one may take \( a = 1 \), and it follows that

(18.a) \[ l \sim \mathfrak{L}_1^l. \]

Thirdly, if \( a = 0 \) and if \( c_i \neq 0 \) for some \( i \in [1, l] \), let \( m \) be the smallest integer such that \( c_m \neq 0 \); we may then assume that \( c_m = 1 \). If \( m < l \), choose \( m' \) and \( l' \) such that \( mm' + ll' = 1 \); then

(20.) \[ \Lambda = \lambda^{l'} (1 - x)^{m'}. \]
which is the same as the second Ω in proof of Satz 148 in the Zahlbericht, is a primitive element of $K(x)$ whose norm $n(Λ) = \lambda(1 + \cdots)$ has valuation 1 and therefore, as in the second case ($a = 1$),

\[(22.) \quad I \sim \mathfrak{L}_1.\]

Finally, if $m = l$, then the equation $x^l - \Lambda = 0$ takes the simple form

\[(23.) \quad x^l = 1 - \lambda^l.\]

Hensel puts $\frac{1 - x}{\lambda} = \xi$ (this too can be found in Hilbert), so that the new primitive element $\xi$ satisfies

\[(23.a) \quad f(\xi) = \xi^l - \frac{l_1}{\lambda} \xi^{l-1} + \frac{l_2}{\lambda^2} \xi^{l-2} - \cdots + \frac{l}{\lambda^{l-1}} \xi - 1 = 0.\]

Reducing modulo $\lambda$, and noting that $-l = \lambda^{l-1}(1 + \cdots)$, he gets the congruence

\[(23.b) \quad f(\xi) \equiv \xi^l - \xi - 1 \pmod{I}.\]

Let $\mathfrak{L}_1$ be a prime factor of $I$ in $K(x)$ and $\xi_0$ a root of $f(x) = 0$ in the Bereich of $\mathfrak{L}_1$ (not $\mathfrak{P}_1$, which is a Druckfehler); it follows from (23.b) that

$$\xi_0^l \equiv \xi_0 + 1 \pmod{\mathfrak{L}_1},$$

and therefore, for $i = 1, 2, \ldots, l - 1$,

$$\xi_0^i \equiv \xi_0 + i \pmod{\mathfrak{L}_1}.$$

As the $l$ conjugates $\xi_0, \xi_0^l, \ldots, \xi_0^{l-1}$ of $\xi_0$ are units incongruent modulo $\mathfrak{L}_1$, congruent respectively to $\xi_0, \xi_0 + 1, \ldots, \xi_0 + (l - 1)$, the relative degree of $\mathfrak{L}_1$ is $l$, and therefore

\[(24.) \quad I \sim \mathfrak{L}_1.\]

(Note that Artin and Schreier could have drawn the inspiration for their theory from this proof; they were instead inspired by the archimedean prime $\mathbf{R}$, which is equally worthy of our contemplation. Note also that, in giving this local proof of a part of Hilbert’s Satz 148, Hensel missed the opportunity of proving the other part by computing the relative discriminant and the ring of integers, even though he had the uniformisers $\sqrt[\lambda]{\lambda}$ and (20.) in the two ramified cases $a = 1$, resp. $a = 0$, $m < l$. Finally,
by taking \( l \neq 2 \), he cannot connect the unramified case \( m = l \), when \( l = 2 \), with his earlier result (th. 6) on local discriminants.

In the second paper ([27]), although the formulation of the theorem is still global, the above local proof is carried over (pp. 207–8) to the case of any finite extension \( K \) of \( \mathbb{Q}(\zeta) \) and \( l \mid l \) a prime of \( K \) of residual degree \( f \). Hensel notes that \( K(l) \) contains (cf. prop. 24) the number

\[
\Lambda = l^{-1\sqrt{-l}}.
\]

As he shows in [28], (cf. prop. 30 and 33, or prop. 42), one is reduced to considering the equation \( x^f = 1 - \xi_0 \Lambda^l \), with \( \xi_0 \) a unit of \( K(l) \) whose trace

\[
s_0 = \xi_0 + \xi_0^l + \xi_0^{l^2} + \cdots + \xi_0^{l^{f-1}}
\]

is not divisible by \( l \) and hence congruent to one of \( 1, 2, \ldots, l-1 \) (mod \( l \)). (The meaning of \( \xi_0 \) is different in the two papers.) Then the \( l \) conjugates

\[
(9) \quad \xi, \xi^{lf}, \xi^{2lf}, \ldots, \xi^{l(l-1)f}
\]

of the new primitive element \( \xi = \frac{1-x}{\Lambda} \) are units incongruent modulo \( \mathfrak{L} \), where \( \mathfrak{L} \) is a prime divisor of \( l \) in \( K(x) \). Indeed, dividing

\[
(\xi \Lambda - 1)^l = \xi^l \Lambda^l - l_1 \xi^{l-1} \Lambda^{l-1} + l_2 \xi^{l-2} \Lambda^{l-2} - \cdots + l \xi \Lambda - 1 = \xi_0 \Lambda^l - 1
\]

throughout by \( \Lambda^l \) and recalling that \( \Lambda^{l-1} = -l \), he gets the equation

\[
(12.\text{a}) \quad f(\xi) = \xi^l - \frac{l \xi^{l-1}}{\Lambda} + \frac{l^2}{\Lambda^2} \xi^{l-2} - \cdots - \xi - \xi_0 = 0.
\]

Reducing modulo \( \mathfrak{L} \) and noting that the coefficients of \( \xi^{l-1}, \xi^{l-2}, \ldots, \xi^2 \) are divisible by \( \Lambda \) and hence by \( \mathfrak{L} \), he gets the congruence

\[
(12.\text{b}) \quad \xi^l \equiv \xi + \xi_0 \pmod{\mathfrak{L}}.
\]

Successively raising this to the exponent \( l \), he gets a series of congruences

\[
\xi^{l^2} \equiv \xi + \xi_0 + \xi_0^l \\
\xi^{l^3} \equiv \xi + \xi_0 + \xi_0^l + \xi_0^{l^2} \\
\xi^{l^f} \equiv \xi + \xi_0 + \xi_0^l + \cdots + \xi_0^{l^{f-1}} \equiv \xi + s_0.
\]
This implies that the $l$ powers (9) are congruent modulo $\mathcal{L}$ respectively to

$$\xi, \xi + s_0, \xi + 2s_0, \ldots, \xi + (l - 1)s_0,$$

(not to $\xi, \xi + \xi_0, \xi + 2\xi_0, \ldots, \xi + (l - 1)\xi_0$, as in the original). In other words, the $l$ powers (9) are distinct modulo $\mathcal{L}$. Hence the relative discriminant is not divisible by $l$, because the $l$ roots $\xi + is_0$ (the original has $\xi + i\xi_0$), $i \in [0, l[$, are distinct modulo $\mathcal{L}$.

This is Hensel’s local proof of Furtwängler’s Satz 4 (= Hecke’s Satz 119); of course, he also had a local proof of Satz 3 (resp. 118), which treats the easier case $l \neq p$. Curiously, Hensel does not cite Furtwängler; it is left to Hasse to do so in his review in the Jahrbuch [JFM 48.1170.01]. Equally curiously, Hasse [20, Satz 9] refers to Hecke for the theorem and its proof, not to Furtwängler and Hensel.

***

**Eisenstein (1850).** The roots of Hensel’s paper [26] can be traced more than 70 years back to Eisenstein’s seminal work [14] on the $\lambda$-adic reciprocity law for a prime number $\lambda \neq 2$. He takes a primitive $\lambda$-th root $\zeta$ of 1 and sets $\eta = 1 - \zeta$. For two mutually prime “complex integral numbers” $A, B (\in \mathbb{Z}[\zeta])$, he defines a $\lambda$-th root $(A/B)$ of 1, “the $\lambda$-tic character of $A$ modulo $B$”, using Kummer’s ideal prime divisors. (For an ideal prime $b$ other than $\eta\mathbb{Z}[\zeta]$, define $(A/b)$ by the congruence $(A/b) \equiv A^{\frac{N_b-1}{\lambda}} \pmod{b}$, where $N_b = \text{Card}(\mathbb{Z}[\zeta]/b)$ is the norm of $b$; extend the definition to numbers $B$ by multiplicativity). He investigates, when $A$ and $B$ are not divisible by $\eta$, the ratio

$$(\frac{A}{B}) : (\frac{B}{A}) = \zeta^{\varphi(A,B)} \quad (\varphi(A,B) \in \mathbb{Z}/\lambda\mathbb{Z})$$

(which, if $\lambda$ had been 2 and consequently $\zeta = -1$ and $(A/B)$ the quadratic character of $A$ modulo $B$, would have been given by $\varphi(A,B) = \frac{A-1 B-1}{2}$ for $A, B \in \mathbb{Z}$ odd, mutually prime, and positive: “quadratic reciprocity”). First he shows that $A$ (mod. $\eta^{\lambda+1}$) can be taken to be of the form

$$A \equiv g^{\alpha_1}(1 - k_1\eta)^{\alpha_1}(1 - k_2\eta^2)^{\alpha_2} \cdots (1 - k_\lambda\eta^\lambda)^{\alpha_\lambda} \pmod{\eta^{\lambda+1}}$$

where, in our language, a generator $g$ of $\mathbb{F}_\lambda^\times$ and integers $k_i \in \mathbb{Z}[\zeta]$ prime to $\eta$ are fixed, and the exponents $\alpha \in \mathbb{Z}/(\lambda - 1)\mathbb{Z}$, $\alpha_i \in \mathbb{Z}/\lambda\mathbb{Z}$ vary with $A$. He concludes from this that $\varphi(A,B) = \varphi(A',B')$ if $A \equiv A'$ and $B \equiv B'$ (mod. $\eta^{\lambda+1}$) or, what comes to the same, (mod. $\lambda\eta^2$). He remarks that as
far as the $\lambda$-tic character is concerned, we may take $\alpha = 0$ and $k_i = 1$. One is thus reduced to considering the case of relatively prime $A = 1 - \eta^\mu$, $B = 1 - \eta^\nu$ and to the determination of $\varepsilon_{\mu,\nu} = \zeta^{\varphi(1-\eta^\mu,1-\eta^\nu)}$.

Next, he considers $(\eta/A)$, which, by multiplicativity, reduces to the cases $A = 1 - \eta^\mu$; what is most relevant for us is the basic formula

\[(8.) \quad \left( \frac{\eta}{1-\eta^\mu} \right) = \begin{cases} 1 & \text{if } \mu \neq \lambda \\ \zeta & \text{if } \mu = \lambda. \end{cases} \]

It follows that, for $A \equiv (1 - \eta)^{\alpha_1}(1 - \eta^2)^{\alpha_2} \cdots (1 - \eta^\lambda)^{\alpha_\lambda} \pmod{\eta^{\lambda+1}}$, one has more generally

\[(10.) \quad \left( \frac{\eta}{A} \right) = \zeta^{\alpha_\lambda}. \]

This law may be considered as a remote ancestor of our prop. 38, just as Eisenstein’s analysis (mod. $\eta^{\lambda+1}$) may be said to have prefigured Hensel’s equation (16.a). Indeed, Eisenstein sums up the main achievement of his memoir by saying that $\sigma = \lambda + 1$ is the smallest exponent — if smallest exponent there is — such that $\varphi(A, B) = \varphi(A', B')$ whenever $A, B \equiv A', B' \pmod{\eta^\sigma}$.

Local arithmetic makes it possible for us not only to understand all this wizardry but also sozusagen to anticipate it.

---

It is amusing to note that the shortest path between the global results of Stickelberger (th. 1 and 2) on the one hand, and of Hilbert (th. 56 and 58) and Furtwängler (Hecke’s th. 53 and 54) on the other, passes through purely local results (th. 5 and 6, prop. 15 and 16): the statements are different globally, but they are the same locally.

$l^n$-primary numbers. — In a finite extension $K$ of $\mathbb{Q}_l$ containing a primitive $l^n$-th root of 1, an element $\alpha \in K^\times$ is called $l^n$-primary if the extension $K(\sqrt[l^n]{\alpha})|K$ is unramified. These numbers have been characterised by Hasse (1936) using the theory of Witt vectors, and also by Shafarevich (1950) in his work on the general reciprocity law; see [15, VI, §4] for a comprehensive presentation.
VII. The valuation of the discriminant

Let $p$, $l$ be prime numbers and let $K$ be a finite extension of $\mathbb{Q}_p$. Unless otherwise stated (as in prop. 63), we assume that $K^\times$ has an element $\zeta$ of order $l$. Denote by $k$ the residue field of $K$. For any extension $F$ of $\mathbb{Q}_p$, we denote by $v_F$ the normalised valuation of $F$, so that $v_F(\pi) = 1$ if $\pi$ is a generator of the maximal ideal of the ring of integers of $F$.

**Proposition 59.** — Suppose that $p \neq l$. Let $D \neq k^\times / k^\times l$ be an $F_l$-line in $K^\times / K^\times l$ and let $L = K(\sqrt[l]{D})$ be the (ramified) degree-$l$ cyclic extension of $K$ corresponding to $D$. Then $v_K(d_{L|K}) = l - 1$.

**Proof:** This is clear since $L|K$ is a totally ramified extension of degree $l$ prime to $p$ (tame ramification). What is needed is not so much that $l$ be prime, but that it be prime to $p$. Cf. footnote to th. 10.

Hasse uses Hilbert’s theory of higher ramification groups ([31], [32, p. 140]), to compute the valuation of the discriminant in the case $l = p$. (To be consistent with Hilbert, Hecke and Hasse, we denote the prime $p = l$ by $l$, not by $p$). Let $L|K$ be a finite galoisian extension and $G = \text{Gal}(L|K)$, where $K$ is any finite extension of $\mathbb{Q}_l$. The ring of integers $\mathfrak{o}_L$ of $L$ and its maximal ideal $\mathfrak{m}_L$ are stable under the action of $G$; there is thus an induced action on $\mathfrak{o}_L/\mathfrak{m}_L^{n+1}$ for every integer $n \in [-1, +\infty[$.

Define $G_n$ to be the subgroup consisting of those $\sigma \in G$ which act trivially on $\mathfrak{o}_L/\mathfrak{m}_L^{n+1}$; we have $G_{-1} = G$, and $G_0$ is the inertia subgroup : the extension $L_0 = L^{G_0}$ is unramified over $K$, whereas $L$ is totally ramified over $L_0$. Also, $G_1$ is the (unique) maximal sub-$l$-group of $G_0$ : the extension $L_1 = L^{G_1}$ of $L_0$ is (totally but) tamely ramified (and hence cyclic of degree dividing $q - 1$, where $q = \text{Card } \mathfrak{o}_L/\mathfrak{m}_L$), whereas $L$ is a (totally ramified) $l$-extension of $L_1$. The decreasing filtration $(G_n)_{n \in [-1, +\infty[}$ is exhaustive and separated. The valuation of the different of $L|K$ is given by

\begin{equation}
(10) \quad v_L(D_{L|K}) = \sum_{n \in [0, +\infty[} (\text{Card } G_n - 1),
\end{equation}

which also equals $v_K(d_{L|K})$ when $L|K$ is totally ramified. This filtration in the lower numbering is compatible with the passage to a subgroup, but not with the passage to a quotient.

The problem of computing the ramification filtration on a quotient of $G$ was first solved by Herbrand [29] ; one needs to convert the filtration $(G_n)_{n \in [-1, +\infty[}$ to the upper numbering $(G^t)_{t \in [-1, +\infty[}$, defined for any real $t$, and then take the quotient. See [46, ch. IV] for the details, where the upper-numbering filtration on $\text{Gal}(\mathbb{Q}_l(\zeta_{l^n}) | \mathbb{Q}_l) = (\mathbb{Z}/l^n\mathbb{Z})^\times$ is also shown,
using prop. 23, to be the quotient of the natural filtration of \( \mathbb{Z}_l^\times \) by units of various levels.

Let us now revert to a \( K \) which contains a primitive \( l \)-th root of 1 and denote by \( e = (l - 1)e_1 \) the ramification index of \( K \) over \( Q_l \).

**Proposition 60.** — For an \( F_l \)-line \( D \neq \bar{U}_{e_1} \) in \( K^\times/K^{\times l} \), let \( L = K(\sqrt[l]{D}) \) be the (ramified) degree-\( l \) cyclic extension of \( K \) corresponding to \( D \). Let \( m \) be the integer such that \( D \subset \bar{U}_m \) but \( D \not\subset \bar{U}_{m+1} \), with the convention that \( \bar{U}_0 = K^\times/K^{\times l} \). Then \( v_K(d_{L|K}) = (l - 1)(1 + e_1 - m) \).

*Proof:* Suppose first that \( m = 0 \). Then \( D \) is generated by the class modulo \( K^{\times l} \) of some uniformiser \( \lambda \) of \( K \), and \( L \) is defined by \( g = T^l - \lambda \), which is Eisenstein. As \( g' = lT^{l-1} \), the exponent of the different \( D_{L|K} \) is \( v_l(l) + (l - 1) = le_1 - 1 = (l - 1)(1 + e_1) \), and, as \( L|K \) is totally ramified, this is also the valuation \( v_K(d_{L|K}) \) of the discriminant \( d_{L|K} \).

Suppose next that \( m > 0 \); then \( m < le_1 \) (because \( D \neq \bar{U}_{e_1} \)) and \( m \) is prime to \( l \) (prop. 42). Let \( (G_i)_{i\in[-1,+\infty]} \) be the ramification filtration; we have \( G = G_{-1} = G_0 = G_1 = \cdots = G_t \) but \( G_{t+1} = \{\text{Id}_L\} \) for some integer \( t \) which is strictly positive because \( L|K \) is wildly ramified. As \( v_K(d_{L|K}) = (l - 1)(1 + t) \) (cf. [46, prop. IV.4]), it is enough to show that \( t = le_1 - m \).

The line \( D \) is generated by the class modulo \( K^{\times l} \) of some unit \( \mu \) of \( K \) and there is a unit \( \xi \) such that \( v_K(\xi^l - \mu) = m \) (prop. 45). Fix a root \( \sqrt[l]{\mu} \) of \( T^l - \mu \) in \( L \). As \( N_{L|K}(\xi - \sqrt[l]{\mu}) = \xi^l - \mu \) and as \( L|K \) is totally ramified, we also have \( v_L(\xi - \sqrt[l]{\mu}) = m \).

Let \( x, y \in \mathbb{Z} \) be such that \( mx + ly = 1 \); the element \( \Lambda = (\xi - \sqrt[l]{\mu})^y \lambda^y \) is then a uniformiser of \( L \) for any fixed but arbitrary uniformiser \( \lambda \) of \( K \). Taking a generator \( \sigma \in G \) and writing \( \sigma(\sqrt[l]{\mu}) = \zeta \cdot \sqrt[l]{\mu} \) for some order-\( l \) element \( \zeta \) of \( K^\times \), we have

\[
\sigma(\Lambda) = \left( \frac{\xi - \zeta \sqrt[l]{\mu}}{\xi - \sqrt[l]{\mu}} \right)^x = \left( 1 + \frac{(1 - \zeta) \sqrt[l]{\mu}}{\xi - \sqrt[l]{\mu}} \right)^x = (1 + \alpha)^x,
\]

defining \( \alpha \). Hence \( \sigma(\Lambda)/\Lambda \equiv 1 + x\alpha \mod \Lambda^{le_1 - m+1} \). As \( v_L(\alpha) = le_1 - m \), and as \( x \) is prime to \( l \), this means that \( \sigma \in G_{le_1 - m} \) but \( \sigma \notin G_{le_1 - m+1} \), and hence \( t = le_1 - m \), as desired (cf. [20, p. 266]).

Notice that when \( m = 0 \), our direct computation of \( v_K(d_{L|K}) \) in this case shows that \( t = le_1 \). Thus, \( t + m = le_1 \) for all ramified degree-\( l \) kummerian extensions.

(This allows one to compute the valuation of the discriminant of \( Q_l(\zeta_n) \mid Q_l \) by induction, without invoking the fact that the ramification filtration is a quotient of the filtration on \( \mathbb{Z}_l^\times \) by units of various levels.)
Corollary 61. — For an $F_l$-line $D \subset K^\times/K^\times l$, let $L = K(\sqrt[l]{D})$ and let $\mathcal{O}_L$ be the ring of integers of $L$. If $D \not\subset \bar{U}_1$, then there is a uniformiser $\mu$ such that $\bar{\mu} \in D$; in this case, $\sqrt{\bar{\mu}}$ is a uniformiser of $L$ and $\mathcal{O}_L = \mathcal{O}[\sqrt{\bar{\mu}}]$. Suppose next that $D \subset \bar{U}_1$ and let $\mu \in \mathcal{O}_1^\times$ be a unit such that $\bar{\mu}$ generates $D$. If there is an $m < le_1$ such that $\bar{\mu} \in \bar{U}_m$ but $\bar{\mu} \not\in \bar{U}_{m+1}$, then $m$ is prime to $l$; for any $x, y \in \mathbb{Z}$ such that $mx + ly = 1$, the element $\Lambda = (\xi - \sqrt[l]{\bar{\mu}})^x \lambda^y$ is a uniformiser of $L$ and $\mathcal{O}_L = \mathcal{O}[\Lambda]$. Finally, if $D = \bar{U}_{le_1}$, then $\lambda$ remains a uniformiser of $L$, the class of $\mu = 1 - \eta(1 - \zeta)$ generates $D$ for any $\eta \in \mathfrak{o}$ whose image generates $k/\varphi(k)$, and $\mathcal{O}_L = \mathcal{O}[(\sqrt[l]{\bar{\mu}} - 1)/(1 - \zeta)]$.

Only the last part (the one about $\bar{U}_{le_1}$) does not follow from the proof of the previous prop.; this part was already dealt with in cor. 37.

Corollary 62. — Let $K$ be a finite extension of $\mathbb{Q}_l(\zeta)$, $L$ a degree-$l$ cyclic extension of $K$, $(G_i)_{i \in [-1, +\infty]}$ the ramification filtration of $G = \text{Gal}(L/K)$, $t$ the integer such that $G_t = G$, $G_{t+1} = \{\text{Id}_L\}$. Then $t = -1$ if $L|K$ is unramified; otherwise $t \in [1, le_1]$ and $t$ is prime to $l$, unless $t = le_1$. Each such $t$ occurs for some $L$; $t = le_1$ occurs only when $L$ is the splitting field of $T^l - \lambda$ for some uniformiser $\lambda$ of $K$.

This is clear if $L|K$ is unramified, for then the inertia subgroup $G_0$ is trivial. Otherwise, let $D = \text{Ker}(K^\times/K^\times l \to L^\times/L^\times l)$ be the $F_l$-line in $\bar{U}_0 = K^\times/K^\times l$ which corresponds to $L$; we have $D \neq \bar{U}_{le_1}$ (prop. 16). Let $m$ be the integer such that $D \subset \bar{U}_m$ but $D \not\subset \bar{U}_{m+1}$; we have $m < le_1$ and $m$ is prime to $l$ (prop. 42) unless $m = 0$, which can happen only when $D$ is generated by the image of some uniformiser of $K$. As $m + t = le_1$ (prop. 60), the statement follows.

Hasse [20, p. 251] first proves that in the ramified case $t \in [1, le_1]$ is prime to $l$ unless $t = le_1$ and uses it to conclude from the equality $m + t = le_1$ ([20, p. 266]) that $m \in [0, le_1]$ is prime to $l$ unless $m = 0$, a fact which we had seen directly in prop. 42. Indeed, cor. 62 can be used to recover [20, p. 251], which specifies the break in the ramification filtration of a $(\mathbb{Z}/l\mathbb{Z})$-extensions $L|K$, and the possibilities for $v_K(d_{L|K})$, even when the finite extension $K$ of $\mathbb{Q}_l$ does not contain an element of order $l$:

Proposition 63. — Suppose that $K^\times$ does not contain an element of order $l$, let $L|K$ be a degree-$l$ cyclic extension, $G = \text{Gal}(L|K)$, and $t$ the integer such that $G_t = G$ but $G_{t+1} = \{\text{Id}_L\}$. Then $t = -1$ if $L|K$ is unramified; otherwise $t \in [1, le_1]$ and $t$ is prime to $l$.

Clearly $t = -1$ if the extension $L|K$ is unramified, so assume that it is (totally) ramified. Let’s first give two proofs of the fact that $t \in [1, le_1]$ and that $t$ is prime to $l$ if $t \neq le_1$; then we will show that $t \neq le_1$. 

46
Put $K' = K(\zeta)$ (where $\zeta^l = 1$ but $\zeta \neq 1$) and $L' = LK'$. The degree of the extension $K'|K$, and a fortiori the relative ramification index $s$, divide the degree $l - 1$ (cf. prop. 23) of the extension $Q_l(\zeta)|Q_l$. The extension $L'|K'$ is a totally ramified kummerian extension of degree $l$. Denoting by $t'$ the break in the ramification filtration of $\text{Gal}(L'|K')$, it is sufficient, by cor. 62, to show that $t' = st$. (Note that the absolute ramification index of $K'$ is $s(l - 1)e_1$, where $(l - 1)e_1$ is the absolute ramification index of $K$; the number $e_1$ need not be an integer, cf. prop. 25.)

Now, $L'|L$ is a tamely ramified extension whose relative ramification index is also $s$; choose a uniformiser $\varpi$ of $L'$ such that $\varpi^s$ is a uniformiser of $L$. Also, the restriction map $\text{Gal}(L'|K') \to \text{Gal}(L|K)$ is an isomorphism; choose a generator $\sigma$ of these groups. By the definition of $t$,

$$s(t + 1) = s\nu_L(\sigma(\varpi^s) - \varpi^s) = \nu_{L'}(\sigma(\varpi)^s - \varpi^s).$$

Let $\xi$ be an element of order $s$ in $Q_i^\times$ (recall that $s$ divides $l - 1$) and write

$$\sigma(\varpi)^s - \varpi^s = (\sigma(\varpi) - \varpi)(\sigma(\varpi) - \xi \varpi)\ldots(\sigma(\varpi) - \xi^{s-1} \varpi).$$

By the definition of $t'$, the $L'$-valuation of the first factor is $t' + 1$; let us show that it is 1 for the other $s - 1$ factors. For $0 < i < s$, the element $1 - \xi^i$ is a unit of $L'$; writing $\sigma(\varpi) - \xi^i \varpi = (\sigma(\varpi) - \varpi) + (1 - \xi^i) \varpi$ and noting that $\nu_{L'}(\sigma(\varpi) - \varpi) = t' + 1 > 1$ because $t' > 0$ (cor. 62), we have $\nu_{L'}(\sigma(\varpi) - \xi^i \varpi) = 1$. Therefore $\nu_{L'}(\sigma(\varpi)^s - \varpi^s) = (t' + 1) + (s - 1) = t' + s$, and thus

$$s(t + 1) = \nu_{L'}(\sigma(\varpi)^s - \varpi^s) = t' + s.$$

Hence $t' = st$, as desired. Cf. [7, p. 127].

(Notice, before moving on, that the claim about $K'|K$ being totally ramified made in [7, p. 127] is not correct when $p \neq 2$. Take, for example, $K = \mathbb{Q}_p(\sqrt[p-1]{\alpha})$, which is totally ramified of degree $p - 1$ and admits $\pi = \sqrt[p-1]{\alpha}$ as a uniformiser. Writing $-p = \varepsilon \pi^{p-1}$, we deduce $\varepsilon = -1$; in particular $\varepsilon \notin \mathbb{F}_p^{\times(p-1)}$, therefore $\zeta \notin K$ (prop. 25). On the other hand, the extension $K(\sqrt[p-1]{\alpha})$ is unramified over $K$ and contains $\zeta$, for it contains $\sqrt[p-1]{\alpha}$ (prop. 24). Therefore $K' = K(\zeta)$ is unramified over $K$; as the degree of $K'|K$ is $p > 1$, it cannot be totally ramified. More generally, if the ramification index of a finite extension $K|\mathbb{Q}_p$ is a multiple of the ramification index $p - 1$ of $\mathbb{Q}_p(\zeta)|\mathbb{Q}_p$, then $K(\zeta)|K$ is unramified, as follows from Abhyankar’s lemma [39, p. 236].)

Remark that, with the above notation, the equality $t' = st$ can also be derived by computing the different $\mathfrak{D}_{L'|K}$ in two different ways by
transitivity in the square

\[
\begin{array}{c}
\xymatrix{
L \ar[r]^{s-1} & L' \\
K \ar[r]_s & K'
\}
\end{array}
\]

\[(l-1)(1+t) \ar[u] \quad l \ar[u] \quad (l-1)(1+t') \ar[u]
\]

in which the internal letters indicate the relative ramification index and the external expressions the valuation of the different of the extension in question. Using the tower of extensions \(L'|L|K\), we get

\[v_{L'}(D_{L'|K}) = v_{L'}(D_{L'|L}) + s.v_L(D_{L|K}) = (s-1) + s.(1-l)(1+t)
\]

whereas using the tower \(L'|K'|K\), we get

\[v_{L'}(D_{L'|K}) = v_{L'}(D_{L'|K'}) + l.v_{K'}(D_{K'|K}) = (1-l)(1+t') + l.(s-1).
\]

Comparing the two expressions, we deduce \(t' = st\), as claimed. The hypothesis \(lK = \{1\}\) has not been used so far.

Let us show finally that if \(L|K\) is a degree-\(l\) cyclic extension whose ramification break occurs at \(le_1\), then \(K^\times\) has an element of order \(l\) (and therefore \(L|K\) is kummerian). Let \(\lambda\) (resp. \(\Lambda\)) be a uniformiser of \(K\) (resp. \(L\)); \(\Lambda'/\lambda\) is a unit of \(L\). By assumption, for any generator \(\sigma \in \text{Gal}(L|K)\), we have

\[
\frac{\sigma(\Lambda)}{\Lambda} \equiv 1 + \theta\lambda^{e_1} \pmod{\Lambda^{le_1+1}}
\]

for some \(\theta \in k^\times\) invertible in the common residue field \(k\) of \(K\) and \(L\). Applying \(N_{L|K}\), we get \(1 \equiv (1 + \theta\lambda^{e_1})^l \pmod{\Lambda^{le_1+1}}\), which we take to mean that the map \((\ )^l : U_{e_1}/U_{e_1+1} \to U_{le_1}/U_{le_1+1}\) is not injective. This is possible only if \(K^\times\) has an element of order \(l\) (prop. 29). Cf. [15, p. 75].

(Note in passing that a finite extension \(K\) of \(Q_l\) \((l\) being an odd prime) may very well not contain a primitive \(l\)-th root of \(1\) and still admit ramified \((Z/lZ)\)-extensions, contrary to the inadvertent exercise 30 in [8, p. 280]. The simplest example would be the unique degree-\(l\) extension \(L\) of \(K = Q_l\) contained in \(M = Q_l(\sqrt[l]{\zeta})\), where \(\zeta^l = 1\) but \(\zeta \neq 1\). Recall that \(M|Q_l\) is totally ramified galoisian with \(\text{Gal}(M|Q_l) = (Z/l^2Z)^\times\) (cf. prop. 23), a group which has a unique order-\(l\) quotient (prop. 34). Another aside : for every ramified \((Z/lZ)\)-extension of \(Q_l\) \((l \neq 2)\), the break in the
ramification filtration occurs at $t = 1$, because $le_1 < 2$. Consequently, for every $(\mathbb{Z}/l\mathbb{Z})$-extension of $K' = Q_l(\zeta)$ which comes from a $(\mathbb{Z}/l\mathbb{Z})$-extension of $K = Q_l$ (such as $M/K'$; indeed $M = LK'$), the ramification break occurs at $l - 1$ (and hence $\bar{\zeta} \not\in \bar{U}_2$). However, $Q_2$ has two quadratic extensions with $t = 1$ and four with $t = 2$, because there are two $\mathbb{F}_2$-lines (generated respectively by $-1$ and $-u$, where $u = 1 + 2^2$) in $Q^2_2/Q^{2}_2$ of “level” $m = 1$ and four lines with $m = 0$; the remaining line $\{1, u\}$ is of level $m = 2 = 2e_1$ and gives the unramified quadratic extension, for which of course $t = -1$.

**Corollary 64.** — As $L$ runs through the degree-$l$ cyclic extensions of $K$, the possibilities for $v_K(d_{L|K})$ are $0$, $(l - 1)(1 + t)$ (for $0 < t < le_1$ prime to $l$) and $(l - 1)(1 + le_1)$.

Let us note finally that the number of degree-$l$ kummerian extensions of $K$ (when $K^\times$ has an element of order $l$) which have a given ramification break $t$ (equivalently, a given valuation of the discriminant or a given “level” $m$) can be determined using cor. 43. For every positive integer $n$, denote by

$$\delta_l(n) = \frac{l^{1+n} - 1}{l - 1} = 1 + l + l^2 + \cdots + l^n$$

the number of lines in the vector $\mathbb{F}_l$-space of dimension $1 + n$; equivalently, $\delta_l(n)$ is the number of points in $P_n(\mathbb{F}_l)$. According to our current convention, $\bar{U}_0 = K^\times/K^\times l$, a vector space of dimension $2 + d$. Also, $\bar{U}_1$ is of dimension $1 + d$, so the number of $\mathbb{F}_l$-points of $P(\bar{U}_0)$ which are not in $P(\bar{U}_1)$ is $\delta_l(1 + d) - \delta_l(d)$. Thus $\delta_l(1 + d) - \delta_l(d) = l^{1+d}$ is the number of degree-$l$ cyclic extension of $K$ whose ramification break occurs at $le_1$, or, equivalently, the normalised valuation of whose discriminant is $(l - 1)(1 + le_1)$. For example, $Q_l(\zeta)$ has $l^1$ extensions whose ramification break occurs at $l$. In other words, there are $l^1$ extensions of $Q_l(\zeta)$ the valuation of whose discriminant is $l^2 - 1$, where the valuation of $1 - \zeta$ is $1$.

Let us come to the other possibilities for the ramification break (cor. 62). Define

$$\mu(t) = \left( t - \left[ \frac{t}{l} \right] \right) f \quad (t \in [0, le_1[), \quad \mu(le_1) = 1 + d.$$  

We have seen (cor. 43) that $\mu(t)$ is the $\mathbb{F}_l$-dimension of the projective space $P(\bar{U}_m)$, with $m = le_1 - t$ and $\bar{U}_0 = K^\times/K^\times l$, for every $t \in [0, le_1[.$

For $t \in [1, le_1[,$ the number of degree-$l$ cyclic extensions of $K$ having a ramification break at $t$ is the number of $\mathbb{F}_l$-points in $P(\bar{U}_m)$ ($m = le_1 - t$) which are not in $P(\bar{U}_{m+1})$; this number equals $\delta_l(\mu(t)) - \delta_l(\mu(t - 1))$. Notice that $\mu(le_1 - 1) = d$, so the number of degree-$l$ cyclic extensions
of $K$ whose ramification break occurs at $le_1$ can also be written as $\delta_t(\mu(\mu(l))) - \delta_t(\mu(\mu(l)-1))$. When $t=1$, the number of extensions is

$$\delta_l(\mu(1)) - \delta_l(\mu(0)) = \delta_l(f) - \delta_l(0) = \delta_l(f) - 1 = l + l^2 + \cdots + l^f.$$ 

For example, $Q_l(\zeta)$ has exactly $l^t$ degree-$l$ cyclic extensions whose ramification break occurs at $t$, for every $t \in [1, l]$.

In general, we have proved

**COROLLARY 65.** — Suppose that $K^\times$ has an element of order $l$. For $t \in [1, le_1]$, the number of degree-$l$ kummerian extensions of $K$ whose ramification break occurs at $t$ is $\delta_l(\mu(t)) - \delta_l(\mu(t-1))$; this number vanishes when $t$ is a multiple of $l$, except when $t = le_1$.

More concretely, write $l + l^2 + \cdots + l^d = n_1 + n_2 + \cdots + n_e$, where $n_1$ is the sum of the first $f$ terms on the left, $n_2$ the sum of the next $f$ terms, ..., $n_e$ the sum of the last $f$ terms. There are exactly $e$ numbers $1 = t_1 < t_2 < \cdots < t_e = le_1 - 1$ in $[1, le_1]$ which are prime to $l$; also put $t_{e+1} = le_1$ and $n_{e+1} = l^{1+d}$. We have seen (cor. 62) that the ramification break of a degree-$l$ cyclic extension $L|K$ occurs at (precisely) one of $-1$, $t_1$, ..., $t_e$, $t_{e+1}$. Cor. 65 says that the number of degree-$l$ cyclic extensions $L|K$ having these breaks is respectively $1$, $n_1$, ..., $n_e$, $n_{e+1}$.

Let us rewrite the number of (totally) ramified degree-$l$ cyclic extensions of $K$. The number in question is the sum over the number of degree-$l$ cyclic extensions whose ramification break occurs at $t_1$, ..., $t_e$, $t_{e+1}$ respectively, as indicated:

$$n_1 + \cdots + n_{e+1} + l + l^2 + \cdots + l^d + l^{1+d} = \delta_l(1 + d) - 1.$$

**COROLLARY 66.** — Suppose that $K^\times$ has an element of order $l$. The number of degree-$l$ kummerian extensions $L|K$ with $v_\K(d_{L|K}) = (l-1)(1 + t_i)$ is $n_i = p^{(i-1)f+1} + \cdots + p^if$ for $i \in [1, e]$ but $n_{e+1} = l^{1+d}$ for $i = e + 1$.

This allows us to compute the contribution of degree-$l$ kummerian extensions to the degree-$l$ “mass formula” of Serre. Recall that this formula states that

$$\sum_L \frac{1}{l^{c(L)f}} = l,$$

where $L$ runs through all (totally) ramified degree-$l$ extensions of $K$ and $c(L) = v_\K(d_{L|K}) - (l-1)$ [47]. On the other hand, cor. 65 allows us
(when $\zeta \in K$) to compute the contribution to this sum coming from kummerian $L|K$. If the ramification break occurs at $t_i$ ($i \in [1, e + 1]$), then $c(L) = (l - 1)t_i$, and the number of such extensions is $n_i$. Thus

$$\sum_{i \in [1, e + 1]} \frac{n_i}{l^{(l-1)t_i}}$$

is the contribution of degree-$l$ kummerian extensions to Serre’s degree-$l$ mass formula. This gives the proportion of ramified degree-$l$ extensions which are kummerian.

When $l = 2$, we are dealing with quadratic extensions, which are all kummerian, so the sum (11) must equal 2. This can be verified directly:

**Lemma 67.** — Let $e > 0$ and $f > 0$ be integers. We have the identity

$$2 + 2^2 + \cdots + 2^f = \frac{2^{(e-1)f+1} + 2^{(e-1)f+2} + \cdots + 2^{ef}}{2^{(2e-1)f}} + \frac{2^{1+ef}}{2^{2ef}} = 2.$$  

For $i \in [1, e]$, the numerator of the $i$-th term on the left-hand side is

$$2^{(i-1)f+1} + 2^{(i-1)f+2} + \cdots + 2^{if} = 2^{(i-1)f}(2^2 + \cdots + 2^f) = 2^{(i-1)f+1}(2^f - 1),$$

so the $i$-th term is $2(2^f - 1)/2^{if}$. Thus the sum of the first $e$ terms is

$$2(2^f - 1) \left( \frac{1}{2^f} + \frac{1}{2^{2f}} + \cdots + \frac{1}{2^{ef}} \right) = \frac{2^{ef} - 1}{2^{ef-1}}$$

$$= 2 - \frac{1}{2^{ef-1}},$$

which, when added to the $(e + 1)$-th term, gives 2, proving the statement.

**Final remark.** The perceptive reader must have noticed that the problem of computing the relative discriminant of a finite extension $L|K$ of number fields has been reduced to the computation of the relative discriminant of a local kummerian extension of degree equal to the residual characteristic, and that prop. 60 and prop. 45 solve this local problem. Let us briefly indicate the argument for reducing the global problem to the local problem, and the local problem to the prime-degree kummerian case.

The relative discriminant $\mathfrak{d}_{L|K}$ is an integral ideal of $K$, so it is determined by the knowledge of the exponents $v_p(\mathfrak{d}_{L|K})$ with which various
primes $p$ of $K$ appear in its prime decomposition. This exponent is a purely local invariant: it is the valuation of the discriminant of the étale $K_p$-algebra $L \otimes_K K_p$. This valuation is the sum of the valuations of the discriminants of the various finite extensions of $K_p$ into which $L \otimes_K K_p$ splits. In other words, it is sufficient to know how to compute the discriminant of an extension of local fields.

So let $L|K$ now be a finite extension of $\mathbb{Q}_p$ ($p$ prime). The first reduction is to the galoisian case: if $M|K$ is a galoisian extension containing $L$, then $M|L$ is also galoisian, and if we know how to compute the different $D_M|K$ and $D_M|L$ of these galoisian extensions, then we can compute $D_L|K$, since $D_M|K = D_M|L \cdot i_M|L(D_L|K)$, of which the Schachtelungssatz (8) is but an avatar, and where $i_M|L$ takes ideals of $L$ to ideals of $M$. We have already used this formula in the more conceptual proof of prop. 63.

So assume now that $L|K$ is galoisian. The next reduction is to the case of a totally ramified $p$-extension. Indeed, there are intermediate extensions $L|L_1|L_0|K$ such that $L_0$ is the maximal unramified extension of $K$ in $L$ and $L_1$ is the maximal tamely ramified extension of $L_0$ in $L$; the extension $L|L_1$ has degree a power of $p$. As we know how to compute the valuations $v_K(d_{L_0}|K) = 0$ and $v_{L_0}(d_{L_1|L_0}) = [L_1 : L_0] - 1$ (prop. 59), it suffices to know how to compute $v_{L_1}(d_{L|L_1})$.

So assume now that $L|K$ is a (finite) $p$-extension, and let $G = \text{Gal}(L|K)$. The $p$-group $G$ admits a finite decreasing sequence of subgroups $(G_n)_n$ (we are not talking about higher ramification groups here) such that $G_{n+1}$ is normal in $G_n$ and each quotient $G_n/G_{n+1}$ is a group of order $p$. We are thus reduced to the case of (cyclic) degree-$p$ extensions.

So assume now that $L|K$ is a cyclic degree-$p$ extension. The valuation of the discriminant $v_K(d_{L|K})$ can be computed if we know the break $t$ in the ramification filtration of $\text{Gal}(L|K)$, which is given by the formula $t' = st$, where $s$ is the ramification index of $K' = K(\zeta)$ ($\zeta^p = 1$, $\zeta \neq 1$) over $K$, and $t'$ is the break in the ramification filtration of the degree-$p$ kummerian extension $L'|K'$, with $L' = LK'$; cf. the proof of prop. 63.

So assume now that $\zeta \in K$ and that $L|K$ is a degree-$p$ cyclic extension; it corresponds to an $\mathbb{F}_p$-line $D \subset K^\times/K^\times p$. As we saw (prop. 16), $L|K$ is unramified ($\text{le cas non ramifié}$) precisely when $D = \mathbb{U}_{p\epsilon_1}$ (where $(p - 1)e_1$ is the absolute ramification index of $K$). In this case $v_K(d_{L|K}) = 0$, of course.

Assume finally that $L|K$ is a ramified kummerian degree-$p$ extension, so it corresponds to a line $D \neq \mathbb{U}_{p\epsilon_1}$, and denote by $m$ the integer such
that $D \subset \tilde{U}_m$ but $D \nsubseteq \tilde{U}_{m+1}$; we have $m \in [0, p e_1]$, and $m$ is prime to $p$ unless $m = 0$. The break in the ramification filtration of $L|K$ occurs at $p e_1 - m$ and therefore $v_K(d_{L|K}) = (p - 1)(1 + p e_1 - m)$ (prop. 60). As for computing the integer $m$, there are two cases. Either $D$ can be generated by the image of a uniformiser, in which case $m = 0$, or it can be generated by the image $\bar{u}$ of a unit, in which case $m$ is the exponent in the highest power $p^m$ of the maximal ideal $\mathfrak{p}$ of the ring of integers $\mathfrak{o}$ of $K$ modulo which $u$ is a $p$-th power: $\hat{u} \in (\mathfrak{o}/\mathfrak{p}^m)\times$ but $\hat{u} \notin (\mathfrak{o}/\mathfrak{p}^{m+1})\times$ (prop. 45).

This solves the problem in the local kummerian case (of degree equal to the residual characteristic), and hence the global problem of determining the relative discriminant of an extension of number fields. Taking the base field to be $\mathbb{Q}$, this also helps decide if a given order in a number field is the maximal order, which happens precisely when the discriminant of the order equals the absolute discriminant of the number field in question.

VIII. Discriminants of elliptic curves over local fields

Let $p$ be a prime number and let $K$ be a finite extension of $\mathbb{Q}_p$. The basic reason why the discriminant $d_{L|K}$ of a finite extension $L|K$ is an element of $K^\times/\mathfrak{o}\times^2$ is that the discriminant $d_B \in K^\times$ of an $\mathfrak{o}$-basis $B$ of $\mathfrak{o}_L$ changes by an element of $\mathfrak{o}\times^2$ if we change $B$ (to another $\mathfrak{o}$-basis of $\mathfrak{o}_L$). Moreover, $\mathfrak{o}$-bases always exist, and any two $\mathfrak{o}$-bases of $\mathfrak{o}_L$ differ by an $\mathfrak{o}$-automorphism of the module $\mathfrak{o}_L$.

Now let $E$ be an elliptic curve over $K$. It can be defined by a minimal weierstrassian cubic $f$, whose discriminant $d_f$ — the result of eliminating the indeterminates $x, y$ from $f, f'_x, f'_y$ — belongs to $K^\times$. If we replace $f$ by another minimal weierstrassian cubic $g$ defining $E$, then $d_f$ gets multiplied by an element of $\mathfrak{o}^{\times 12}$. Moreover, any two minimal weierstrassian cubics defining $E$ can be changed into each other. This suggests the definition of the discriminant of $E$ as the class in $K^\times/\mathfrak{o}^{\times 12}$ of the discriminant of any minimal weierstrassian cubic defining $E$ (def. 68).

More precisely, if $f = y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6 = 0$ is a minimal weierstrassian cubic defining $E$, then, according to [52, p. 180],

$$d_f = -b_2^2 b_8 - 2^3 b_4^3 - 3^3 b_6^2 + 3^2 b_2 b_4 b_6$$

where

$$b_2 = a_1^2 + 2^2 a_2, \quad b_4 = a_1 a_3 + 2 a_4, \quad b_6 = a_3^2 + 2^2 a_6$$

and

$$b_8 = b_2 a_6 - a_1 a_3 a_4 + a_3^2 a_4 - a_1^2.$$
If we replace \( f \) by another minimal Weierstrassian cubic \( g = 0 \), there is change of variables \( x = u^2x' + r, \ y = u^3y' + u^2sx' + t \) with \( u \in \sigma^\times \) and \( r, s, t \in \sigma \). One has \( d_f = u^{12}d_g \) [52, p. 181], which leads to the following definition.

**Definition 68.** — Let \( E \) be an elliptic curve over \( K \). The discriminant \( d_{E|K} \in K^\times/\sigma^{\times 12} \) of \( E \) is the class of the discriminant \( d_f \in K^\times \) of any of the minimal Weierstrassian cubics \( f \) defining \( E \). (4)

If \( E \) has good reduction, then \( d_{E|K} \in \sigma^\times/\sigma^{\times 12} \). We might ask which elements of this finite group occur as \( d_{E|K} \) for some (good-reduction elliptic curve) \( E \) over \( K \). We shall see that they all do; this should be contrasted with th. 6 and prop. 15 which exclude, when \( p = 2 \), certain elements of \( \sigma^\times/\sigma^{\times 2} \) from being discriminants of (unramified) extensions of \( K \).

**Proposition 69.** — Suppose that \( p \neq 2, 3 \) and let \( \delta \in \sigma^\times \). There exists a minimal Weierstrassian cubic \( f \) such that \( d_f = \delta \).

The invariants \( c_4 = b_2^2 - 2^3.3.b_4, \ c_6 = -b_2^3 + 2^2.3^2b_2b_4 - 2^3.3^3.b_6 \), of a Weierstrassian cubic \( f \) satisfy \( c_6^2 - c_4^3 - 2^6.3^3.d_f \). In imitation, consider the cubic \( \Gamma: \eta^2 = \xi^3 - 2^6.3^3.\delta \). Its discriminant is \(-2^4.3^3.(2^6.3^3)^2\delta^2 \), so \( \Gamma \) is an elliptic curve over \( K \); it even has good reduction \( \Gamma \). Let \((\xi, \eta)\) be a point in \( \Gamma(K) \) with \( \xi, \eta \in \sigma \), for example a point whose reduction is \( \neq 0 \) in \( \Gamma(k) \), a group which is not reduced to \( \{0\} \) because it has at least \( q + 1 - 2\sqrt{q} \) points (Hasse) and \( q \) is at least 5. Then the Weierstrassian cubic

\[
y^2 = x^3 - (\xi/2^3.3)x - (\eta/2^5.3^3),
\]

has discriminant \( \delta \) (and \( c_4 = \xi, \ c_6 = \eta \)). It is minimal because its coefficients are in \( \sigma \) and discriminant in \( \sigma^\times \). Cf. [33, p. 76].

**Proposition 70.** — Suppose that \( p = 2 \) or 3 and let \( \delta \in \sigma^\times \). There exists a minimal Weierstrassian cubic \( f \) such that \( d_f = \delta \).

The following proof was suggested by Joseph Oesterlé. Consider the Weierstrassian cubic \( f = y^2 + xy - x^3 - a_6 = 0 \). It has

\[
b_2 = 1, \quad b_4 = 0, \quad b_6 = 4a_6, \quad b_8 = a_6, \quad \text{and} \quad d_f = -a_6 - 2^4.3^3.a_6^2.
\]

(4) It turns out that the global version of this definition, which we also arrived at [9] — the discriminant of an elliptic curve over a number field as an idèle-modulo-twelfth-powers-of-unit-idèles, in perfect analogy with Fröhlich’s definition of the idélic discriminant of an extension of number fields as an idèle-modulo-squares-of-unit-idèles — has already been considered by J. Silverman [48]. He was inspired by the same paper [17] as us, and used it practically for the same purpose — a criterion for the existence of a global minimal Weierstrassian cubic.

54
The last equation can be solved, by Hensel’s lemma, for $a_6$ when $d_f = \delta$, both for $p = 2$ and for $p = 3$. Explicitly, we write

\[ a_6 = -\delta - 2^4 \cdot 3^3 \cdot a_6^2 \]

\[ = -\delta - 2^4 \cdot 3^3 \cdot (-\delta - 2^4 \cdot 3^3 \cdot a_6^2)^2 \]

and so on, which also shows that $a_6$ is a unit and hence $f$ minimal. Thus every unit is the discriminant of some minimal weierstrassian cubic.

**Corollary 71.** — Every element $\delta \in o^\times/o^{\times 12}$ is the discriminant of a (good-reduction) elliptic curve over $K$.

**Corollary 72.** — Let $k$ be a finite field. Every element $\delta \in k^\times/k^{\times 12}$ is the discriminant of an elliptic $k$-curve.

Let $K|\mathbb{Q}_p$ be the unramified extension whose residue field is $k$, denote by $\mathfrak{o}$ its ring of integers, and let $\eta \in \mathfrak{o}^\times/\mathfrak{o}^{\times 12}$ an element whose image is $\delta$. There is a good-reduction elliptic curve $E|K$ whose discriminant is $\eta$; the discriminant of its reduction is $\delta$.

**IX. Starting from** $D \equiv 0, 1 \pmod{4}$

Before coming to the genesis of these notes, let us summarise their main features. First, we have done everything intrinsically, without choosing any bases for the spaces which appear. The invariant language of points and lines and $\mathbb{F}_p$-spaces is also an aid to the imagination; compare, for example, the statement of th. 52 with its translation into our language. Secondly, we have emphasised that questions about discriminants are purely local, and that locally they have analogues for $p$-primary numbers. Thirdly, a central role is played by the exact sequence

\[ 1 \to p\mu \to U_{e_1} / U_{e_1+1} \overset{(\_)^p}{\longrightarrow} U_{pe_1} / U_{pe_1+1} \to \hat{U}_{pe_1} \to 1. \]

which becomes isomorphic, upon choosing a primitive $p$-th root of 1 or a $(p - 1)$-th root of $-p$, to the exact sequence $0 \to \mathbb{F}_p \to k \to k \to \mathbb{F}_p \to 0$ involving $\varphi$; the isomorphism has been made explicit. Finally, we have systematised a certain number of results from the literature, and seen that many of them continue lines of enquiry which can be traced back to the beginning of the 20-th century and even earlier.

This investigation was begun in response to a question by a student (K. Srilakshmi) as to why the absolute discriminant of a number field is $\equiv 0, 1 \pmod{4}$. I told her that it is a purely local matter at the prime 2 and
perhaps Cassels [6] had a proof. He had it indeed; more importantly, he
had a reference to Fröhlich [17] for the idélic notion of the discriminant.
It is the dissatisfaction with the formulation of the absolute version in
Cassels and of the relative version in Fröhlich — after such a beautiful
definition — which led to prop. 15 and, somewhat later, generalising from
the prime 2 to any prime $p$, to prop. 16. The analogue for good-reduction
elliptic curves (cor. 71) was just an amusing afterthought.

At this point, seeking to generalise Fröhlich’s theorem (th. 52) about
rings of integers from dyadic quadratic extensions to kummerian exten-
sions of degree equal to the residual characteristic, we discovered Hecke’s
theorems and, somewhat later, Hilbert’s theorems from the Zahlbericht
which Hecke generalises.

The question arose as to what the generalisation of the other part —
the one about the valuation of the discriminant — of Hilbert’s theorems is.
Luckily we found the key to this question in Hasse’s Klassenkörperbericht
in the form of the relationship between the “level” of a line and the break in
the ramification filtration of the corresponding kummerian extension. By
providing a uniformiser in the ramified case, this relationship determines
the ring of integers (prop. 61) and the ramification break (prop. 62) at one
stroke. The fact that we could recently acquire copies of Hecke [23] and
Hilbert [32], and that Hasse (at least Teil I and Teil Ia [20]) is available
online, was crucial. Very recently we learnt about the local proof by Hensel
and the papers by Furtwängler and Eisenstein. Ironically, the sought-after
uniformiser can be guessed at from the second $\Omega$ in the proof of Satz 148
in the Zahlbericht.

Let it be mentioned that a local version, and a generalisation to all
$p$-primary numbers (for any prime $p$), of Martinet’s congruence on the
absolute norm of the relative discriminant of an extension of number fields
[35] has recently been obtained by S. Pisolkar [42].

Prop. 16 can be taken to mean that the inertia subgroup $G^0$ of
$G = \text{Gal}(M|K)$ — where $M = K(\sqrt[p]{K^\times})$ and $K|Q_p$ is a finite extension
containing a primitive $p$-th root of 1 — which happens to be the same
as the higher ramification subgroup $G^1$, equals $\hat{U}_{pe_1}$ (orthogonal for the
Kummer pairing), $(p - 1)e_1$ being the absolute ramification index of
$K$. The question arose — and we had put it to a student (S. Das) —
as to the orthogonality $G^n = \hat{U}_{pe_1}^\perp (n = [1, pe_1 + 1])$ of the
ramification filtration in the upper numbering on $G$ with respect to the
natural filtration on $\hat{U}_0 = K^\times/K^{\times p}$. The basic idea was that the filtration
on $G$ is uniquely determined by the filtrations on the order-$p$ quotients
of $G$, for which see cor. 62. We have discovered that this orthogonality
relation has recently been established by I. Del Corso and R. Dvornicich

56
[13, p. 286], albeit for somewhat special \( K \), namely those of the form \( K = F(\sqrt[p]{F}) \) for some finite extension \( F \) of \( \mathbb{Q}_p \).

Let us summarise their proof in the general situation where \( K \) is any finite extension of \( \mathbb{Q}_p \) containing a primitive \( p \)-th root of 1.

Think of \( G \) and \( \bar{U}_0 = K \times \mathbb{Q}_p \) as finite-dimensional \( \mathbb{F}_p \)-spaces dual to each other under the pairing

\[ \langle \sigma, \bar{\eta} \rangle = \frac{\sigma(\xi)}{\xi} \ (\xi^p = \eta), \]

where \( \eta \) runs through \( K^\times \), with image \( \bar{\eta} \) in \( K \times /\mathbb{Q}_p \), and \( \xi \in M^\times \) is any \( p \)-th root — it doesn’t matter which — of \( \eta \) (“Kummer theory”; see [4, p. V.84–87]). For every subspace \( H \subset G \), the subspace \( \bar{D} = H^\perp \) of \( \bar{U}_0 \) satisfies

\[ K(\sqrt[p]{D}) = M^H, \quad \text{Gal}(K(\sqrt[p]{D})/K) = G/H. \]

Conversely, for every subspace \( D \subset \bar{U}_0 \), these relations hold with \( H \) the subspace \( D^\perp \subset G \).

Now let \( n > 0 \) be an integer and consider the subspace \( G^n \subset G \). As we know that \( G^1 = \bar{U}_{pe_1}^\perp \) (prop. 16), assume that \( n > 1 \). Let us determine the hyperplanes of \( G \) which contain \( G^n \); clearly \( G^n \subset \bar{U}_{pe_1}^\perp \).

Every hyperplane \( H \neq \bar{U}_{pe_1}^\perp \) is of the form \( H = D^\perp \) for some \( \mathbb{F}_p \)-line \( D \neq \bar{U}_{pe_1} \) in \( \bar{U}_0 \). Let \( m \in [0, pe_1[ \) be the integer such that \( D \subset \bar{U}_m \) but \( D \not\subset \bar{U}_{m+1} \). (As we saw in prop. 42, \( m \) is prime to \( p \) unless \( m = 0 \); this fact plays no role in the present proof). We know that the upper as well as the lower ramification break of \( \text{Gal}(K(\sqrt[p]{D})/K) = G/H \) occurs at \( pe_1 - m \) (cf. cor. 62). In other words, \( (G/H)^{pe_1-m} \neq 0 \) but \( (G/H)^{pe_1+1-m} = 0 \). By the compatibility of the upper-numbering filtration under passage to the quotient (see [46, Chapter IV, Proposition 14], for example), we also have \( (G/H)^n = G^n/(G^n \cap H) \). This implies that \( G^n \subset H \) if and only if \( n > pe_1 - m \) (equivalently, \( m > pe_1 - n \) or still \( D \subset \bar{U}_{pe_1-n+1} \)).

We have seen that for every \( n > 0 \) and every hyperplane \( H = D^\perp \) in \( G \),

\[ G^n \subset H \iff D \subset \bar{U}_{pe_1-n+1}. \]

As \( G^n \) is the intersection of all hyperplanes containing it, \( (G^n)^\perp \) is generated in \( \bar{U}_0 \) by the union of all lines contained in \( \bar{U}_{pe_1-n+1} \). Therefore \( (G^n)^\perp = \bar{U}_{pe_1-n+1} \) (for \( n \in [1, pe_1 + 1] \), with the convention that \( \bar{U}_0 = K^\times /K^\times \)). As claimed. In particular \( G^{pe_1+1} = \{1\} \) and the breaks in the ramification filtration in the upper numbering occur at \( -1 \) (\( M/K \) is not totally ramified), at the \( e \) integers in \( [1, pe_1] \) which are prime to \( p \), and at \( pe_1 \); no break occurs at 0 because \( M/K \) is a \( p \)-extension.
The argument can be carried out for every real \( t \in [-1, +\infty] \) to determine the filtration \((G^t)_{t \in [-1, +\infty]}\) in terms of the filtration \((\bar{U}_m)_{m \in [0, +\infty]}\). Combined with our knowledge of \( \dim_{\mathbb{F}_p} \bar{U}_m \) (cor. 43), this allows one to determine the breaks in the ramification filtration and to compute \( v_K(d_{M|K}) \) by formula (10), which becomes applicable after converting the filtration to the lower numbering.

An interesting application can be made by taking \( K = F(\sqrt[p-1]{F}) \), where \( F \) is any finite extension of \( \mathbb{Q}_p \); note that \( K^\times \) has an element of order \( p \) (cf. prop. 24). Recall that \( F^\times \) has an element of order \( p - 1 \) (cf. prop. 22), and that the \((\mathbb{Z}/(p - 1)\mathbb{Z})\)-module \( F^\times / F^\times(p-1) \) is free of rank 2, containing the free rank-1 submodule \( \mathfrak{o}_F^\times / \mathfrak{o}_F^\times(p-1) \). As the extension \( K_0|F \) obtained by adjoining the \((p-1)\)-th roots of \( \mathfrak{o}_F^\times(p-1) \), we have \( v_F(d_{K|F}) = (p-1)(p-2) \), by the \textit{Schachtelungssatz} (8) and prop. 59. Equivalently, \( v_K(\mathfrak{o}_{K|F}^\times(p-1)) = p-2 \), by an application of prop. 59 or of formula (10) to the filtered group \( \text{Gal}(K|F) : \)

\[
\text{Gal}(K|F)_0 = (\mathfrak{o}_F^\times / \mathfrak{o}_F^\times(p-1))^\perp, \quad \text{Gal}(K|F)_n = \{\text{Id}_L\} \quad (n > 0),
\]

where the orthogonal is taken with respect to the Kummer pairing between \( \text{Gal}(K|F) \) and \( F^\times / F^\times(p-1) \), with values in \( p-1\mu \).

By another application of the \textit{Schachtelungssatz}, one can compute \( v_F(d_{M|F}) \) in terms of \( v_K(d_{M|K}) \), which was computed above. Alternately, one can compute the filtration \( (\text{Gal}(M|F)_n)_{n \in \mathbb{N}} \) from our knowledge of the filtrations \( (\text{Gal}(M|K)_n)_{n \in \mathbb{N}} \) and \( (\text{Gal}(K|F)_n)_{n \in \mathbb{N}} \), and thereby recover the value of \( v_F(d_{M|F}) \) by applying formula (10).

The interest in \( v_F(d_{M|F}) \) comes from the fact that \( M \) is the compositum of all degree-\( p \) extensions of \( F \) [13, p. 273].

Note that the orthogonality relation \( G^n = \bar{U}_{p-1-n+1}^\perp \) is closely related to explicit formulas for the Hilbert symbol, for which see [54].

It is entirely fitting that these ramblings, which were prompted by a question from a student as to why \( D \equiv 0, 1 \pmod{4} \), should close with what was in effect a question to a student, as to whether \( G^n = \bar{U}_{p-1-n+1}^\perp \) \((n \in [1, pe_1])\).

***

\textbf{Acknowledgements.} I am grateful to Joseph Oesterlé for his timely encouragement and advice, to Dipendra Prasad for his interest, to Peter Roquette for his indulgence and his letter, to Victor Abrashkin and Ivan
Fesenko for their emails, to the Göttinger Digitalisierungszentrum and the Cellule Mathdoc in Grenoble for making many of the bibliographic items freely available online, and to the American Mathematical Society for awarding points which can be redeemed for [32] and [23].

I thank the organisers of the 2007 Annual Meeting of the Ramanujan Mathematical Society in Mangalore, Microsoft Research in Bangalore, and the universities of Ratisbon and Heidelberg for their invitations to present some of these results.

Bibliographic References

[1] ANONYME. — Rapport sur l'article 37-08, Papiers secrets des Annales de la Faculté des Sciences de Toulouse, 20 janvier 2009.

[2] ARTIN (E.) and SCHREIER (O.). — Über eine Kennzeichnung der reell abgeschlossenen Körper, Abh. Math. Sem. Hamburg 5, 1927, pp. 225–232.

[3] BERLEKAMP (E.). — An analog[ue] to the discriminant over fields of characteristic two, J. Algebra 38 (1976), no. 2, pp. 325–327.

[4] BOURBAKI (N.). — Algèbre, Chapitres 4 à 7, Masson, Paris, 1981, 422 pp.

[5] BRILL (A.). — Ueber die Discriminante, Math. Annalen, 12, 1877, pp. 87–89.

[6] CASSELS (J.). — Local Fields, Cambridge University Press, 1986, 360 pp.

[7] CHILDS (L.). — Taming wild extensions, American Mathematical Society, 2000. viii+215 pp.

[8] COHEN (H.). — Number theory. Vol. I. Springer, 2007, xxiv+650 pp.

[9] DALAWAT (C.). — Minimal bases, minimal cubics, in preparation.

[10] DALAWAT (C.). — Wilson’s theorem, J. de Théorie de nombres de Bordeaux, 21 (2009) 3, pp. 517–521. Cf. arXiv:0711.3879v1.

[11] DALEN (K.). — On a theorem of Stickelberger, Math. Scand. 3, 1955, pp. 124–126.

[12] DEDEKIND (R.). — Über die Diskriminanten endlicher Körper, Abh. der Königl. Ges. d. Wiss. zu Göttingen, 29 (1882), pp. 1–56.

[13] DEL CORSO (I.) and DVORNICICH (R.). — The compositum of wild extensions of local fields of prime degree, Monatsh. Math. 150 (2007), no. 4, pp. 271–288.

[14] EISENSTEIN (G.). — Über ein einfaches Mittel zur Auffindung der höheren Reciprocitätsgesetze und der mit ihnen zu verbindenen Ergänzungssätze,
15. FESENKO (I.) and VOSTOKOV (S.). — *Local fields and their extensions*, American Mathematical Society, 2002. xii+345 pp.

16. FREI (G.) and ROQUETTE (P.). — *Emil Artin und Helmut Hasse, Die Korrespondenz 1923–1934*, Universitätsverlag Göttingen, 2009, 499 pp.

17. FRÖHLICH (A.). — *Discriminants of algebraic number fields*, Math. Zeitschrift, 74, 1960, pp. 18–28.

18. FURTWÄNGLER (Ph.). — Über die Reziprozitätsgesetze zwischen l-ten Potenzresten in algebraischen Zahlkörpern, wenn l eine ungerade Primzahl bedeutet, Math. Ann. 58, 1903, pp. 1–50.

19. GRAS (G.). — *Class field theory*, Springer, Berlin, 2003, xiv+491 pp.

20. HASSE (H.). — Bericht über neuere Untersuchungen und Probleme aus der Theorie de algebraischen Zahlkörper, Teil Ia, Jahresbericht der Deutschen Mathematiker-Vereinigung, 436, 1927, pp. 233–311.

21. HASSE (H.). — Über das Reziprozitätsgesetz der m-ten Potenzreste, J. f. d. reine und angewandte Math., 158, 1927, pp. 228–259.

22. HASSE (H.). — Zahlentheorie, Akademie-Verlag, Berlin, 1969, 611 pp.

23. HECKE (E.). — Vorlesungen über die Theorie der algebraischen Zahlen, Akad. Verlagsges., Leipzig, 1923, pp. 265.

24. HENSEL (K.). — Über die zu einem algebraischen Körper gehörigen Invarianten, J. f. d. reine und angewandte Math., 129, 1905, pp. 68–85.

25. HENSEL (K.). — Die multiplikative Darstellung der algebraischen Zahlen für den Bereich eines beliebigen Primteilers, J. f. d. reine und angewandte Math., 146, 1916, pp. 189–215.

26. HENSEL (K.). — Über die Zerlegung der Primteiler in relativ zyklischen Körpern, nebst einer Anwendung auf die Kummerschen Körper, J. f. d. reine und angewandte Math., 151, 1921, pp. 112–120.

27. HENSEL (K.). — Die Zerlegung der Primteiler eines beliebigen Zahlkörpers in einem auflösbaren Oberkörper, J. f. d. reine und angewandte Math., 151, 1921, pp. 200–209.

28. HENSEL (K.). — Zur multiplikativen Darstellung der algebraischen Zahlen für den Bereich eines Primteilers, J. f. d. reine und angewandte Math., 151, 1921, pp. 210–212.
et de ramification, J. de math. pures et appl., 10, 1931, pp. 481–498.

[30] Herbrand (J.). — Une propriété du discriminant des corps algébrique, Ann. sci. École Norm. Sup. 49, 1932, pp. 105–112.

[31] Hilbert (D.). — Grundzüge einer Theorie des Galoischen Zahlkörpers, Nachrichten d. Ges. d. Wiss. zu Göttingen, 1894, pp. 224–236. = Ges. Abhandlungen I, pp. 13–23.

[32] Hilbert (D.). — Die Theorie der algebraischen Zahlkörper, Jahresbericht der Deutschen Mathematiker-Vereinigung, 4, 1897, pp. 175–546. = Ges. Abhandlungen I, pp. 63–363.

[33] Kraus (A.). — Quelques remarques à propos des invariants $c_4$, $c_6$ et $\Delta$ d’une courbe elliptique. Acta Arith. 54 (1989), no. 1, pp. 75–80.

[34] Kraus (A.). — Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive, Manuscripta Math. 69 (1990), no. 4, pp. 353–385.

[35] Martinet (J.). — Les discriminants quadratiques et la congruence de Stickelberger, Sém. Théor. Nombres Bordeaux (2) 1 (1989), no. 1, pp. 197–204.

[36] Movahhedi (A.) and Zahidi (M.). — Symboles des restes quadratiques des discriminants dans les extensions modérément ramifiées, Acta Arith. 92, 2000, no. 3, pp. 239–250.

[37] Naipaul (V.). — A way in the world, William Heinemann, London, 1994.

[38] Nakagoshi (N.). — The structure of the multiplicative group of residue classes modulo $p^{N+1}$, Nagoya Math. J. 73 (1979), pp. 41–60.

[39] Narkiewicz (W.). — Elementary and analytic theory of algebraic numbers, 2nd ed., Springer-Verlag, 1990, 746 pp.

[40] Neukirch (J.). — Class Field Theory, Springer-Verlag, Berlin, 1986, 140 pp.

[41] Pellet (A.). — Sur la décomposition d’une fonction entière en facteurs irréductibles suivant un module permier, Comptes Rendus 86, 1878, pp. 1071–1072.

[42] Pisolkar (S.). — Absolute norms of $p$-primary numbers, J. de Théorie de nombres de Bordeaux, 21 (2009) 3, pp. 733–740. Cf. arXiv:0807.1174v1.

[43] Roquette (P.). — Letter to the author, 8 July 2007.

[44] Schur (I.). — Elementarer Beweis eines Satzes von L. Stickelberger, Math. Zeitschrift, 29, 1929, pp. 464–465.

[45] Sekiguchi (T.), Oort (F.) and Suwa (N.). — On the deformation of Artin-Schreier to Kummer, Ann. sci. École Norm. Sup. (4) 22, 1989,
no. 3, pp. 345–375.

[46] 

SERRE (J.-P.). — Corps locaux, Publications de l’Université de Nancago, No. viii, Hermann, Paris, 1968, 245 pp.

[47] 

SERRE (J.-P.). — Une “formule de masse” pour les extensions totalement ramifiées de degré donné d’un corps local, Comptes Rendus 286, 1978, pp. 1031–1036.

[48] 

SILVERMAN (J.). — Weierstrass equations and the minimal discriminant of an elliptic curve, Mathematika 31, 1984, no. 2, pp. 245–251.

[49] 

SKOLEM (Th.). — On a certain connection between the discriminant of a polynomial and the number of its irreducible factors (mod. p), Norsk Mat. Tidsskr. 34, 1952, pp. 81–85.

[50] 

STICKELBERGER (L.). — Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper, Verh. I. int. Math. Kongr., 1897, pp. 182–193.

[51] 

SWAN (R.). — Factorization of polynomials over finite fields, Pacific J. Math. 12, 1962, pp. 1099–1106.

[52] 

TATE (J.). — The arithmetic of elliptic curves, Invent. Math. 23, 1974, pp. 179–206.

[53] 

VORONOI (G.). — Sur une propriété du discriminant des fonctions entières, Verh. des 3. int. Math. Kongr., 1905, pp. 187–189.

[54] 

VOSTOKOV (S.). — Explicit formulas for the Hilbert symbol. in Invitation to higher local fields, Geom. Topol. Monogr., 3, Geom. Topol. Publ., Coventry, 2000, pp. 81–89.

[55] 

WADSWORTH (A.). — Discriminants in characteristic two, Linear and Multilinear Algebra 17 (1985), no. 3-4, pp. 235–263.

[56] 

WATERHOUSE (W.). — A unified Kummer-Artin-Schreier sequence, Math. Ann. 277, 1987, no. 3, pp. 447–451.

[57] 

WATERHOUSE (W.). — Discriminants of étale algebras and related structures, J. f. d. reine und angwandte Math. 379, 1987, pp. 209–220.

[58] 

WITT (E.). — Konstruktion der galoischen Körpern der Charakteristik p zu gegebener Gruppe der Ordnung pf, J. f. d. reine und angwandte Math. 174, 1936, pp. 237–245.