QUATERNION FIELDS of DEGREE 8: Galois Module Structure.

Jacques MARTINET Last update: Nov. 24th, 2014; first on line: January 16th, 2015.

Abstract. The note [8] of my homepage, as most of the *Notes aux Comptes Rendus de l'Académie des Sciences de Paris*, contains almost no proof. I give here detailed proofs for most of the results of [8]. In particular, we shall see that case C in Proposition 1 does not exist, as announced in the preceding *Corrigendum*.

Some of the proofs could have been found in Fröhlich's *Inventiones* paper [Fr], but Fröhlich's proofs make use of specific techniques from papers he wrote in the fifties, scarcely used by other mathematicians, so that it seems reasonable to write self-contained proofs.

We shall consider as in [8] a quaternionic extension of $N/\mathbb{Q}$ of degree 8. with quadratic subfields k_1, k_2, k_3 and biquadratic subfield K; the notation $d_i, m_i, \dots$ is as in *Corrigendum*, and focus on ramification properties of primes p of $\mathbb{Q}$ (or $p = \infty$), with special emphasis on $p = 2$. However we first consider more generally Galois extensions of a field K_0 of characteristic $\kappa \neq 2$, with Galois group a subgroup of $H_8 =: \langle \sigma, \tau \mid \sigma^4 = 1, \tau^2 = \sigma^2, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle$, thus H_8 itself or a cyclic group of order 4, 2, or 1 (these subgroups naturally occur when we replace K_0 by its completion at some place).

1. Embedding problems for $\boldsymbol{H_8}$: general results. By a theorem of Witt ([Wi]), K embeds in a H_8-extension N of K_0 if and only if the quadratic form $Q := m_1X^2 + m_2Y^2 + m_3Z^2$ is equivalent over K_0 to $Q_0 := X^2 + Y^2 + Z^2$.

To a quadratic forms $\sum_{i=1}^r a_i X_i^2$ on K_0 one can attach (cohomological) invariants $w_i, i \geq 0$, of which we only need w_0 (the *rank* $r \in \mathbb{Z}$), w_1 (the *discriminant* $d = \prod_i a_i \in K_0/{K_0^\times}^2$), and w_2 (the Hasse-Witt invariant $= \prod_{i<j}(a_i, a_j) \in \mathrm{Br}_2(K_0)$). [Br is the Brauer group, and the symbol (a, b) is the image (of order 2) of the quaternion algebra over K_0 defined by $i^2 = a$, $j^2 = b$, $ji = -ij$.]

The forms Q and Q_0 both have rank 3 and discriminant $1 \in K_0/{K_0^\times}^2$. If K_0 is a local field, a quadratic form is well-defined up to equivalence by w_0, w_1, w_2, and w_2 is the Hilbert symbol thanks to the identification $\mathrm{Br}_2(K_0) = \{\pm 1\}$; and if K_0 is a number field, then the Hasse-Minkowski theorem shows that equivalence can be read on the completions of K_0.

The situation is somewhat similar for cyclic groups of order 4: it is well known (and easy to prove) that a quadratic extension $K_0(\sqrt{m})$ embeds in a cyclic extension of degree 4 if and only if m is the sum of two squares in K_0, i.e. if and only if $mX^2 - Y^2 - Z^2$ represents zero, and in the local case, this is equivalent to $(m,-1) = +1$.

The following proposition makes easy the calculation of w_2 for H_8-extensions.

Proposition We have $w_2(Q) = (-1,-1)(-m_1,-m_2)$.
Proof. Since $m_3 \equiv m_1 m_2 \bmod K_0^2$, we have $(m_1,m_3) = (m_1, m_1 m_2)$ and $(m_2,m_3) = (m_2,m_1m_2)$, hence $(m_1,m_3)(m_2,m_3) = (m_1m_2,m_1m_2)$, and by the rule $(a,-a) = 1$, this is equal to

$$(m_1m_2,-1) = (m_1,-1)(m_2,-1)\,.$$

We then have $w_2(Q) = [(m_1,m_2)(-1,m_2)(-m_1,-1)](-1,-1)$, and the result follows by bilinearity. $\square$

Over $\mathbb{R}$, we have

$(a,b) = -1$ if a and b are negative, $(a,b) = +1$ otherwise. $\quad (*_\infty)$

Over $\mathbb{Q}_p$, the symbol (a,b) can be the calculated using the formulae below, taken from [Se2]. Write

$$a = p^\alpha u \quad \text{and} \quad b = p^\beta v$$

where u, v are p-units, and for $u \in \mathbb{Z}_2$ or $\mathbb{Z}$, set

$$\varepsilon(u) = \tfrac{u-1}{2} \mod 2 \text{ and } \omega(u) = \tfrac{u^2-1}{8} \mod 2\,.$$

Then we have

$$p \text{ odd}: \quad (a,b)_p = (-1)^{\alpha\beta\varepsilon(p)} \left(\tfrac{v}{p}\right)^\alpha \left(\tfrac{u}{p}\right)^\beta; \quad (*_p)$$

$$p = 2: \quad (a,b)_2 = (-1)^{\varepsilon(u)\varepsilon(v)+\alpha\omega(v)+\beta\omega(u)}\,. \quad (*_2)$$

In particular, we have $(-1,-1) = -1$ over $\mathbb{R}$ and $\mathbb{Q}_2$, and $(-1,-1) = +1$ otherwise.
[More generally, over an extension L of $\mathbb{Q}_p$, we have $(-1,-1) = -1$ if and only if $p = 2$ and $[L:\mathbb{Q}_p]$ is odd.]

2. Embedding problems for H_8: results over Q and Q_p. As a set of representatives for $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$, we may take

$$\{\pm 1, \pm 3, \pm 2, \pm 6\}\,,$$

defining seven quadratic extensions: $\mathbb{Q}_2(\sqrt{-3})$, unramified; $\mathbb{Q}_2(\sqrt{3})$ and $\mathbb{Q}_2(\sqrt{-1})$, with ramification jump 1; and $\mathbb{Q}_2(\sqrt{\pm 2})$ and $\mathbb{Q}_2(\sqrt{\pm 6})$, with ramification jump 2.
[For $m_1 \equiv m_2 \equiv 1 \bmod 2$ (resp. $\equiv 2 \bmod 4$), $\mathbb{Q}_2(\sqrt{m_1}) \simeq \mathbb{Q}_2(\sqrt{m_2})$ is equivalent to $m_1 \equiv m_2 \bmod 8$ (resp. $m_1 \equiv m_2 \bmod 16$).]

The calculation of the symbols $(m,-1)_2$ shows that $\mathbb{Q}_2(\sqrt{-3}) = \mathbb{Q}_2(\sqrt{5})$, $\mathbb{Q}_2(\sqrt{2})$ and $\mathbb{Q}_2(\sqrt{-6}) = \mathbb{Q}_2(\sqrt{10})$ embed in cyclic extensions of degree 4 and that the the remaining four do not.

From the list of quadratic extensions we deduce that there are also seven biquadratic extensions of $\mathbb{Q}_2$, that we list below according to the ramification index e_2 of 2, giving the corresponding sets $\{m_1, m_2, m_3\}$:
$e_2 = 2$: $\{-3,-1,3\}$, $\{-3,2,-6\}$, $\{-3,-2,6\}$;
$e_2 = 4$: $\{3,2,6\}$, $\{3,-2,-6\}$, $\{-1,2,-2\}$, $\{-1,6,-6\}$.

To list those of these fields which embed in a H_8-extension, we may discard from the list above those for which Q represents -1, since Q_0 does not. We are then left with three biquadratic extensions of $\mathbb{Q}_2$ out of seven, those with

$$\{m_1, m_2, m_3\} = \{-3,-2,6\}\ (e_2 = 2),\ \{3,2,6\} \text{ or } \{3,-2,-6\}\ (e_2 = 4)\,,$$

and using $(*_2)$ we check that these extensions do embed in a H_8 one.

It is a well-known fact (immediate from the very definition of ramification groups) that in a cyclic extension of prime power degree, an ideal which ramifies at some step then ramifies at all the further steps. Putting together this remark and the calculations above, we obtain the following statement, in which n_2 stands for the local degree and e_2 (as above) for the ramification index of 2 of the biquadratic subfield of an H_8-extension of $\mathbb{Q}$:

Theorem. Assume that 2 is ramified in $K/\mathbb{Q}$. Then one of the following holds for the completion $\widehat{N}_2$ of $N/\mathbb{Q}$ at a prime above 2 of N:

(1) $(n_2, e_2) = (2,2)$. $\widehat{N}_2/\mathbb{Q}_2$ is cyclic of degree 4 and contains $\mathbb{Q}_2(\sqrt{2})$ or $\mathbb{Q}_2(\sqrt{-6})$.
(2) $(n_2, e_2) = (4,2)$. $\widehat{N}_2$ contains $\mathbb{Q}_2(\sqrt{3}, \sqrt{2})$.
(3) $(n_2, e_2) = (4,4)$. $\widehat{N}_2$ contains one of the two fields $\mathbb{Q}_2(\sqrt{3}, \sqrt{2})$ or $\mathbb{Q}_2(\sqrt{3}, \sqrt{\pm 2})$.

For the sake of completeness, I give below the embedding conditions at an odd prime p, using $\{1, u, p, pu\}$ as a set of representatives for $\mathbb{Q}_p/\mathbb{Q}_p^2$, where $u \in \mathbb{Z}_p^\times$ is a non-residue modulo p.

(a) We have $(u,-1)_p = +1$ and $(p,-1)_p = (pu,-1)_p = \left(\frac{-1}{p}\right)$, so that embedding in a cyclic extension of degree 4 is possible for all quadratic extensions if $p \equiv 1 \mod 4$, but uniquely for the unramified one if $p \equiv -1 \mod 4$.

(b) There is a unique biquadratic extension, associated with the set $\{u, p, pu\}$. Since $(u,p)_p = \left(\frac{u}{p}\right) = -1$, this does not embed in a quaternionic extension.

(c) Putting together (a) and (b), we see that an odd prime p which ramifies in $K/\mathbb{Q}$ ramifies in two quadratic sub-extensions of $K/\mathbb{Q}$ and splits in the third one.

3. Ramification and discriminants. From now on N stands for an H_8-extension of $\mathbb{Q}$ with quadratic subfields $k_i = \sqrt{m_i}$, where the m_i are square-free integers, and biquadratic subfield K. Let d_i be the discriminant of k_i ($d_i = m_i$ or $4m_i$) and $D = d_1 d_2 d_3$ that of K (a square). Finally let Δ be the discriminant of N, related to that of K by the standard *transitivity relation*

$$\Delta = D^2 \,\mathrm{N}_{K/\mathbb{Q}}(\delta_{N/K})\,.$$

The behaviour in $N/\mathbb{Q}$ of the real prime of $\mathbb{Q}$ is clear: N is totally real or totally imaginary, K is totally real in both cases (because $\sigma^2 = \tau^2$ is the only element of order 2 in H_8), and Δ is strictly positive.

From now on let p be a finite prime of $\mathbb{Q}$, ramified in N.

We first consider the ramification index of p in $N/\mathbb{Q}$. If this index in $K/\mathbb{Q}$ is 1 (resp. 2, resp. 4), it is 1 or 2 (resp. 4, resp. 8) in $N/\mathbb{Q}$, and the latter cases may occur only if $p = 2$. We keep the following convention of [8]:

(1) If p is not totally ramified in $K/\mathbb{Q}$, then p is not ramified in k_1.
(2) If $p = 2$ is totally ramified in $K/\mathbb{Q}$, then $m_1 \equiv 3 \mod 4$ and $m_2 \equiv m_3 \equiv 2 \mod 4$.

Assume first that p is odd.

By the results proved at the end of the section above, if p is ramified in $K/\mathbb{Q}$, it splits in $k_1/\mathbb{Q}$ and we have $p\mathbb{Z}_N = (\mathfrak{P}\mathfrak{P}')^4$, and since the ramification is tame, $\mathfrak{P}$ and $\mathfrak{P}'$ have exponent 3 in the different $\mathcal{D}_{N/\mathbb{Q}}$. Hence $v_p(\Delta) = 6$.

If p is ramified only in N/K, then $p\mathbb{Z}_N$ is the square of a product of 4 prime ideals of degree 1 or 2 prime ideals of degree 2, having exponent 1 in $\mathcal{D}_{N/\mathbb{Q}}$. Hence $v_p(\Delta) = 4$.

To deal with $p = 2$ we shall use the following two results, valid in great generality for any Galois extension M/L relatively to a Dedekind domain A with fraction field L and its integral closure B in M (at least when the residue extensions are separable). Let $\mathfrak{p}$ be a prime ideal in A and $\mathfrak{P}$ a prime ideal in B lying above $\mathfrak{p}$, of ramification index e.

(1) We have $G_i(\mathfrak{P}) = \{1\}$ if $i > \frac{v_{\mathfrak{P}}(p)}{p-1}$ ([Se1], Sec. IV.2, Exer. (3)).

(2) (The Hasse-Arf theorem.) If M/L is Abelian then the ramification jumps *in upper numbering* are integral. (This is equivalent to the existence of strong congruences among the jumps in lower numbering;

such congruences are explicitly written in [Se1], Section IV.3; note that the weaker result of Prop. 11 in Section IV.2 sometimes suffices.)

Assume finally that $p = 2$. Let t_1 or t_1, t_2 or t_1, t_2, t_3 be the ramification jumps. Recall that the exponent of a prime ideal $\mathfrak{P}$ in the different of a Galois extension is given by the formula

$$v_{\mathfrak{P}}(\mathcal{D}) = \textstyle\sum_{i\geq 0} (|G_i| - 1)\,,$$

and note that we have $t_1 \geq 1$ since our Galois group is a 2-group.

If $e_2 = 1$ (i.e., if 2 is unramified in $K/\mathbb{Q}$) we have a single jump t_1 which satisfies $1 \leq t_1 \leq 2$, hence $t_1 = 1$ or 2, $v_{\mathfrak{P}}(\mathcal{D}_{N/\mathbb{Q}}) = 2$ or 3, and $v_2(\Delta) = 8$ or 12, cases (A) or (B) of [7].

If $e_2 = 2$, then $\widehat{K}_{\mathfrak{P}}/\mathbb{Q}_2$ is the extension by $\sqrt{2}$ or $\sqrt{-6}$ of an unramified extension of $\mathbb{Q}_2$, so that $t_1 = 2$, hence $t_2 = 4$ (because $t_2 \equiv t_1$ mod 2 and $t_2 \leq 4$), whence $v_{\mathfrak{P}}(\mathcal{D}_{N/\mathbb{Q}}) = 3 \times (4-1) + 2 \times (2-1) = 11$, and $v_2(\Delta) = 22$, case (D) of [7] (and case (C) of [7] does not exist).

If $e_2 = 4$, then 2 is totally ramified in N/Q, we have $G^1 = G_1 = G$, and G_2 corresponds to $\mathbb{Q}_2(\sqrt{3})/\mathbb{Q}_2$, which implies $t_1 = 1$ hence $t_2 = 3$, then $t_3 = 5$ or 7, and indeed $t_3 = 7$ by Hasse-Arf applied to N/k_1, whence

$$v_2(\Delta) = v_{\mathfrak{P}}(\mathcal{D}_{N/\mathbb{Q}}) = 2 \times 7 + 2 \times 3 + 4 \times 1 = 14 + 6 + 4 = 24\,,$$

case (E) of [7].

Remark. In all cases the upper ramification jumps are integral. This is clear for primes which are not totally ramified (because the inertia groups are cyclic), and the explicit calculation of Herbrand's function φ ([Se1], Section IV.3) shows that in the totally ramified case, the upper ramification jumps, namely $1, 2, 3$, are integral. However this is not general for non-Abelian extensions; see [Se1], Section IV.3, Exer. 3 for a quaternionic example (over $\mathbb{Q}(i)$); many examples can be found in [Fo].

4. The associated order. We keep the notation $N, K, \ldots$ of the previous sections, we set by $G = \mathrm{Gal}(N/\mathbb{Q})$ ($G \simeq H_8$), and denote by $\mathfrak{O}_G$ the order in $\mathbb{Q}[G]$ associated to N:

$$\mathfrak{O}_G = \{\lambda \in \mathbb{Q}[G] \mid \lambda\mathbb{Z}_N \subset \mathbb{Z}_N\}\,.$$

Let $g = G/\{1, \tau^2\}$. Let H be the skew-field of "ordinary" quaternions over $\mathbb{Q}$, with basis $(1, i, j, k)$ ($i^2 = j^2 = -1$, $ij = -ji = k$) we consider the order $\mathfrak{O}_0 = \mathbb{Z}[i, j, k]$. Note that $\mathfrak{O}_0$ is contained in a unique maximal order, namely the *Hurwitz order* $\mathfrak{M} = \mathfrak{O}_0 \cup \mathfrak{O}_0 + \omega$, $\omega = \frac{-1+i+j+k}{2}$.

Consider in $\mathbb{Q}[G]$ the two central idempotents

$$e' = \tfrac{1-\sigma^2}{2} \text{ and } e'' = \tfrac{1+\sigma^2}{2}\,.$$

They are orthogonal and add to 1, hence split $\mathbb{Q}[G]$ as

$$\mathbb{Q}[G] = \mathbb{Q}[G]e' \times \mathbb{Q}[G]e'' \simeq \mathbb{Q}[g] \times H\,.$$

These idempotents split N into a direct sum $N = K \perp K'$ (orthogonal for the bilinear form trace; K', not a field, is the kernel of $\mathrm{Tr}_{N/\mathbb{Q}}$). We now show that when 2 is ramified, these idempotent split $\mathbb{Z}_N$ into the direct sum of $\mathbb{Z}_K$ and the set $\mathbb{Z}_{K'}$ of integral elements of K'.

Let t be the highest ramification jump of some ideal $\mathfrak{P} \mid 2$. It results from Section 3 that G_t is the center $\{1, \tau^2\}$ of G and that $t+1 = e_{\mathfrak{P}}$, the ramification index of $\mathfrak{P}$. The definition of ramification groups shows that we have on $\mathbb{Z}_N$ the congruence $\tau^2 x \equiv x \mod \mathfrak{P}^e$ for every $\mathfrak{P}$, hence $\tau^2 \equiv x \mod 2$, that is, $e'\mathbb{Z}_N \subset \mathbb{Z}_N \cap K = \mathbb{Z}_K$, and finally $e'\mathbb{Z}_N = \frac{1}{2}\,\mathrm{Tr}_{N/K}(\mathbb{Z}_N) = \mathbb{Z}_K$.

Thanks to this splitting of $\mathbb{Z}_N$ the projection on $\mathbb{Z}[g]$ of $\mathfrak{O}_G$ is the order $\mathfrak{O}_g$ associated to $\mathbb{Z}_K$ in $\mathbb{Q}[g]$; see *Corrigendum*. The discriminant calculation of the note then shows that $\mathfrak{O}_G = \mathfrak{O}_g \times \mathfrak{O}_0$.

The result above completes the proofs of the note except that of Proposition 2. I leave it to the reader, and state instead its generalization to an arbitrary rank

Proposition 2'. (Plesken, [Pl].) *Let M be a finitely generated (left, torsion free)) module over $\mathfrak{O}_0$. Then M is isomorphic to a direct sum $\mathfrak{O}_0^p \oplus \mathfrak{M}^q$ (where $r := p+q$ is the rank of M).*

Results of this kind could be considered in the following setting: first establish that projective modules (over a convenient order) are locally free, then calculate the kernel in class groups of extension map to a maximal order.

References

[Fo] J.-M. Fontaine, *Groupes de ramification et représentation d'Artin*, Ann. Sci. E.N.S. **4** (1971), 337–392.

[Fr] A. Fröhlich, *Artin Root Numbers and Normal Integral Bases for Quaternion Fields*, Invent. Math **17** (1972), 143–166.

[Pl] W. Plesken, *Private communication* (Bonn, May 1991).

[Se1] J.-P. Serre, *Corps locaux*, Hermann, Paris (1962; 4-ième éd.: 2004). English ed.: *Local Fields*, Springer, Heidelberg, GTM 67 (1979).

[Se2] J.-P. Serre, *Cours d'Arithmétique*, P.U.F., Paris (1970; 4-ième éd.: 1995). English ed.: *A Course in Arithmetic*, Springer, Heidelberg, GTM 7 (1996).

[Wi] E. Witt, *Konstruktion von galoisschen Körpern der Characteristik p zu vorgegebener Gruppe der Ordnung p^f*, J. reine angew. math. **176** (1937), 31–44, = Ges. Abh., Springer, Heidelberg (1998), 120–128.