A NOTE ON THE KERNEL OF THE NORM MAP

MAREK SZYJEWSKI

Abstract. We investigate kernel of the norm map on power classes for cyclic field extensions.

1. Introduction

For fixed integer p and for a field K let $g(K) = K^*/K^{*p}$ be p-th powers class group. For $p = 2$ there is well known Gross-Fischer exact sequence

$$\{1, a\} \hookrightarrow g(K) \to g\left(K\left(\sqrt[p]{a}\right)\right) \xrightarrow{N} g\left(K\right). \tag{1.1}$$

(c.f. [3, p. 203].) The group $g(K)$ may be expressed as Galois cohomology group

$$g(K) = H^1\left(K, \mu_p\right) = H^1\left(G\left(K_s/K\right), \mu_p\left(K_s\right)\right)$$

which is the group $Hom\left(G\left(K_s/K\right), \mu_p\left(K\right)\right)$, provided K contains a primitive p-th root of unity. The norm map $H^1\left(L, \mu_p\right) \to H^1\left(K, \mu_p\right)$ is corestriction. In the case $p = 2$, $L = K\left(\sqrt{a}\right)$ the sequence above may be included in long exact sequence

$$\cdots \to H^{i-1}\left(K, \mu_2\right) \xrightarrow{\cup(a)} H^i\left(K, \mu_2\right) \longrightarrow H^i\left(L, \mu_2\right) \longrightarrow H^i\left(K, \mu_2\right) \xrightarrow{\cup(a)} H^{i+1}\left(K, \mu_2\right) \to \cdots$$

(e.g. [1, Cor. 4.6].)

A generalization of the sequence (1.1) for $p = 2$ and several square roots (a multiquadratic extension) appeared in [2, Th. 2.1].

We are interested in a direct generalization for other values of p, assuming that K contains all p-th roots of unity. We show that in general the sequence (1.1) need not to be exact even for $p = 3$. We show that this sequence is exact for p prime if K is a finite or local field, except the case p is characteristic of residue field. Thus we produce counterexamples that show that well-known zero sequence

$$H^1\left(K, \mu_p\right) \xrightarrow{res} H^1\left(L, \mu_p\right) \xrightarrow{cor} H^1\left(K, \mu_p\right)$$

2000 *Mathematics Subject Classification.* Primary 12E99; Secondary 12F99.
Key words and phrases. field extension, norm.

need not be exact for $p > 2$.

2. Notation and basic facts

Let p be fixed positive integer. In this section we don't need p to be a prime.

With a field K we associate an abelian group $g(K)$ - the cokernel of the homomorphism $\pi_K : x \mapsto x^p$. The usual notation is following:

$$\begin{aligned} K^{*p} &= im\,(\pi_K) \\ K^*/K^{*p} &= g(K), \end{aligned}$$

altough K^{*p} looks like p-th cartesian power.

The operation g is functorial: an embedding $r : K \to L$ induces a homomorfizm $\breve{r} : g(K) \to g(L)$.

$$coim\,(\breve{r}) = K^*/r^{-1}\left(L^{*p}\right) \cong \left(r\left(K^*\right) L^{*p}\right)/L^{*p} = im\,(\breve{r})\,.$$

If L/K is a finite field extension, then there is a norm homomorphism $N = N_{L/K}$, which commutes with π:

$$N \circ \pi_L = \pi_K \circ N;$$

thus $N : L^* \to K^*$ induces a homomorfizm $\breve{N} : g\,(L) \to g(K)$.

For every finite extension L/K of degree p (the same p fixed in the beginning to define g) if $r : K \to L$ is a K-embedding, then

$$\breve{N} \circ \breve{r} = 0$$

where 0 is a trivial homomorphism $g(K) \to g(K)$ (it follows from $N \circ r = N \mid_{K^*} = \pi_K$.)

In other words: the sequence

$$g(K) \xrightarrow{\breve{r}} g(L) \xrightarrow{\breve{N}} g(K) \tag{2.1}$$

is a zero-sequence, or is a complex, for $(L : K) = p$.

A natural question is if for a degree p extension image of $\breve{r}$ is the kernel of $\breve{N}$, or if this sequence is exact. The answer is positive for:

- $p = 2$ and all K of characteristic different from 2 (Gross-Fischer theorem);
- finite K and either arbitrary p dividing $|K| - 1$ or prime p different from $char\,(K)$;
- local K and prime p different from characteritic of the residue field.

Proposition 1. *If K is a finite field and either p divides $|K| - 1$ or p is a prime different form $char\,(K)$, $(L : K) = p$ then the sequence (2.1) is exact.*

Proof. A finite field K has unique extension L of degree p. Let v be a generator of the cyclic group L^*. Its norm is a product of its conjugates:

$$N_{L/K}(v) = v^{1+|K|+|K|^2+\cdots+|K|^{p-1}} = v^{(|K|^p-1)/(|K|-1)}$$

and has order $|K|-1$. Thus $N_{L/K} : L^* \to K^*$ is surjective, and so is $\breve{N} : g(L) \to g(K)$.

The assumption that p divides $|K|-1$ yields that $L = K(\sqrt[p]{u})$, where u is a generator of K^*: $K^* = \langle u \rangle$. Moreover

$$\mu_p(K) = Ker(\pi_K) = \langle u^{(|K|-1)/p} \rangle$$

is a cyclic group of order p. Thus $im(\pi_K)$ is a cyclic group of order $\frac{|K|-1}{p}$ and $g(K)$ is a cyclic group of order p. Since $|K|-1$ divides $|L|-1$, the same holds for L:

$$|g(K)| = |g(L)| = p.$$

A generator uK^{*p} of $g(K)$ is a p-th power in L, so $\breve{r} : g(K) \to g(L)$ is trivial and $N : g(L) \to g(K)$ is surjective; hence $N : g(L) \to g(K)$ is bijective.

In the case of p prime not dividing $|K|$ it is easy to see that $\gcd(p, |L|-1) = \gcd(p, |K|-1)$ since $|L| = |K|^p \equiv |K| \, (\mathrm{mod}\, p)$. Thus L contains $K(\sqrt[p]{u})$ (and $(K(\sqrt[p]{u}) : K) = \gcd(p, |K|-1)$,) $\breve{r} : g(K) \to g(L)$ is trivial and $|g(K)| = |g(L)| = \gcd(p, |K|-1)$; hence N is bijective. □

3. The first counterexample

Let $p = 3$. Let moreover $L = \mathbb{C}(t)$ be the field of rational functions in one variable t, and $K = \mathbb{C}(t^3)$. K is also a field of rational functions in one variable t^3 (we find the standard notation $K = \mathbb{C}(X)$, $t = \sqrt[3]{X}$ cumbersome.) Choose $\varepsilon = \frac{-1+\sqrt{-3}}{2}$ a primitive root of 1.

Proposition 2. *If $p = 3$, $L = \mathbb{C}(t)$ and $K = \mathbb{C}(t^3)$, then the norm of $h(t) = \frac{t-1}{\varepsilon t-1}$ is a cube, while $h(t)$ is not a product of element of K and a cube.*

Proof. L/K is cyclic and the automorphism σ of L defined by

$$\sigma(t) = \varepsilon t, \qquad \sigma|_{\mathbb{C}} = id_{\mathbb{C}}$$

generates the Galois group $G(L/K)$. It is easy to express norm $N_{L/K}$ in terms of decomposition of irreducibles in $\mathbb{C}[t]$:

$$N_{L/K}\left(a(t-b)^k\right) = a^3\left(t^3-b^3\right)^k.$$

Let $\varphi : L^* \longrightarrow \mathbb{Z}^3$ (a cartesian product here) be a homomorphism

$$\varphi(f(t)) = (v_{t-1}(f(t)), v_{\varepsilon t-1}(f(t)), v_{\varepsilon^2 t-1}(f(t)))$$

which assigns orders of zeros in $1, \varepsilon^2, \varepsilon$ to a rational function $f(t)$.

Firstly note that

$$\varphi\left(L^{*3}\right) = 3\mathbb{Z}^3.$$

Secondly

$$\varphi\left(K^*\right) = \mathbb{Z}\cdot(1,1,1).$$

The first observation enables a reduction mod 3:

$$\breve{\varphi} : g(L) \longrightarrow {\mathbb{Z}_3}^3, \qquad \breve{\varphi}\left(fL^{*3}\right) = \varphi(f) \pmod 3$$

where ${\mathbb{Z}_3}^3$ is again a cartesian power. The second observation yields that $\breve{\varphi}\left(\breve{r}\left(g\left(K\right)\right)\right) = lin\left((1,1,1)\right)$ is a line through $(1,1,1)$ in ${\mathbb{Z}_3}^3$.

Now the rational function

$$h(t) = \frac{t-1}{\varepsilon t - 1} = \frac{t-1}{\sigma\left(t-1\right)} \in L^*$$

has norm 1, $N_{L/K}\left(h\left(t\right)\right) = 1$, so the coset $h(t)L^{*3}$ is in the kernel of $\breve{N} : g(L) \longrightarrow g(K)$. On the other hand

$$\breve{\varphi}\left(h(t)L^{*3}\right) = (1,-1,0)$$

does not belong to the line $\breve{\varphi}\left(\breve{r}\left(g\left(K\right)\right)\right) = lin\left((1,1,1)\right)$, hence $h(t)L^{*3}$ does not belong to $\breve{r}\left(g\left(K\right)\right)$, i.e. is not a product of element of K and a cube. □

4. Local fields

We shall prove that for prime p, and local K containing primitive p-th root of unity, and L/K cyclic, the sequence 2.1 is exact except the case when p is characteristic of the residue field.

Lemma 1. *For a finite extension L/K of degree p the equality $Ker\left(\breve{N}\right) = im\left(\breve{r}\right)$ holds iff every α in L such that $N_{L/K}\left(\alpha\right) = 1$ is of the form $\alpha = x\beta^p$ for some $x \in K^*$, $\beta \in L^*$.*

Proof. If $Ker\left(\breve{N}\right) = im\left(\breve{r}\right)$ and $N\left(\alpha\right) = 1$, then $\alpha L^{*p} \in Ker\left(\breve{N}\right)$, so $\alpha L^{*p} = \breve{r}\left(x\right)$ for suitable $x \in K^*$; therefore $\alpha L^{*p} = xL^{*p}$.

Conversely, if $N\left(\alpha\right) = 1$ implies that $\alpha L^{*p} = \breve{r}\left(x\right)$ and $\gamma \in L^*$ is such that $\breve{N}\left(\gamma\right) = K^{*p}$, then

$$\begin{aligned} N\left(\gamma\right) &= y^p \text{ for suitable } y \in K^*, \\ N\left(y^{-1}\gamma\right) &= 1 \end{aligned}$$

and substitution $\alpha = y^{-1}\gamma$ shows that

$$\begin{aligned} y^{-1}\gamma &= x\beta^p \\ \gamma &= yx\beta^p \\ \gamma L^{*p} &\in im\left(\breve{r}\right). \end{aligned}$$

Thus $Ker\left(\breve{N}\right) \subset im\left(\breve{r}\right)$. □

Theorem 1. *If p is a prime, K is a local field with the residue field $\overline{K}$ of characteristic different from p, K contains a primitive degree p root of unity, L/K is a cyclic extension and $L = K\left(\sqrt[p]{a}\right)$, then the image of $\breve{r}$: $g(K) \to g\left(L\right)$ is the kernel of $\breve{N} : g\left(L\right) \to g\left(K\right)$.*

Note that for $p = 2$ (the case of Gross-Fischer theorem), every field K of characteristic different from 2 contains a primitive degree p root of 1 and every extension of degree p is cyclic.

Proof. Let $\left|\overline{K}\right| = q$, let O_K be the ring of integers, and let $x \longmapsto \overline{x}$ be the residue homomorphism $O_K \to \overline{K}$. By assumption K contains p-th primitive root ε of 1; the residue $\overline{\varepsilon} \in \overline{K}$ is a primitive p-th root of 1, so $p \mid q - 1$.

Consider following two cases:

Case 1. L/K is unramified.

If L/K is unramified and $\overline{L}$ is the residue field of the local field L, then $\overline{L}/\overline{K}$ is cyclic. If $N_{L/K}\left(\alpha\right) = 1$, then $N_{\overline{L}/\overline{K}}\left(\overline{\alpha}\right) = 1$; thus there exist $t \in \overline{K}^*$ and $b \in \overline{L}^*$ such that

$$\overline{\alpha} = tb^p.$$

If $\theta \in K^*$ has residue $\overline{\theta} = t$, then the polynomial

$$X^p - \theta^{-1}\alpha \in O_K\left[X\right]$$

has a root b in $\overline{L}$, thus $X^p - \theta^{-1}\alpha$ has a root β in L by Hensel Lemma; therefore

$$\beta^p - \theta^{-1}\alpha = 0, \qquad \alpha = \theta\beta^p.$$

The lemma above yields that $Ker\left(\breve{N}\right) = im\left(\breve{r}\right)$.

Case 2. L/K is ramified.

Since p is a prime, $\overline{L} = \overline{K}$ and $L = K\left(\sqrt[p]{\pi}\right)$, where π generates the maximal ideal of the ring O_K. Let $N\left(\alpha\right) = 1$. Then $\overline{\alpha}$ is a p-th root of 1:

$$\begin{aligned} \overline{N\left(\alpha\right)} &= 1 \\ \overline{\alpha}^p &= 1 \end{aligned}$$

Let $\rho \in K^*$ be a p-th root of 1 such that $\overline{\rho} = \overline{\alpha}$. Obviously,

$$\begin{aligned} N\left(\rho^{-1}\alpha\right) &= \left(\rho^{-1}\right)^p N\left(\alpha\right) = 1, \\ \overline{\rho^{-1}\alpha} &= 1. \end{aligned}$$

The polynomial

$$X^p - \rho^{-1}\alpha \in O_K\left[X\right]$$

has root 1 in $\overline{L}$, hence it has root β in L (even in K);

$$\beta^p - \rho^{-1}\alpha = 0, \qquad \alpha = \rho\beta^p$$

and the lemma above yields that $Ker\left(\breve{N}\right) = im\left(\breve{r}\right)$. $\square$

The other case is $p = char\left(\overline{K}\right)$. In this case there is another counterexample.

Proposition 3. *If* $p = 3$, $K = \mathbb{Q}_3\left(\sqrt{-3}\right)$, $\overline{K} = \mathbb{F}_3$, $L = K\left(\sqrt[6]{-3}\right)$, *then the image of* $\check{r} : g(K) \to g(L)$ *is smaller than the kernel of* $\check{N} : g(L) \to g(K)$.

Proof. The subring $O_K/3O_K$ of the factor ring

$$O_L/3O_L \cong \mathbb{F}_3[X]/\left(X^6\right)$$

corresponds to $\mathbb{F}_3\left[X^3\right]/\left(X^6\right)$. It is easy to see that

$$\left(a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4 + a_5X^5\right)^3 = a_0 + a_1X^3,$$

so any product $x\alpha^3$ with $x \in O_K$, $\alpha \in O_L$ reduces mod 3 to an element of $\mathbb{F}_3\left[X^3\right]/\left(X^6\right)$.

$\varepsilon = \frac{\sqrt{-3}-1}{2}$ is a primitive root of unity. If σ is the generator of Galois group $G(L/K)$ such that

$$\sigma\left(\sqrt[6]{-3}\right) = \varepsilon\sqrt[6]{-3},$$

then

$$\frac{1-\varepsilon\sqrt[6]{-3}}{1-\sqrt[6]{-3}} = \frac{\sigma\left(1-\sqrt[6]{-3}\right)}{1-\sqrt[6]{-3}}$$

has norm 1. Since

$$\begin{aligned}\frac{1-\varepsilon\sqrt[6]{-3}}{1-\sqrt[6]{-3}} &= \frac{1}{2}\sqrt[6]{-3}\left(1+\sqrt[6]{-3}+\left(\sqrt[6]{-3}\right)^2\right)+\frac{1}{1-\sqrt[6]{-3}} \\ &= 1+\left(\sqrt[6]{-3}\right)^4+\left(\sqrt[6]{-3}\right)^5+\left(\sqrt[6]{-3}\right)^6 \\ &\quad +\frac{1}{2}\left(\left(\sqrt[6]{-3}\right)^7+\left(\sqrt[6]{-3}\right)^8+\left(\sqrt[6]{-3}\right)^9\right) \\ &\quad +\frac{\left(\sqrt[6]{-3}\right)^{10}}{1-\sqrt[6]{-3}},\end{aligned}$$

if $\frac{1-\varepsilon\sqrt[6]{-3}}{1-\sqrt[6]{-3}}$ is a product $x\alpha^3$ with $x \in K$, $\alpha \in L$, then clearing denominators one may assume that $x \in O_K^*$, $\alpha \in O_L^*$. Thus $\frac{1-\varepsilon\sqrt[6]{-3}}{1-\sqrt[6]{-3}}$ should reduce mod 3 to an invertible element of $\mathbb{F}_3\left[X^3\right]/\left(X^6\right)$, while actually it reduces to $1 + X^4 + X^5$. □

5. Global fields

Theorem 2. *Let* p *be a prime,* $p > 2$, *and let* K *be a global field. If* L/K *is a cyclic Galois extension of degree* p, *then the factor group* $Ker\left(\check{N}\right)/im\left(\check{r}\right)$ *is infinite.*

Proof. Denote R, S the ring of integers in K, L respectively. Let σ be a generator of the Galois group $G(L/K)$. There exist infinitely many prime ideals q of R which split completely in S:

$$qS = \mathfrak{q} \cdot \sigma(\mathfrak{q}) \cdot \sigma^2(\mathfrak{q}) \cdot \cdots \cdot \sigma^{p-1}(\mathfrak{q}).$$

There exists $c \in \mathfrak{q} \setminus \mathfrak{q}^2$ which is coprime with

$$qS \cdot \mathfrak{q}^{-1} = \sigma(\mathfrak{q}) \cdot \sigma^2(\mathfrak{q}) \cdot \cdots \cdot \sigma^{p-1}(\mathfrak{q}).$$

The choice of c yields that $\mathfrak{q}$-adic valuation of c equals 1 and $\mathfrak{q}$-adic valuation of $\sigma(c)$ and $\sigma^2(c)$ is 0. The element $h(q) = \frac{c}{\sigma(c)} \bmod L^{*p}$ belongs to $Ker\left(\breve{N}\right)$. There is no $x \in K^*$ and $\beta \in L^*$ such that

$$h = \frac{c}{\sigma(c)} = x\beta^p,$$

because it would imply that

$$\begin{aligned} \frac{h}{\sigma(h)} &= \frac{\frac{c}{\sigma(c)}}{\sigma\left(\frac{c}{\sigma(c)}\right)} = \frac{x\beta^p}{x\sigma(\beta)^p} = \left(\frac{\beta}{\sigma(\beta)}\right)^p, \\ \frac{h}{\sigma(h)} &= \frac{c\sigma^2(c)}{(\sigma(c))^2} = \left(\frac{\beta}{\sigma(\beta)}\right)^p, \end{aligned}$$

while $\mathfrak{q}$-adic valuation of $\frac{c\sigma^2(c)}{(\sigma(c))^2}$ is exactly 1, so it is not divisible by p.

Thus there is infinte set of distinct elements

$$hL^{*p} = \frac{c}{\sigma(c)}L^{*p} \in Ker\left(\breve{N}\right)$$

which are not in $im(\breve{r})$. □

Remark 1. *In the setup of Proposition 2 one may use* $h(t) = \frac{t-a}{\varepsilon t-a}$ *for* $a \in \mathbb{C}^*$ *to see that* $Ker\left(\breve{N}\right)/im(\breve{r})$ *has cardinality of the continuum. One may use an algebraically closed field of arbitrary transfinite cardinality to obtain the same cardinality of* $Ker\left(\breve{N}\right)/im(\breve{r})$.

Acknowledgment. We thank the referee for pointing out to us the argument in the proof of Theorem 2.

References

[1] Jon Kr. Arason *Cohomologische Invarianten Quadratischer Formen* J. of Algebra **36** (1975), pp. 448 - 491

[2] Richard Elman, T.Y. Lam, Adrian R. Wadsworth *Quadratic Forms under Multiquadratic Extensions*, Indagationes Mathematicae v. **42** fasc. 2 (1980), .pp. 131 - 145

[3] T. Y. Lam *The Algebraic Theory of Quadratic Forms* W. A. Benjamin, Reading, Mass., 1973

(Marek Szyjewski) ul. Mieszka I 15/97, PL40-877 Katowice
E-mail address, M. Szyjewski: `szyjewsk@ux2.math.us.edu.pl`