Proceedings of the 3rd International Conference on Computing Innovation and Applied Physics
DOI: 10.54254/2753-8818/13/20240800

The interconnection between local and global m-th powers and Grunwald-Wang theorem

Peiwu Chen

Taishan College, Shandong University, Jinan, Shandong, China, 250100

zjlscpw@sina.com

Abstract. The relation between local and global solution of an equation can be discussed with the method of class field theory and algebraic number theory. In this piece of writing, the author will introduce the behavior of both local and global m-th power in some specific number field. Of course, the result in this paper can be extended into the function field, but it will not be involved in this paper. This paper will prove that if $k(\omega_{2^t})/k$ is cyclic then the Local m-th powers everywhere is equivalent to the global m-th power. In the Non-cyclic case this decomposition becomes $P(m, S) = k^m \cup \delta k^m$. This paper will also prove some useful propositions in topological group theory, which will be used in the proof of Grunwald-Wang theorem. Grunwald-Wang theorem states that we can find a cyclic extension with given local behaviors. To describe the extension, this paper combines character theory with a topological group, one can depict the cyclic extension. This theorem can be used in the further exploration of central simple algebra.

Keywords: Local And Global M-Th Powers, Cyclotomic Field, Algebraic Number Theory, Class Field Theory, Grunwald-Wang Theorem.

1. Introduction

There are lots of local and global phenomena in number theory. Artin-Hasse theorem shows that any Quadratic form has solutions in the global field if and only if it has solutions in every local field. However, things will become a little bit difficult if we want to solve the higher dimension situation. A widely known counterexample is that $3x^3 + 4y^3 = 5z^3$, this equation can be proved to have a local solution everywhere, however, it doesn't have the nontrivial solution in Q. Therefore, the local and global principle will lose its efficiency when it comes to the higher cases.

In this paper, the author will primarily use the method in cyclotomic field theory and class field theory to show that the local and global principle can still be true in some special cases, which is, in some specific number field, local m-th power everywhere is equivalent to the global m-th power. And the author will show that even in those particular number fields that don't fit the condition, it can still be described explicitly.

The proof offers us means by which we can use to do some further exploration in the local and global principle in number field. One can even use this to prove the Grunwald-Wang theorem, which states that we can find a cyclic extension with specific local behavior.

2. The interconnection of local m-th powers and global m-th powers

To begin with, first assume that k is a number field, in particular, it is a global field. In this section, the proof where k is a function field will be omitted which can be proved by the same token[1].

Denoting S to be a finite set of prime ideals, and let $\mathrm{P(m,S)}$ be the group of elements that are m-power in $\mathrm{k_p}$, where $\mathrm{p} \in \mathrm{S}$. Then it is easy to see that $\mathrm{k^m} \in \mathrm{P(m,S)}$ since every elements in $\mathrm{k^m}$ is a global m-th power, which is a local m-th power everywhere. Thus, it comes a natural question that in what condition:

$$\mathrm{P(m,S)} = \mathrm{k^m} \tag{1}$$

If the equality doesn't hold, than how to describe the group $\mathrm{P(m,S)}$.

Now the author will prove the following theorem which shows the interconnection between Local and Global m-th powers of a number field.

Theorem 1: Let k be a number field, $\mathrm{m} = 2^{\mathrm{t}}\mathrm{n}$, where n is an odd number. $\mathrm{P(m,S)}$ defined as above, if $\mathrm{k}(\omega_{2^{\mathrm{t}}})/\mathrm{k}$ if cyclic then one have $\mathrm{P(m,S)} = \mathrm{k^m}$.

Otherwise, at least $\mathrm{k}^{\mathrm{m}/2} \in \mathrm{P(m,S)}$. (Here in the second situation one can divide m with 2 since if $\mathrm{t} \leq 2$ then the cyclic condition holds)

Proof: First notice that if (m, n)=1, and let x be both m-th power and n-power, then x is a mn-th power. Therefore, WLOG, assume $\mathrm{m} = \mathrm{p^r}$.

If $\omega_{\mathrm{m}} \in \mathrm{k}$, then $\mathrm{K} = \mathrm{k}(\sqrt[\mathrm{m}]{\mathrm{x}})$ is well defined, and for β that not in S, one have $\mathrm{K}_\beta = \mathrm{k}_\beta$. Which means β splits completely in K. However, from class field theory[2]. the Dirichlet Density of completely splitting ideals equals to the degree of the extension, but S is a finite set, which means the Dirichlet Density of such β is 1[3]. Thus K=k, or x is a m-th power in k, or $\mathrm{P(m,S)} = \mathrm{k^m}$.

Else, ω_{m} not in k. From the above discussion, let $\mathrm{L} = \mathrm{k}(\omega_{\mathrm{m}})$ be the new ground field, and $\mathrm{x} = \mathrm{y^m}, \mathrm{y} \in \mathrm{L}$. Consider the decomposition of

$$\mathrm{X^m} - \mathrm{x} = \prod \mathrm{f_i(x)}\,, \tag{2}$$

$\mathrm{f_i(x)}$ is irreducible polynomials in k. Then the root of each $\mathrm{f_i(x)}$ is $\mathrm{y} * \omega_{\mathrm{m}}^{\mathrm{j}}$. While in the same time, we know that x is a local m-th power, thus for those p not in S, p splits completely in some splitting field of $\mathrm{f_i(x)}$[4].

Next, assume L/k is cyclic of prime power degree, then there exists a smallest extension $\mathrm{k}(\mathrm{y} * \omega_{\mathrm{m}}^{\mathrm{j}})$, since for p not in S, it must split completely in some subextension, so it must split completely in $\mathrm{k}(\mathrm{y} * \omega_{\mathrm{m}}^{\mathrm{j}})$. Again, using the conclusion in class field theory, we have $\mathrm{k}(\mathrm{y} * \omega_{\mathrm{m}}^{\mathrm{j}})$=k. Therefore, x is a m-th power in k.

For those odd primes p, let $\mathrm{I} = \mathrm{k}(\omega_{\mathrm{p}})$, then L/I is cyclic and of prime power degree, thus $\mathrm{x} = \mathrm{v^m}$,$\mathrm{v} \in \mathrm{I}$. Take norm on the both sides, $\mathrm{x^d} \in \mathrm{k^m}$, d is a factor of p-1, thus (d,m)=1, Thus $\mathrm{x} \in \mathrm{k^m}$.

For p=2, since in this situation, the degree of K/k is a prime order, thus if $\mathrm{k}(\omega_{2^{\mathrm{t}}})$/k is cyclic then we have already solved the problem. Therefore, we assume it is non-cyclic, and consequently $\mathrm{t} > 2$. Then let $\mathrm{U} = \mathrm{k(i)}$, we know that K/U is cyclic, which means $\mathrm{x} = \gamma^{\mathrm{m}}$, $\gamma \in \mathrm{U}$. Take norm on the both sides, we attain that $\mathrm{x}^2 = \mu^{\mathrm{m}}$,$\mu \in \mathrm{k}$. Then $\mathrm{x} = \pm\mu^{\mathrm{m}/2}$. However, if the negative sign hold, then $-1 = \mathrm{x}/\mu^{\mathrm{m}/2}$, since x is a local m-th power almost everywhere, thus -1 is a local square almost everywhere, thus k(i)=k, contradiction! Thus $\mathrm{x} = \mu^{\mathrm{m}/2}$,or $\mathrm{k}^{\mathrm{m}/2} \in \mathrm{P(m,S)}$.

The above theorem have solved the most situation of P(m, S), but one still can't write P(m, S) explicitly when $\mathrm{k}(\omega_{2^{\mathrm{t}}})$/k is non-cyclic. Therefore, we want to explore it further.

For the sake of simplification, denote $\mu_{\mathrm{r}} = \omega_{2^{\mathrm{t}}}$, and $\rho_{\mathrm{r}} = \mu_{\mathrm{r}}$+1/$\mu_{\mathrm{r}}$. Then it is easy to find that

$$\mathrm{k(i)k}(\rho_{\mathrm{r}}) = \mathrm{k}(\mu_r). \tag{3}$$

And those who know some cyclotomic field will know that $\mathrm{k}(\rho_{\mathrm{r}})$/k is a cyclic extension, which is not hard to verify.

Assume s is the maximal integer s.t. $\rho_s \in k$ but $\rho_{s+1} \notin k$. Then $k(\rho_{s+1})/k$ is then cyclic and if $i \in k(\rho_{s+1})$ then $k(\rho_r) = k(\mu_r)$ for all r. And conversely if $k(\mu_r)/k$ cyclic then since it has the only quadratic subfield, $k(\rho_{s+1})$=k(i).

Therefore, in the non-cyclic case, $k(\rho_r)k(i)$=$k(\mu_r)$ is an extension of degree 4 and has 3 degree 2 subextension which is $k(\rho_r)$, $k(i\rho_r)$, $k(i)$. Which means $2+\rho_s, i, -2-\rho_s$ are non-squares in k.

Consider $\rho_s \in k$, then $k(i) = k(\mu_s)$ which is cyclic, so if we want achieve non-cyclic, we must have $t > s$. And let σ be the automorphism of $k(i)/k$, then we must have $\sigma(\mu_s) = 1/\mu_s$.

Assume $x \in P(m, S)$, and $x \notin k^m$. let k(i) to be the ground field then $x = y^m$,$y \in k(i)$.

Then $(y/\sigma(y))^m$=1, thus $y/\sigma(y)$ is a m-th root of unity, however, since $\mu_{s+1} \notin k(i)$, it is a $2^s - th$ root of unity. Write $y = {\mu_s}^{\tau}$, then τ is an odd integer, else let $z = y * {\mu_s}^{2^{s-1}-\tau/2}$, then $z \in k$, and z^{2^t}=x, contradiction!

WLOG, assume $y/\sigma(y) = {\mu_s}^n$,here $m = 2^t n$.

Then $y/\sigma(y) = {\mu_s}^n = ((1+\mu_s)/(1+1/\mu_s))^n = ((1+\mu_s)/\sigma(1+\mu_s))^n$

Let$\gamma = y/(1+\mu_s)^n$, then $\gamma = \sigma(\gamma)$, thus $\gamma \in k$.

Here we obtain x=$\delta * \gamma^{2^t}$, where

$$\delta = \left(1+\mu_s\right)^m = \left(2+\rho_s\right)^{\frac{m}{2}} = \left(-2-\rho_s\right)^{\frac{m}{2}} \tag{4}$$

So far it have been proved that $P(m, S) \in k^m \cup \delta k^m$. But it still need to be verified that if this expression is significative. Which means we have to show that $\delta \notin k^m$ and $\delta \in P(m, S)$.

First we notice that $\delta = (2+\rho_s)^{m/2}$,and $i \notin k$, thus $\delta \notin k^m$ holds. Secondly, for $\delta \in k_p^m$, we must have $k(i)k(\mu_s)/k$ collapse, which means it can be a 4-degree extension. Conversely, if it does collapse, then δ indeed become s local m-th power.

According to the above discussion, we have attained the following theorem.

Theorem 2:k a number field. Then $P(m, S) = k^m$, except $k(\mu_{2^t})/k$ is non-cyclic and S contains all the prime ideals that $k(i)k(\mu_s)/k$ is a 4-degree extension, in this situation, $P(m, S) = k^m \cup \delta k^m$. As a corollary to theorem2, one can make an explicit description of J_m and C_m, which is the the subgroup of idele group and idele class group consist of those elements with m periods.

Corollary1: J_m and C_m, then $\widetilde{J_m} = C_m$,($\widetilde{J_m}$ means the image of J_m in C. Unless in the case that there is no prime ideal such that the local extension $k(i)k(\mu_s)/k$ is a 4-degree extension. Then in this case, $\exists a$, s.t.

$$\widetilde{J_m} \cup a\widetilde{J_m} = C_m. \tag{5}$$

Proof: It is a natural corollary according to the above discussion.

3. Topological groups

Consider an open finite order subgroup N of $P = \prod_{p \in S} k_p^*$, then if one can find an open finite order subgroup M of the ideal class group such that $M \cap P = N$, then one can describe the local behavior on S of class field belonging to M. To find this M, we have to prove some lemmas.

And we use $\overline{P}$ to represents the same group but with product topology.

Now consider some lemmas of topological groups.

Lemma 1: C is a topological group, A is a compact subset, B is a closed subset, Then AB is closed.

Proof: First transform this lemma, to prove AB is closed, we only need to prove AB is open, we have to prove if $x \notin AB$, then $\exists V$, an open neighborhood of x, s.t.$V \notin AB$. Which means if $A^{-1}x \cap B = 0, then\, \exists V, A^{-1}x \cap B = 0$. Note that $A^{-1}x$ is a compact subset, WLOG, we can assume A compact, $A \cap B = 0$, we want to prove the existence of V s.t.$AV \cap B = 0$. For $x \in A$, since B is an closed subset, then $\exists W_x, \mathrm{s.t.}\ xW_x \cap B = 0$, and for $WxW_y \in W_x$, since A is compact, there exist finite x, s.t. $V \in \cap W_x$, and $xW_x \cap B = 0$, then $\forall a \in A, \text{assume } a \in xW_x, aV \in xW_xV \in xW_xW_x \in xW_x \cap B = 0$, thus $AV \cap B = 0$.

Lemma 2:$P \cap C^m = P^m$, unless there is prime ideal such that the local extension $k(i)k(\mu_s)/k$ is a 4-degree extension, in this special case,

$$P \cap C^m = P^m \cup cP^m, \tag{6}$$

where c has component δ in those prime that doesn't collapse and 1 in other where.

Proof: let $x \in P \cap C^m$, then let y be an idele element that represents it, we can write $y = \alpha n^m$, $\alpha \in P(m, S)$, by theorem2, we have the lemma2 holds.

Lemma 3:Consider P as a topological group, then P^m is close in P, and P/P^m , $\overline{P}/\overline{P^m}$ compact.

Proof: First C^m is an open and finite order subgroup, thus it is closed, and therefore unless in the special case, else $P \cap C^m = P^m$ is also closed. Assume we are in the special case, then $P \cap C^{2m} \in P^m$, since $P \cap C^{2m}$ is closed, thus P^m is closed too.

For the map is continuous, thus we only need to show the compactness of $\overline{P}/\overline{P^m}$. We show k_p^*/k_p^{m*} is compact. For the archimedean, this is finite of order 1 or 2 depending on m. For those non-archimedean, we have k_p^*/k_p^{m*}=$Z/mZ \times U_p^*/U_p^{m*}$, and as we all know, the unit group is compact, therefore, it is compact too. It is not difficult to prove that the open subgroup of finite order of P and $\overline{P}$ corresponds to each other.

Lemma 4: Consider N is an open subgroup of finite index in P, then NC^n is closed in C.

Proof: Consider $\overline{W}$ be an open and compact neighborhood of 1 contained in $\overline{N}$. And let $n|m$ and $\overline{P}^m \in \overline{N}$, then since we have $\overline{N}/\overline{P}^m$ is compact. Therefore we can find a finite covering such that $\overline{N}$=∪ $p_i\overline{W}\overline{P}^m$, therefore we have the following finite covering, N=∪ p_iWP^m →NC^n=∪ $p_iWP^mC^n$=∪ p_iWC^n. Since W is compact and C^n is closed, thus NC^n is closed.

Lemma 5: C/C^n is compact.

Proof: Since we know that $C \cong R^+ \times C_0$, we have $C/C^n \cong C_0/C_0^n$, and C_0 is compact, therefore it is compact.

Lemma 6: one can find a neighborhood systems V s.t. C^nV is open subgroup of finite index in C.

Proof: Consider N to be a compact neighborhood of 1 in J. And let M to be its image in C, then since C/C^m is compact, we have C^nV is of finite order.Lemma 7: Consider N an open subgroup of finite order of P. Then ∃M an open subgroup of finite order of C, s.t. $P \cap M$=$N(P \cap C^n)$, here n is a given number, and M contains C^n.

Proof: As we all know, NC^n and PC^n is closed in C. And by assumption NC^n is of finite order in PC^n, thus NC^n is open in PC^n, which means $K \cap PC^n \in x$, where K is an open subgroup of C. Let M=KNC^n, then M is an open subgroup of finite order in C, and $P \cap M$=$P \cap PC^n \cap KNC^n$=$P \cap NC^n$=$N(P \cap C^n)$.

Theorem 3:Consider N be an open subgroup of finite order of P, then ∃M, open and finite order, s.t $M \cap P = N$. And the smallest integer that can be the exponent of C/M is equal to the smallest integer n s.t. $P \cap C^n \in N$, then

$P/N \cong PM/M$, and for the exponent m of P/N, then if $P \cap C^m \in N$, then n=m else n=2m.

Proof: Firstly, if $P \cap C^n \in N$, then by lemma7 we have already find the M. Now conversely we assume that $M \cap P = N$ and n to be the exponent of C/M, then $C^n \in M$, and $P \cap C^n \in M \cap P \in N$.

4. Grunwald-Wang theorem

Now consider the case that P/N is a cyclic group, those who familiar with characters will know that in this case we can attach P/N with a character χ, and write χ_p to be the local character act on k_p^*, and write n_p to be its periods. Therefore, according to the above discussion we have proven the following theorem.

Theorem 4:S be a finite set of prime ideals, and χ_p be local characters with periods n_p, m be their least common multiple. Then $\exists\chi$ a global character on C, and its has local behavior χ_p on k_p^*. And if $\prod_{p \in S} \chi_p(\delta)$=1 then it has period m, else it has period 2m.

Grunwald-Wang Theorem: k a global field, and S be a finite set of prime ideals, and $\mathrm{n_p}$ be a set of integers, m be their least common multiple. Then there exist a cyclic extension K/k with degree m and $\mathrm{K_\beta/k_p}$ has degree $\mathrm{n_p}$ for all p∈ S.

Proof: For Archimedean p, the choice is unique. For non-Archimedean p that collapse, choose the unramified extension with degree $\mathrm{n_p}$. Describe all these local extensions by characters, and apply the precious theorem we have prove the Grunwald-wang theorem.

This theorem has a lot of application in class field theory, and it holds in the functional field. What is more, the result can also be used in the theory of abelian variety[5].

5. Conclusion

In this paper, the author has proved the interconnection between Local and Global m-th powers and some proposition of topological groups, and combine this two theories by applying the character theory to prove Grunwald-Wang theorem. However, this paper is simply the proof without any example or counterexample. These examples can be found in Milne's book Class field theory. What's more, the author only mentions the number field, but show few thing about function field, this part of theory can be find in Tate's book Class field theory.

The Grunwald-Wang theorem can be extended into a more general one, and the condition can ve interpreted into character theory.

For further study, those who familiar to central division algebra can use Grunwald-Wang theorem to prove every division algebra over a number field K, it contains a maximal sub-cyclic extension of K. And this result can be used in the theory of abelian varieties.

References

[1] ARTIN, E. AND TATE, J. 1961. Class field theory. Harvard, Dept. of Mathematics. Notes from the Artin-Tate seminar on class field theory given at Princeton University 1951–52. Reprinted 1968, 1990; second edition AMS Chelsea Publishing, 2009.

[2] Milne, J. S. Class Field Theory. www.jmilne.org/math/. 2020:31-32,84

[3] Neukirch, J. Class Field Theory, volume 280 of Grundlehren der Mathematishen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin. 1986

[4] Lang, S. Algebraic Number Theory. Addison-Weysley Publishing Co.,Inc., Reading, Mass.-London-Don Mills, Ont. 1970

[5] Milne, J, S. v2.00 (March 17, 2008). Corrected, revised, and expanded; https://www.jmilne.org/math/CourseNotes/CFT.pdf