SOME NORMAL EXTENSIONS OF THE DIOPHANTINE GROUP

Kenneth K. Nwabueze

Department of Mathematics,
University of Brunei Darussalam,
BE 1410, Gadong, BRUNEI

Ajai Choudhry

High Commission of India,
P.O. Box 439, M.P.C., Airport Lama, Berakas,
Bandar Seri Begawan, BB 3577, BRUNEI

Abstract

Let $\mathbf{D}$ denote the Diophantine group and let K/F be an extension of number fields. For a prime p not dividing $(K : F)$, it is shown that the transfer of ideals $\phi_{F \rightarrow K} : \mathbf{D}_p(F) \rightarrow \mathbf{D}_p(K)$ is injective, the relative norm $N_{K/F} : \mathbf{D}_p(K) \rightarrow \mathbf{D}_p(F)$ is surjective, and $\mathbf{D}_p(K) \cong \mathbf{D}_p(K/F) \times \mathbf{D}_p(F)$. Some consequences of this result are also considered.

Mathematics Subject Classification: 11D09, 20D15

Keywords: Diophantine equation, Galois group, field extensions, relative norm, ideals

1 Introduction

The Diophantine equation

$$(1) \quad x^2 + y^2 = z^2$$

has attracted attention since ancient times. It arises from the Pythagorean theorem on right-angled triangles because the problem of finding all integral solutions to (1) is equivalent to geometric the problem of finding all right angled triangles whose sides are integral valued. A complete integral solution is given, in geometric terms, in the tenth book of Euclid's Elements. In modern notation, the complete integral solution is given by $x = (m^2 - n^2)l$, $y = 2mnl$, $z = (m^2 + n^2)l$, where l, m, n are arbitrary integers. Recall (see [2]) that if we insist that $l > 0$ and m, n are such that $m > n > 0$, then we get the Pythagorean triples, that is, all positive integral values of the triple

$[x, y, z]$ satisfying equation (1). Some authors do not distinguish all solutions to equation (1) from the Pythagorean triples. Strictly speaking, the Pythagorean triples take only the positive integral values of the solutions to the equation (1), since they arose from the geometric problems concerning right-angled triangles. In this paper, we abide by this convention and drop the term Pythagorean triples because we shall allow l, m, n to take any integral values. This means that our triples contain negative integers. The aim of this paper is to study some basic normal extensions induced by a group arising from integral solutions of the equation (1).

2 The Diophantine group

We use standard notations. $\mathbb{R}$, $\mathbb{Z}$ and $\mathbb{N}$, stand for the set of rationals, integers and natural numbers, respectively. Now let $L = \{[x, y, z] \mid x, y, z \in \mathbb{Z}\}$ denote the set to all integer solutions of equation (1), excluding the trivial solution $[0, 0, 0]$. Since (1) is a homogeneous equation, if $[x, y, z]$ is a solution to (1) then, for any rational number $\lambda \neq 0$, the triple $[\lambda x, \lambda y, \lambda z]$ is a solution. Define a relation " $\sim$ " on L by stipulating that $[x_1, y_1, z_1] \sim [x_2, y_2, z_2]$ if there exist a rational number $\lambda \neq 0$ such that $[x_1, y_1, z_1] = [\lambda x_2, \lambda y_2, \lambda z_2]$. It is easy to see that " $\sim$ " is a well defined equivalence relation, and so partitions the set of all triples satisfying equation (1) into disjoint classes. In particular, each equivalence class contains one and only one primitive triple, that is a triple of the form $\{[x, y, z] \mid \gcd(x, y, z) = 1\}$. Therefore we can take the primitive triples as representatives of these classes. Now let $L/\sim$ denote the set of equivalence classes induced by the equivalence relation $\sim$. We shall write the equivalence class of a triple $[x, y, z]$ in $L/\sim$ typically as $[x : y : z]$ in order to avoid confusion with the triple $[x, y, z]$. Next, define for any two elements $[x_1 : y_1 : z_1]$ and $[x_2 : y_2 : z_2]$ in the set $L/\sim$ a binary operation " $\star$ " as follows: $[x_1 : y_1 : z_1] \star [x_2 : y_2 : z_2] := [x_1 x_2 - y_1 y_2 + x_2 y_1 : z_1 z_2]$. It is easy to verify that under this operation, the structure $(L/\sim, \star)$ is an abelian group (see [3]). It is routine to check that the binary operation $\star$ is well-defined, closed, and commutative. Moreover, the identity element, $1_{(L/\sim, \star)}$ exists in $(L/\sim, \star)$, namely, the class $[x : 0 : x]_{(x \in \mathbb{Z})}$. Furthermore, the inverse of any element $[x : y : z] \in (L/\sim, \star)$, is $[x : -y : z]$. More precisely, if we set $\mathbf{D} = (L/\sim, \star)$, then the structure $\mathbf{D}$ is an abelian group. We will henceforth refer to $\mathbf{D}$ as the Diophantine group.

3 Algebraic number theoretic properties

For a number field K , denote by R_K its ring of integers, I_K its group of fractional ideals $\neq 0$, and $\mathbf{D}(K)$ the Diophantine group over K (i.e. with values

from K). Let D_4 denote the dihedral group of order 8, and A_4 the alternating group of order 12. Observe that for any relative extension K/F of number fields, the relative norm given by $N_{K/F} : I_K \rightarrow I_F$ induces a homomorphism $\mathbf{D}(K) \rightarrow \mathbf{D}(F)$, which we shall also denote by $N_{K/F}$. We shall call the kernel $\mathbf{D}(K/F)$ of this map *the relative diophantine group*. Furthermore also observe that the p -Sylow subgroup $\mathbf{D}_p(K/F)$ of $\mathbf{D}(K/F)$ is the kernel of the restriction of $N_{K/F}$ to the p -Sylow subgroup $\mathbf{D}_p(K)$ of $\mathbf{D}(K)$. Now, let $\phi_{F \rightarrow K} : \mathbf{D}(F) \rightarrow \mathbf{D}(K)$ denote the transfer of ideal classes arising from mapping ideals xR_F to xR_K ; whence

$$N_{K/F} \cdot \phi_{F \rightarrow K}(x) = x^{(K/F)}.$$

So, for all primes p not dividing the index of F in K , we have that the map $\mathbf{D}_p(F) \rightarrow \mathbf{D}_p(K)$ given by $d \rightarrow d^{(K:F)}$ is an isomorphism. This implies

$$\phi_{F \rightarrow K} : \mathbf{D}_p(F) \rightarrow \mathbf{D}_p(K)$$

is injective and

$$N_{K/F} : \mathbf{D}_p(K) \rightarrow \mathbf{D}_p(F)$$

is surjective. This means that $\phi_{F \rightarrow K}$ is a section of the exact sequence

$$(2) \quad 1 \longrightarrow \mathbf{D}_p(K/F) \longrightarrow \mathbf{D}_p(K) \xrightarrow{N_{K/F}} \mathbf{D}_p(F) \longrightarrow 1.$$

Therefore this sequence splits, and we have

$$\mathbf{D}_p(K) \cong \mathbf{D}_p(K/F) \times \mathbf{D}_p(F).$$

In other words, we have proved the following

Proposition 3.1 *Suppose K/F is an extension of number fields and p is a prime such that $p \nmid (K:F)$. Then the transfer of ideal classes*

$$\phi_{F \rightarrow K} : \mathbf{D}_p(F) \rightarrow \mathbf{D}_p(K)$$

is injective, the relative norm

$$N_{K/F} : \mathbf{D}_p(K) \rightarrow \mathbf{D}_p(F)$$

is surjective, and

$$\mathbf{D}_p(K) \cong \mathbf{D}_p(K/F) \times \mathbf{D}_p(F).$$

4 Applications

We can use proposition 3.1 to derive constraints on the diophantine groups of normal extensions. To do this, we need the presence of conjugate fields. Recall that the Hasse diagrams of subfields of extension with Galois groups A_4 and D_4 are respectively as follows:

Figure 1

Figure 2

The first application of proposition 3.1 is

Corollary 4.1 *Let $V_4 = C_2 \times C_2$ denote Klein four group, and C_n a cyclic group of order n . Suppose J/F is a V_4 -extension of number fields with quadratic subextensions $j_i, i = 0, 1, 2$. Then for any $p \neq 2$, we have*

$$(3) \quad \mathbf{D}_p(J/F) \cong \mathbf{D}_p(j_0/F) \times \mathbf{D}_p(j_1/F) \times \mathbf{D}_p(j_2/F),$$

and

$$(4) \quad \mathbf{D}_p(J/j_0) \cong \mathbf{D}_p(j_1/F) \times \mathbf{D}_p(j_2/F).$$

Proof: First of all observe that the operation of squaring is an automorphism on every finite abelian group of odd order. Now, suppose ω_i is the nontrivial automorphism of j_i/F . Then the identity

$$2 + (1 + \omega_0 + \omega_1 + \omega_2) = (1 + \omega_0) + (1 + \omega_1) + (1 + \omega_2)$$

in the group ring $\mathbb{Z}(V_4)$, gives rise to a homomorphism

$$\mathbf{D}_p(K/F) \longrightarrow \mathbf{D}_p(j_1/F) \times \mathbf{D}_p(j_2/F) \times \mathbf{D}_p(j_3/F) :$$

indeed we can write $d \in \mathbf{D}_p(K/F)$ in the form $d = c^2$, (observe that $c^{(1+\omega_0+\omega_1+\omega_2)} = 1$), and map d to $(c^{(1+\omega_3)}, c^{(1+\omega_3)}, c^{(1+\omega_2)})$. To check that this map is an isomorphism is easy, therefore we have the relation (3). By observing that

$$\mathbf{D}_p(J) \cong \mathbf{D}_p(J/j_0) \times \mathbf{D}_p(j_0)$$

together with the fact that

$$\mathbf{D}_p(j_0) \cong \mathbf{D}_p(j_0/F) \times \mathbf{D}_p(F),$$

yields

$$(5) \quad \mathbf{D}_p(J) \cong \mathbf{D}_p(J/j_0) \times \mathbf{D}_p(j_0/F) \times \mathbf{D}_p(F).$$

Now by comparing relation (5) with

$$\mathbf{D}_p(J) \cong \mathbf{D}_p(J/F) \times \mathbf{D}_p(F),$$

we deduce

$$(6) \quad \mathbf{D}_p(J/F) \cong \mathbf{D}_p(J/j_0) \times \mathbf{D}_p(j_0/F).$$

Relation (6) together with (3) gives (4) as claimed. $\diamond$

Corollary 4.2 *Let K/F be a dihedral extension of degree 8, having subextensions as in figure (2). Then we have that*

$$\mathbf{D}_p(K/J) \cong \mathbf{D}_p(J_1/j_1) \times \mathbf{D}_p(J_1/j_1)$$

for every prime $p \neq 2$.

Proof: Because J_1 and J'_1 are conjugate fields (over F), they have isomorphic ideal diophantine group, and by corollary 4.1 this implies that

$$\mathbf{D}_p(K/J) \cong \mathbf{D}_p(J_1/j_1) \times \mathbf{D}_p(J_1/j_1)$$

for every odd prime p . $\diamond$

Corollary 4.3 *Let K/F be an A_4 extension, with subextensions as denoted in figure 1. Then*

$$\mathbf{D}_p(K/J) \cong \mathbf{D}_p(J_1/J) \times \mathbf{D}_p(J_1/J) \times \mathbf{D}_p(J_1/J)$$

for all primes $p \neq 2$.

Proof. This follows at once from corollary 4.2 by noting that the fields J_i are conjugate over F . $\diamond$

References

- [1] K. Iwasawa, A note on ideal class groups, *Nagoya Math. J.*, **27**, (1966), 239-247.
- [2] K. K. Nwabueze, *Basic number theory: a first course*, Educational Technology Centre, Universiti Brunei Darussallam, 2003.
- [3] K. K. Nwabueze, and A. Choudhry, An example of a group, *Int. J. Pure Appl. Math.*, **15**, No. 3 (2004), 397-400.

Received: October 18, 2005