



Universiteit  
Leiden  
The Netherlands

## Complex multiplication constructions of abelian extensions of quartic fields

Asuncion, J.G.

### Citation

Asuncion, J. G. (2022, May 24). *Complex multiplication constructions of abelian extensions of quartic fields*. Retrieved from <https://hdl.handle.net/1887/3304503>

Version: Publisher's Version

License: [Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden](#)

Downloaded from: <https://hdl.handle.net/1887/3304503>

**Note:** To cite this publication please use the final published version (if applicable).

Co-supervised thesis presented to obtain the qualification of

**DOCTOR OF THE UNIVERSITY OF BORDEAUX  
AND LEIDEN UNIVERSITY**

Doctoral School of Mathematics and Computer Science

Specialization: Pure Mathematics

by

**JARED ASUNCION**

**Complex multiplication constructions of  
abelian extensions of quartic fields**

Under the supervision of Andreas Enge and Marco Streng

Defense on: 24 may 2022

**Members of the examination panel:**

Mr. David KOHEL	Professor, Aix-Marseille Université	President
Mr. Claus FIEKER	Professor, Technische Universität Kaiserslautern	Referee
Mr. David KOHEL	Professor, Aix-Marseille Université	Referee
Mrs. Sorina IONICA	Maître de conférences, Université de Picardie	Examiner
Mr. Ronald VAN LUIJK	Professor, Universiteit Leiden	Examiner
Mr. Andreas ENGE	Directeur de recherche, INRIA	Co-director
Mr. Marco STRENG	Associate Professor, Universiteit Leiden	Co-director

**Title:** Complex multiplication constructions of abelian extensions of quartic fields

**Abstract:** Let  $(K, \Phi)$  be a primitive quartic CM pair and  $(K^r, \Phi^r)$  be its reflex. In a 1962 article titled *On the class-fields obtained by complex multiplication of abelian varieties*, Shimura considered a particular family  $\{F_{K^r}(m) : m \in \mathbb{Z}_{>0}\}$  of abelian extensions of  $K$ , and showed that the Hilbert class field  $H_{K^r}(1)$  of  $K$  is contained in  $F_{K^r}(m)$  for some positive integer  $m$ . In this thesis, we make this  $m$  explicit. We also give a way to determine, given a positive integer  $n$ , whether or not  $H_{K^r}(1) \subseteq F_{K^r}(n)$ . In addition, we show a way to compute defining polynomials of the extension  $F_{K^r}(n)/K^r$  for any positive integer  $n$ . We also give an algorithm that computes a set of defining polynomials for the Hilbert class field  $H_{K^r}(1)$  using information on  $F_{K^r}(m)$ . Our proof-of-concept implementation of this algorithm computes a set of defining polynomials much faster than current implementations of the generic Kummer algorithm for certain examples of quartic CM fields.

**Keywords:** complex multiplication, CM fields, Hilbert class fields

**Title:** Constructions de multiplication complexe d'extensions abéliennes de corps quartiques

**Abstract:** Soit  $(K, \Phi)$  une paire CM quartique primitive et  $(K^r, \Phi^r)$  son réflexe. Dans un article de 1962 intitulé *On the class-fields obtained by complex multiplication of abelian varieties*, Shimura considère une famille particulière  $\{F_{K^r}(m) : m \in \mathbb{Z}_{>0}\}$  d'extensions abéliennes de  $K$ , et montre que le corps de classe Hilbert  $H_{K^r}(1)$  de  $K$  est contenu dans  $F_{K^r}(m)$  pour un certain entier positif  $m$ . Dans cette thèse, nous donnons une valeur explicite de cet entier  $m$ . Nous donnons également un moyen de déterminer, étant donné un entier positif  $n$ , si  $H_{K^r}(1) \subseteq F_{K^r}(n)$  ou non. De plus, nous donnons une manière de calculer les polynômes de définition de l'extension  $F_{K^r}(n)/K^r$  pour tout entier positif  $n$ . Nous donnons également un algorithme qui calcule un ensemble de polynômes de définition pour le corps de classes de Hilbert  $H_{K^r}(1)$  en utilisant des informations sur  $F_{K^r}(m)$ . Nous avons implanté cet algorithme et nous calculons un ensemble de polynômes de définition beaucoup plus rapidement que les implantations actuelles de l'algorithme générique de Kummer pour certains exemples de corps CM quartiques.

**Keywords:** multiplication complexe, corps CM, corps de classes de Hilbert

Institut de Mathématiques de Bordeaux UMR 5251  
Université de Bordeaux  
351, cours de la Libération - F 33 405 TALENCE

Mathematisch Instituut  
Universiteit Leiden  
Niels Bohrweg 1 2333 CA Leiden

**Complex multiplication constructions of  
abelian extensions of quartic fields**

PROEFSCHRIFT

ter verkrijging van  
de graad van doctor aan de Universiteit Leiden,  
op gezag van rector magnificus prof. dr. ir. H. Bijl,  
volgens besluit van het college voor promoties  
te verdedigen op dinsdag 24 mei 2022  
klokke 11:15 uur  
door

Jared Guissmo Asuncion

geboren te Mandaluyong, de Filipijnen  
in 1992

**Promotores:**

prof. dr. Andreas Enge (INRIA)

prof. dr. Peter Stevenhagen

**Copromotor:**

dr. Marco Streng

**Promotiecommissie:**

prof. dr. Bas Edixhoven †

prof. dr. Claus Fieker (Technische Universität Kaiserslautern)

dr. Sorina Ionica (Université de Picardie)

prof. dr. David Kohel (Aix-Marseille Université)

prof. dr. Ronald van Luijk

This work was funded by a cotutelle program between  
Leiden University and University of Bordeaux.

# Contents

<b>Introduction (English)</b>	<b>9</b>
<b>Introduction (Français)</b>	<b>13</b>
<b>Samenvatting</b>	<b>17</b>
<b>1 Class field theory and elliptic curves</b>	<b>21</b>
1.1 Class field theory . . . . .	21
1.2 Complex multiplication theory for elliptic curves . . . . .	23
1.2.1 Elliptic curves and their endomorphism rings . . . . .	24
1.2.2 Fields of moduli of elliptic curves . . . . .	26
1.2.3 Torsion points of elliptic curves . . . . .	27
1.2.4 Elliptic curves as complex tori . . . . .	28
<b>2 CM theory on principally polarized abelian varieties</b>	<b>35</b>
2.1 CM fields . . . . .	35
2.1.1 The type norm . . . . .	36
2.1.2 The reflex field . . . . .	37
2.1.3 The field generated by CM . . . . .	38
2.2 Jacobians of hyperelliptic curves . . . . .	39
2.2.1 Hyperelliptic curves and their Jacobians . . . . .	39
2.2.2 Principal polarizations on complex tori . . . . .	43
2.2.3 Fields of moduli of Jacobian surfaces . . . . .	46
2.2.4 Primitive torsion points of Jacobian surfaces . . . . .	49
2.2.5 Kummer varieties of Jacobian surfaces . . . . .	50
2.2.6 The Main Theorems of Complex Multiplication . . . . .	53
2.3 Theta functions . . . . .	55
2.3.1 Rosenhain invariants . . . . .	56
2.3.2 Mumford polynomials and theta functions . . . . .	58

<b>3</b>	<b>An explicit abelian extension containing the Hilbert class field</b>	<b>63</b>
3.1	Proof of the main theorem . . . . .	65
3.1.1	Embedding problems . . . . .	66
3.1.2	An explicit integer . . . . .	70
3.2	A decision problem . . . . .	75
3.2.1	The Shimura ray class group . . . . .	76
3.2.2	An algorithm to answer the decision problem . . . . .	79
<b>4</b>	<b>Computing abelian extensions generated by CM theory</b>	<b>81</b>
4.1	Abelian extensions in terms of Kummer varieties . . . . .	82
4.2	A Kummer variety over $CM_{K^r, \phi^r}(2)$ . . . . .	83
4.3	An algorithm for computing $CM_{K^r, \phi^r}(m)$ with $2 \mid m$ . . . . .	87
4.3.1	Finding a primitive torsion point . . . . .	87
4.3.2	Finding the conjugates of $h_2$ . . . . .	89
4.3.3	Computing the extension $CM_{K^r, \phi^r}(m)$ . . . . .	92
<b>5</b>	<b>Algorithms for finitely generated abelian groups</b>	<b>95</b>
5.1	Nice groups . . . . .	96
5.1.1	Definitions . . . . .	96
5.1.2	Examples of nice groups . . . . .	98
5.2	Subgroups and Hermite normal forms . . . . .	100
5.2.1	Representing subgroups . . . . .	100
5.2.2	Finding kernels . . . . .	102
5.2.3	Finding images . . . . .	104
5.2.4	Finding intersections . . . . .	105
5.3	Building Nice Groups . . . . .	106
5.3.1	Subgroups as nice groups . . . . .	106
5.3.2	Finding quotients . . . . .	108
5.3.3	Finding group extensions . . . . .	109
5.3.4	Computing the Shimura ray class group . . . . .	111
<b>6</b>	<b>Examples</b>	<b>115</b>
6.1	A detailed example . . . . .	116
6.1.1	Computing the cokernel of $N_1$ . . . . .	117
6.1.2	Computing the kernel of $N_2$ . . . . .	118
6.1.3	Computing the Shimura ray class group . . . . .	118

6.1.4	Verifying that the Hilbert class field is in the compositum . . .	119
6.1.5	Computing the Hilbert class field of the reflex . . . . .	119
6.2	An example involving torsion points . . . . .	121
6.2.1	A base period matrix . . . . .	122
6.2.2	The reflex field and Hilbert class field . . . . .	123
6.2.3	A primitive torsion point . . . . .	123
6.2.4	Approximations . . . . .	125
6.3	On the division-minimality of the integer given in Corollary 3.3 . . . .	126
6.4	Comparison with Kummer theory . . . . .	128
6.5	An experiment . . . . .	129
	<b>Bibliography</b>	<b>137</b>
	<b>Acknowledgments</b>	<b>141</b>
	<b>Curriculum Vitae</b>	<b>143</b>



