QUARTIC CM FIELDS

WENHAN WANG

Abstract. In the article, we describe the basic properties, general and specific properties of CM degree 4 fields, as well as illustrating their connection to the study of genus 2 curves with CM.

1. Background

The study of complex multiplication is closely related to the study of curves over finite fields and their Jacobian. Basically speaking, for the case of non-supersingular elliptic curves over finite fields, the endomorphism ring is ring-isomorphic to an order in an imaginary quadratic extension K of $\mathbf{Q}$. The structure of imaginary extensions of $\mathbf{Q}$ has been thoroughly studied, and the rings of integers are simply generated by $\{1, \sqrt{D}\}$ if $D \equiv 1 \mod 4$, or by $\{1, \sqrt{\frac{D}{4}}\}$ if $D \equiv 0 \mod 4$, where D is the discriminant of the field K. The theory of complex multiplication can be carried from elliptic curves to the (Jacobians) of genus 2 (hyperelliptic) curves. More explicitly, the Jacobian of any non-supersingular genus 2 (and hence, hyperelliptic) curve defined over a finite field has CM by an order in a degree 4, or quartic extension over $\mathbf{Q}$, where the extension field K has to be totally imaginary.

Description of the endomorphism ring of the Jacobian of a genus 2 curve over a finite field largely depends on the field K for which the curve has CM by. Many articles in the area of the study of genus two curves lead to the study of many properties of the field K. Hence the main goal of this article is, based on the knowledge of the author in the study of the genus 2 curves over finite fields, to give a survey of various, general or specific, properties of degree 4 CM fields.

Definition 1.1. A finite extension K of $\mathbf{Q}$ is said to be a CM field if it is totally complex.

Thus, all embeddings of K into $\mathbf{C}$ are complex embeddings, and the degree of K is then $d = r + 2x = 2s$, an even number. This shows that any CM field is of even degree over $\mathbf{Q}$. As a finite extension of $\mathbf{Q}$, a characteristic

Date: 12-10-2010.

zero perfect field, K can be generated by one element, say, $K = \mathbf{Q}(\alpha)$. It then follows that $\beta = \alpha + \bar{\alpha}$ is a real number, as it is fixed by complex conjugation. Similarly, $\gamma = \alpha\bar{\alpha}$ is also a real number. Thus $K_0 := \mathbf{Q}(\beta, \gamma)$ is a real extension of $\mathbf{Q}$, over which K is a degree two extension, as α and $\bar{\alpha}$ satisfy the polynomial $X^2 - \beta X + \gamma = 0$. Note that $\mathbf{Q}(\beta)$ is not always a co-degree two extension, as an example, consider $K = \mathbf{Q}(\sqrt{-2}, \sqrt{3})$. Since $\alpha = 1 + \sqrt{-2} + \sqrt{-6}$ is a generator for this extension, the corresponding $\beta = 2$ is not a generator for the totally real field, as a simple argument can show that $\sqrt{3} \in K$, as a real number, but not in $\mathbf{Q}$.

From now on we suppose K is a degree 4 CM field. Then there are 4 embeddings of K into $\mathbf{C}$, all of which are complex. For all discussions below, we fix an embedding of K and identify K with its image, and thus, this specific embedding, out of all the four embeddings, is denoted by id, the identity. We also denote the complex conjugation as $\rho : K \to \mathbf{C}$, as a ring homomorphism. Since K is a degree 2 extension over its real subfield K_0, ρ is an isomorphism of K. Denote any of the two embeddings of K, other than the identity or ρ, the complex conjugation, by σ, then the other embedding is $\sigma\rho$, as ρ preserves K. Hence the set of all embeddings of K is $\{id, \sigma, \rho, \sigma\rho\}$. Under the equivalent relation $\sigma_1 \sim \sigma_2$ if $\sigma_1 = \sigma_2\rho$, the equivalence class is called a CM type of K.

In the above discussion, we did not make the assumption that K is Galois over $\mathbf{Q}$. If K is Galois over $\mathbf{Q}$, the all embeddings form an order 4 group, which is either isomorphic to $\mathbf{Z}/4$ or $\mathbf{Z}/2 \times \mathbf{Z}/2$, thus K is either cyclic or biquadratic. If K is cyclic, then K_0 is the only subfield of K. If K is biquadratic, then K has three degree 2 subfields, one of which is K_0.

If K is not Galois, i.e., K is not normal, then let L be the normal closure of K. If immediately follows that $[L : K] = 2$. We could give the following outline for a field-theoretic proof. Since K is a CM field, ρ is an automorphism of K. Thus the only possible embeddings that are not automorphisms of K, are σ and $\sigma\rho$. Since L is the normal closure of K, in this case, L is $K.\sigma(K)$. Since the normal closure of K is contained in the splitting field of $f(X)$, where $K \approx \mathbf{Q}[X]/(f(X))$, and exactly two roots of $f(X)$ is in K and exactly two other roots is contained in $\sigma(K)$, thus the normal closure $L \subseteq K.\sigma(K)$. The other direction of inclusion is clear. Hence $\mathrm{Gal}(L/\mathbf{Q})$ is of order 8, hence could only be isomorphic to the Dihedral group $D_8 = \langle \alpha, \beta | \alpha^2 = 1, \beta^4 = 1, \alpha\beta\alpha = \beta^3 \rangle$, as it cannot be abelian.

The field K^r is the subfield of the normal closure of K, generated over $\mathbf{Q}$, by all elements of the form $\prod_i \sigma_i(x)$ for all $x \in K$, where σ_i runs through all embeddings from a CM type. The element $\prod_i \sigma_i(x)$ is sometimes called the type norm of x, note that the complex norm of the type norm (depends on the type) is the square root of the norm of x in $K/\mathbf{Q}$. This field, which consists of all type norms, is called the reflex field of K with respect to the type. This is the one of the two non-Galois sub-extensions over L that has degree 4 over $\mathbf{Q}$ and is not conjugate to K.

2. Jacobians of Genus 2 Curves

Suppose C is non-singular a genus 2 curve over $\mathbf{F}_p$, the prime field of characteristic p, if $p \nmid 30$, then C can be written as the Weierstrass form of genus 2 curves

$$C : \epsilon y^2 = x^5 + a_3 x^3 + a_2 x^2 + a_1 x + a_0.$$

The Jacobian of C, say, J_C, consists of all the equivalence classes of a degree zero divisor on C modulo principal divisors. J_C can be realized as an algebraic variety that is a quotient of a Kummer surface, more precisely, the algebraic structure, addition and scalar multiplication of divisor classes, equips J_C a structure of dimension 2 abelian variety, that is, a variety with an abelian group structure. Any group homomorphism as well as a rational map is called an isogeny between two Jacobians. From J_C to itself, an isogeny is called an endomorphism of J_C. Note that all endomorphism form a ring structure with 1, i.e., the zero endomorphism as the zero element, and the identity map as the identity.

The p-torsion of J_C plays an important rule in the classification of genus 2 curves. Since the order of the p-torsion of J_C is p^r, where r could be 0, 1, or 2, we may classify the curves in the following way, similar as for elliptic curves. If $r = 0$, C or J_C is called *supersingular.* If $r = 2$, C is ordinary. However, there is an intermediate case that does not appear for elliptic curves, i.e., $r = 1$. It has been shown that if $r = 1$ or 2, i.e., J_C is not supersingular, there exists an injective ring homomorphism from the endomorphism ring to some degree 4 CM field K, sending the endomorphism ring to the image, as a lattice in K. Thus the endomorphism ring is isomorphic to an order of K, as a finite-index sub-ring of O_K.

The endomorphism ring contains a special element, which is special because C is defined over a finite field $\mathbf{F}_q$, where $q = p^s$ is a power of a prime number p. The Frobenius map gives an endomorphism of J_C, thus is contained in the endomorphism ring. Another related map, the image of the Frobenius under the Rosati involution, is also an endomorphism of J_C. Thus $\mathbf{Z}[\pi + \bar{\pi}]$ is contained in the endomorphism ring as a sub-ring, which is also an order of K. Note that $\pi \cdot \bar{\pi} = q$. A number whose norm equals the power of a prime number corresponds to an isogeny class of genus 2 curves up to conjugation. As in the example, if $\pi\bar{\pi} = q$, then we say that π is a

Weil q-number . Hence the CM fields related to the study of genus 2 curves contain some Weil q-numbers.

As an example, we shall consider the following field, the first one listed by van Wamelen [vW1], $K = \mathbf{Q}(\zeta_5)$. In $\mathbf{Q}(\zeta_5)$, every element, obviously, can be written as $x = a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3$. Here we may fix the choice of ζ_5 to be $\exp(\frac{2\pi i}{5})$, by convention. However, there is another interesting representation of the same number, as

$$4x = A + B\sqrt{5} + C\sqrt{-5-2\sqrt{5}} + D\sqrt{5-2\sqrt{5}}.$$

More explicitly, this could be shown as following.

Proposition 2.1. *Every algebraic integer in $K = \mathbf{Q}(\zeta_5)$ can be written as $\frac{1}{4}(A + B\sqrt{5} + C\sqrt{-5-2\sqrt{5}} + D\sqrt{5-2\sqrt{5}})$, where A, B, C, D are all integers.*

Proof. Without loss of generality we may fix $\zeta_5 = \exp\left(\frac{2\pi i}{5}\right) = \cos\left(\frac{2\pi i}{5}\right) + i\sin\left(\frac{2\pi i}{5}\right)$. It is easy to compute $\zeta_5^2 = \cos\left(\frac{4\pi i}{5}\right) + i\sin\left(\frac{4\pi i}{5}\right)$, and $\zeta_5^3 = \overline{\zeta_5}$, $\zeta_5^4 = \overline{\zeta_5}$. In order to explicitly compute $\cos\left(\frac{2\pi i}{5}\right)$, we start with $\cos\left(\frac{\pi i}{5}\right)$. Note that $\cos\left(\frac{2\pi i}{5}\right) = \sin\left(\frac{\pi i}{10}\right)$, which leads to the following equation in $\cos\left(\frac{\pi i}{5}\right)$.

$$\left(2\cos^2\left(\frac{\pi i}{5}\right) - 1\right)^2 = \frac{1-\cos\left(\frac{\pi i}{5}\right)}{2}.$$

Explicit computation shows that both $\cos(\frac{2\pi}{5}) + i\sin(\frac{2\pi}{5})$ and $\cos(\frac{4\pi}{5}) + i\sin(\frac{4\pi}{5})$ are of the form above, and it does not need to verify the other two numbers as they are the complex conjugates of the ones displayed. □

Note that in this case, if the Frobenius $4\pi = A + B\sqrt{5} + C\sqrt{-5-2\sqrt{5}} + D\sqrt{5-2\sqrt{5}}$ for some $A, B, C, D \in \mathbf{Z}$, then

$$\begin{aligned}
16\pi\overline{\pi} &= \left(A + B\sqrt{5} + C\sqrt{-5-2\sqrt{5}} + D\sqrt{5-2\sqrt{5}}\right) \\
&\quad \left(A + B\sqrt{5} - C\sqrt{-5-2\sqrt{5}} - D\sqrt{5-2\sqrt{5}}\right) \\
&= \left(A + B\sqrt{5}\right)^2 - \left(C\sqrt{-5-2\sqrt{5}} + D\sqrt{5-2\sqrt{5}}\right)^2 \\
&= A^2 + 2AB\sqrt{5} + 5B^2 + (5+2\sqrt{5})C^2 + 2\sqrt{5}CD + (5-2\sqrt{5})D^2 \\
&= (A^2 + 5B^2 + 5C^2 + 5D^2) + (2AB + 2C^2 + 2CD - D^2)\sqrt{5}.
\end{aligned}$$

Basically if α is any algebraic integer in K, then $\alpha\bar{\alpha}$ is an algebraic integer in $K_0 = \mathbf{Q}(\sqrt{5})$. However, we want $x\bar{x}$ to be an integer, thus $AB + C^2 + 2CD - D^2 = 0$, and $A^2 + 5B^2 + 5C^2 + 5D^2$ is 16 times an odd prime number. It is not hard to observe that it is necessary that $p \equiv 1 \mod 5$.

On the other hand, the curve $y^2 = x^5 - \frac{1}{4}$ has CM by $K = \mathbf{Q}(\zeta_5)$. To see this, we simply observe that the map by sending any point (x, y) on the curve to $(\zeta_5 x, y)$, which remains on the curve, give rise to an endomorphism of the Jacobian. Moreover, the fifth power of this endomorphism corresponds to the fifth power of the map $(x, y) \mapsto (\zeta_5 x, y)$ on the curve, which is the identity map. This shows that the endomorphism ring of J_C contains a fifth root of unity. However, if p is not congruent to 1 modulo 5(10), there is no non-trivial root of unity in $\mathbf{F}_p$, and thus the map $(x, y) \mapsto (\zeta_5 x, y)$ can only induce the identity endomorphism on the Jacobian. However, if $p \equiv 1 \mod 5$, i.e., $p \equiv 1 \mod 10$, there is a non-trivial root of unity ζ^5 in $\mathbf{F}_p^*$, and hence the endomorphism ring contains a non-trivial root of unity, thus contains the unit group U_5, and thus $\mathbf{Z}[\zeta_5]$. This shows that, from another approach, that in order that the curve is not supersingular, p has to be congruent to 1 modulo 5.

Note that the field $\mathbf{Q}(\zeta_5)$, as a degree 4 CM field, is very special (actually unique); this plays an important rule in the study of genus 2 curves. As an analogy, the two imaginary quadratic extension $\mathbf{Q}\left(\sqrt{\frac{1-\sqrt{3}}{2}}\right)$ and $\mathbf{Q}(\sqrt{-1})$, play the similar roles for elliptic curves over finite fields. There exists other cyclotomic fields of degree 4, i.e., $\mathbf{Q}(\zeta_8)$ and $\mathbf{Q}(\zeta_{12})$. However, these are fields that corresponds to dimension 2 abelian varieties that are isogenous to the product of two elliptic curves, i.e., reducible Jacobians, over which computations are equivalent as being performed over, respectively, the two elliptic curves. Hence this kind of degree 4 CM fields does not play as important role as $\mathbf{Q}(\zeta_5)$.

We also have the following fact, regarding the case where $B = 1$ or -1 in the representation.

Lemma 2.2. *Let* $\pi = \frac{1}{4}\left(a + b\sqrt{5} + c\sqrt{-5 - 2\sqrt{5}} + d\sqrt{-5 + 2\sqrt{5}}\right)$ *be a Weil q-number with* $a, b, c, d \in \mathbf{Z}$, *and suppose* $cd \neq 0$. *Then (1)* $\mathbf{Z}[\pi, \bar{\pi}] \cap \mathcal{O}_{K_0} = \mathbf{Z}[\pi + \bar{\pi}]$*; and (2) the index of* $\mathbf{Z}[\pi, \bar{\pi}] \cap \mathcal{O}_{K_0}$ *in* $\mathcal{O}_{K_0}$ *is* B^2.

Proof. To prove the first statement, it suffices to show that $\mathbf{Z}[\pi, \bar{\pi}] \cap \mathcal{O}_{K_0} = \mathbf{Z}[\pi + \bar{\pi}, \pi\bar{\pi}]$. The inclusion "$\supseteq$" is clear. For the other inclusion, for any element α in $\mathbf{Z}[\pi, \bar{\pi}] \cap \mathcal{O}_{K_0}$, $\alpha = f(\pi, \bar{\pi})$ for some f a polynomial with coefficient in $\mathbf{Z}$ of two variables. The condition that $\alpha \in \mathcal{O}_{K_0}$ ensures that f is a symmetric polynomial, and therefore is a polynomial in $\pi + \bar{\pi}$ and $\pi\bar{\pi}$, which finishes the proof of the first statement. By computation, $\pi + \bar{\pi} = \frac{1}{2}(a + b\sqrt{5})$ and $\pi\bar{\pi} = q$, therefore $\mathbf{Z}[\pi, \bar{\pi}] \cap \mathcal{O}_{K_0} = \mathbf{Z}[\pi + \bar{\pi}]$. □

Proposition 2.3. *For a given Weil p-number in K corresponding to a genus 2 Jacobian, then the following statements are equivalent.*

(i) $B = \pm 1$;

(ii) $\mathbf{Z}[\pi, \bar{\pi}] \supseteq \mathcal{O}_{K_0}$;

(iii) $\frac{\sqrt{5}+1}{2}$ *defines an endomorphism in the ring generated by the Frobenius and its complex conjugate.*

Proof. *(i)* $\Rightarrow$ *(ii)*. Suppose $B = 1$ without loss of generality. Then both A, B are odd integers. Note that $\pi + \bar{\pi} = \frac{A}{2} + \frac{1}{2}\sqrt{5}$, which differs from $\frac{\sqrt{5}+1}{2}$ by an integer. Hence $\mathbf{Z}[\pi, \bar{\pi}] \supseteq \mathbf{Z}[\pi + \bar{\pi}] \supseteq \mathcal{O}_{K_0}$.
(ii) $\Rightarrow$ *(iii)*. Since $\mathrm{End}(J) \supseteq \mathbf{Z}[\pi, \bar{\pi}]$, hence $\frac{\sqrt{5}+1}{2}$ defines an endomorphism of J.
(iii) $\Rightarrow$ *(i)*. Suppose that $\frac{\sqrt{5}+1}{2}$ defines an endomorphism in the subring $\mathbf{Z}[\pi + \bar{\pi}]$. Note that for each element $\frac{x}{2} + \frac{y}{2}\sqrt{5} \in \mathbf{Z}[\pi + \bar{\pi}]$, one has $B \mid y$. Applying this statement to $\frac{\sqrt{5}+1}{2}$ one gets $B \mid 1$, hence $B = \pm 1$. □

This case $B = 1$ or -1 is special because it implies that the real subring of the endomorphism ring is the same as the largest possible ring of integers in the real sub-field of K, in our case, it is $K_0 = \mathbf{Q}(\sqrt{5})$. Note that if a prime number l divides the discriminant of the ring $\mathbf{Z}[\pi + \bar{\pi}]$, then it also divides $\mathbf{Z}[\pi, \bar{\pi}]$, and thus, divides the discriminant π. Thus the gap between the endomorphism ring being the ring of integer in K is reflected as some prime numbers that could divide the number B.

In the application of hyperelliptic curves to cryptography, a curve might be more secure in the sense that it is somehow difficult, or time consuming, to construct isogenies to another curve, which thus might be able to attack within shorter time. Intuitively, these curves are somehow isolated from others, by the difficulty to construct such isogeny. In this case, it is crucial to have large prime conductor gaps, and avoid any small factors of B.

If π is a Weil q-number in $K = \mathbf{Q}(\sqrt{5})$, then it is simple to check that $\zeta_5\pi$, $\zeta_5^2\pi$, $\zeta_5^3\pi$, $\zeta_5^4\pi$ are also Weil q-numbers. We have the following propositions regarding their discriminant.

Lemma 2.4.

$$\mathrm{disc}(\pi^5) = \prod_{i=0}^{4} \mathrm{disc}(\zeta_5^i \pi)$$

Proof. Note that by definition, the discriminant of π^5 is the product of $(\pi_i^5 - \pi_j^5)^5$, where π_i^5 and π_j^5 runs through all the Galois conjugates of π^5. Since each component factors as $(\pi_i-\pi_j)(\pi_i-\zeta_5\pi_j)(\pi_i-\zeta_5^2\pi_j)(\pi_i-\zeta_5^3\pi_j)(\pi_i-\zeta_5^4\pi_j)$, it is then obvious that this equation relating two products holds. □

We shall give another few examples of such degree 4 fields that are normal extensions over $\mathbf{Q}$, and in the next section, we shall discuss the property of non-normal extensions.

Another example that is similar to $K = \mathbf{Q}(\sqrt{-2+\sqrt{2}})$. The minimal polynomial of $a = \sqrt{-2+\sqrt{2}}$ is X^4+4X^2+2. Computation in Sage shows that $\{1, a, a^2, a^3\}$ forms an integral basis for K, and computation also gives that $a^2 = -2+\sqrt{2}$, and $a^3 =$ Since $\{1, \sqrt{2}, \sqrt{-2+\sqrt{2}}, \sqrt{-2-\sqrt{2}}\}$ forms an integral basis for $\mathcal{O}_K$, it can be shown that any algebraic integer in $\mathcal{O}_K$ can be written as $A+B\sqrt{2}+C\sqrt{-2-\sqrt{2}}+D\sqrt{-2+\sqrt{2}}$. In which case if the Frobenius map

$$\pi = A+B\sqrt{2}+C\sqrt{-2-\sqrt{2}}+D\sqrt{-2+\sqrt{2}},$$

then the complex norm of π is

$$\begin{aligned}
\pi\bar{\pi} &= \left(A+B\sqrt{2}+C\sqrt{-2-\sqrt{2}}+D\sqrt{-2+\sqrt{2}}\right) \\
&\quad \left(A+B\sqrt{2}-C\sqrt{-2-\sqrt{2}}-D\sqrt{-2+\sqrt{2}}\right) \\
&= (A+B\sqrt{2})^2+\left(C\sqrt{2+\sqrt{2}}+D\sqrt{2-\sqrt{2}}\right)^2 \\
&= (A^2+2B^2+2C^2+2D^2)+2(AB-C^2+2CD+D^2)\sqrt{2}.
\end{aligned}$$

Thus, if $\pi\bar{\pi} = p$, it is necessary that $p = A^2+2B^2+2C^2+2D^2$, and $AB-C^2+2CD+D^2 = 0$. Note that in this case, in order that we have a non-supersingular curve, A needs to be congruent to 1 modulo 16.

3. Non-Normal Extensions

As mentioned before, as an introduction to CM types, the non-normal quartic CM fields, say, K, has a normal closure that has degree 8 over $\mathbf{Q}$, with a Galois group isomorphic to D_8, or in some literature or convention, D_4. Anyways, it is isomorphic to the symmetric group of a square in the plane. Basic finite group theory tells us that the center of the order 8 dihedral group is isomorphic to $\mathbf{Z}/2$, and there are 4 other non-normal subgroups of order 2, forming 2 pairs, each consists 2 conjugate subgroups. We shall display an explicit example to assist the perception of these corresponding fields. The following example is from [MG1].

Example 3.1. Let $K = Q[X]/(X^4 + 34X + 217)$, which is not Galois over $\mathbf{Q}$. Note that explicitly, in the root form, the four roots, up to a fixed embedding of K into $\mathbf{C}$, are $\alpha_1 = \sqrt{-17-6\sqrt{2}}$, $\alpha_2 = -\sqrt{-17-6\sqrt{2}}$, $\beta_1 = \sqrt{-17+6\sqrt{2}}$, and $\beta_2 = -\sqrt{-17+6\sqrt{2}}$. Note that α_1 and α_2, β_1 and β_2, respectively are complex conjugate of each other. This field K, however, is not normal. To see that K is not Galois, note that the product of α_1 and β_1, gives $-\sqrt{217}$, which is a real number, however, is not in K_0, the real subfield of K_0. If we fix a root, say, α_1, then the other two embeddings not into K map α_1 to β_1 and β_2 respectively. Denote the map that maps α_1 to β_1 as σ, and ρ the complex multiplication. In this case, there are two choices of non-conjugate CM types, i.e., $\Phi_1 = \{id, \sigma\}$, and $\Phi_2\{id, \sigma\rho\}$. For both types, all elements of the form $\prod_i \phi_i(x)$ generates the corresponding reflex field of K. As I reviewed the article [MG1], it turns out in the procedure, it can be shown that for quartic CM fields, the reflex can also be generated by the sum $\sum_i \phi_i(x)$, where the sum ranges over all $x \in K$.

It might be worthy to mention this fact in the section which discusses non-normal extensions, where the reflex plays a role, as for the normal extensions, the reflex is the field itself.

If in general, we are considering an irreducible polynomial of the form $X^4 + aX^2 + b$, where $X^2 + aX + b$ is also irreducible over $\mathbf{Q}$, with integer coefficients $a, b \in \mathbf{Z}$, and moreover, if we assume that both roots of $X^2 + aX + b$, say r and s, are totally negative real roots, then the field $\mathbf{Q}[X]/(X^4 + aX^2 + b)$ is a quartic CM field, say, K, with real subfield $K_0 = \mathbf{Q}[X]/(X^2 + aX + b) = \mathbf{Q}(r) = \mathbf{Q}(s)$. In addition, the four roots of $X^4 + aX^2 + b$ are obviously $\sqrt{r}, -\sqrt{r}, \sqrt{s}, -\sqrt{s}$, respectively. Using the same argument for the above example, it follows that any one of the reflex contains $\mathbf{Q}(\sqrt{r}\sqrt{s}) = \mathbf{Q}(\sqrt{rs})$ as a subfield, i.e., $\mathbf{Q}(\sqrt{b})$, if b is not a square, is K_0^r.

Also note that $X^4 + aX^2 + b$ factors as

$$\begin{aligned} X^4 + aX^2 + b &= (X^4 + 2\sqrt{b}X^2 + b) - (2\sqrt{b} - a)X^2 \\ &= (X^2 + \sqrt{b})^2 - [(2\sqrt{b} - a)X]^2 \\ &= (X^2 + \sqrt{2\sqrt{b} - a}X + \sqrt{b})(X^2 - \sqrt{2\sqrt{b} - a}X + \sqrt{b}). \end{aligned}$$

Similarly, another way of factorization is

$$\begin{aligned} X^4 + aX^2 + b &= (X^4 - 2\sqrt{b}X^2 + b) - (-2\sqrt{b} - a)X^2 \\ &= (X^2 - \sqrt{b})^2 - [(-2\sqrt{b} - a)X]^2 \\ &= (X^2 - \sqrt{-2\sqrt{b} - a}X - \sqrt{b})(X^2 - \sqrt{-2\sqrt{b} - a}X - \sqrt{b}). \end{aligned}$$

The above two factorization are valid since $X^2 + aX + b$ has two real roots and hence $|a| > 2\sqrt{b}$.

Therefore the reflex field of K is one of the following two fields,

$$K_1^r = \mathbf{Q}(\sqrt{-17+6\sqrt{2}} + \sqrt{-17-6\sqrt{2}}, \sqrt{217}),$$

and

$$K_2^r = \mathbf{Q}(\sqrt{-17+6\sqrt{2}} - \sqrt{-17-6\sqrt{2}}, \sqrt{217}).$$

We may take any of them as an example, say, K_1^r, we shall show that the reflex of K_1^r is either $K = \mathbf{Q}(\sqrt{-17-6\sqrt{2}})$ or $K' = \mathbf{Q}(\sqrt{-17+6\sqrt{2}})$. Note that there are four embeddings of K_1^r, the identity id, the complex conjugation, the map that takes

$$\sqrt{-17+6\sqrt{2}} + \sqrt{-17-6\sqrt{2}} \mapsto \sqrt{-17+6\sqrt{2}} - \sqrt{-17-6\sqrt{2}},$$

the map that takes

$$\sqrt{-17+6\sqrt{2}} + \sqrt{-17-6\sqrt{2}} \mapsto -\sqrt{-17+6\sqrt{2}} + \sqrt{-17-6\sqrt{2}}.$$

The sum of the identity map and the third map that takes

$$\sqrt{-17+6\sqrt{2}} + \sqrt{-17-6\sqrt{2}} \mapsto \sqrt{-17+6\sqrt{2}} - \sqrt{-17-6\sqrt{2}}$$

maps

$$\sqrt{-17+6\sqrt{2}} + \sqrt{-17-6\sqrt{2}} \mapsto 2\sqrt{-17+6\sqrt{2}}.$$

Thus it is clear that the reflex relation is reflexive.

The above example is a good illustration to understand the term *reflex field* in the study of CM fields, as degree 4 CM fields are the simplest possible fields that could be non-normal, and the structure is easier to understand. The above detailed illustration was not given by the author of [MG1], but I thought it might be worthy to write things in detail down.

Note that the definition of *reflex field* is different literately from the definition of reflex field in Lang's book or Shimura's book [Sh1], where the reflex is defined to be

$$K^r = \mathbf{Q}(\mathrm{Tr}\Phi(x) : x \in K)$$

where Φ is a CM type of $K/\mathbf{Q}$ and $\mathrm{Tr}\phi$ is the trace of Φ, i.e., the sum of all embeddings in Φ. Note that in the case of $[K : \mathbf{Q}] = 4$, each CM type contains 2 embeddings that are not mutually complex conjugate of each other. Let $\Phi = \{\phi_1, \phi_2\}$, then we want to show that the authors' definition is the equivalent to Lang's or Shimura's, that is,

$$\mathbf{Q}(\phi_1(x) + \phi_2(x) : x \in K) = \mathbf{Q}(\phi_1(x)\phi_2(x) : x \in K)$$

for a fixed embedding of K into L and a CM type $\{\phi_1, \phi_2\}$. For any $x \in K$, note that

$$\phi_1(x) + \phi_2(x) = (1 + \phi_1(x))(1 + \phi_2(x)) - 1 - \phi_1(x)\phi_2(x),$$

which proves that $\mathbf{Q}(\phi_1(x) + \phi_2(x) : x \in K) \subseteq \mathbf{Q}(\phi_1(x)\phi_2(x) : x \in K)$. For the other direction, note that

$$2\phi_1(x)\phi_2(x) = (\phi_1(x) + \phi_2(x))^2 - (\phi_1(x))^2 - (\phi_2(x))^2,$$

and that $(\phi_1(x))^2$ and $(\phi_2(x))^2$ are two conjugate (not complex conjugate) real quadratic numbers in K_0, therefore there sum is in $\mathbf{Q}$. In particular, use the notation above, consider $x = \sqrt{r}$, then w.l.o.g. suppose $\phi_1(\sqrt{r}) = \sqrt{r}$ and $\phi_2(\sqrt{r}) = \sqrt{s}$. Then one verifies that $2\phi_1(\sqrt{r})\phi_2(\sqrt{r}) = (\phi_1(\sqrt{r}) + \phi_2(\sqrt{r}))^2 - a$. This shows inclusion in the opposite direction. Therefore these two definitions are equivalent.

It remains as an interesting topic, to analyze the behavior of the Weil p-numbers and their discriminants in a non-normal field. In the case where we have a normal field, and if it is cyclic, most of the work is done by making use of the character modulo some number l, by viewing the field K as a sub-extension of an order l cyclotomic field. Whereas in the case of non-normal extension, we need to go up to its normal closure, which contains two pairs of conjugate sub-fields, with non-commutative structures. Genus 2 curves with p-rank 1 do not show much difference as ordinary curves in the application of discrete log cryptography, though it is largely different in embedding pairs cryptography.

References

vW1. P. van Wamelen. Examples of genus two CM curves defined over the rationals, Math. Comp., vol. 68 (1999), no. 225, 307–320.

vW2. P. van Wamelen. On the CM character of the curves $y^2 = x^q - 1$, J. Number Theory Vol. 64, no. 1 (1997), 59–83.

vW3. P. van Wamelen. Proving that a genus 2 curve has Complex Multiplication, Math. Comp. 68 (1999), no. 228, 1663–1677.

Ko1. N. Koblitz. Algebraic Aspects of Cryptography, Algorithms and Computation in Mathematics Vol. 3, Springer-Verlag, 1998.

Ko2. N. Koblitz. CM-curves with good cryptographic properties, Advances in Cryptology - Crypto '91, Springer-Verlag, 1992, 279-287.

MG1. G. McGuire, et al. CM constructions of p-rank 1 genus 2 curves. *To appear in Journal of Number Theory.*

Sh1. G. Shimura. Abelian Varieties with Complex Multiplication and Modular Functions.