1 Preliminaries: fixed points of homographies

We note that $\mathrm{PSL}_2(\mathbb{R}) = \mathrm{PGL}_2^+(\mathbb{R})$, since any real matrix with determinant > 0 is homothetic to a unique matrix with determinant 1. The group $\mathrm{PSL}_2(\mathbb{R})$ acts on $\mathbb{P}^1(\mathbb{C})$ by homographies: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}$. Moreover, since γ is real, we have $\overline{\gamma \cdot z} = \gamma \cdot \overline{z}$. This means that it is enough to look at the action of $\mathrm{PSL}_2(\mathbb{R})$ on the quotient of $\mathbb{P}^1(\mathbb{C})$ by complex conjugation, which is $\mathcal{H} \cup \mathbb{R} \cup \{\infty\}$.

The fixed points for the homographic action of γ correspond to (complex) eigenspaces of γ.

Proposition 1. *Two matrices $\gamma, \gamma' \in \mathrm{PGL}_2(\mathbb{R})$ have the same fixed points in $\mathbb{P}^1(\mathbb{C})$ iff $\mathbb{R}[\gamma] = \mathbb{R}[\gamma']$.*

This means that a quadratic field $K \subset \mathbb{R}^{2\times 2}$ is determined by its fixed points in $\mathcal{H} \cup \mathbb{R} \cup \{\infty\}$. The field is imaginary iff it has one fixed point in $\mathcal{H}$ and real iff it has two in $\mathbb{R} \cup \infty$.

Numerically, the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with eigenvalues $\lambda, \lambda' = a + d - \lambda$ corresponds to the fixed points $\frac{\lambda - d}{c}$, $\frac{a-\lambda}{c}$.

Définition 2. We say that an element γ of $\mathrm{PSL}_2(\mathbb{R})$ is

(i) *elliptic* if it has two complex conjugate fixed points;

(ii) *hyperbolic* if it has two distinct fixed points in $\mathbb{R} \cup \{\infty\}$;

(iii) *parabolic* if it has one single, real fixed point.

Since $\det \gamma = 1$, it is easy to see that γ is hyperbolic iff $|\mathrm{Tr}\,\gamma| > 2$ (or its discriminant is < 0), elliptic iff $|\mathrm{Tr}\,\gamma| < 2$ (or its discriminant is > 0), and parabolic iff $|\mathrm{Tr}\,\gamma| = 2$ (or its discriminant is 0).

This means that, if γ is algebraic over $\mathbb{Q}$, then the algebra $\mathbb{Q}(\gamma)$ is an imaginary quadratic field if γ is hyperbolic, a real quadratic field (or $\mathbb{Q} \times \mathbb{Q}$) if γ is elliptic, and a local $\mathbb{Q}$-algebra if γ is parabolic.

Let $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ be a discrete subgroup. A point of $\mathcal{H}/\Gamma$ is called *elliptic* if it is fixed by an elliptic element $\gamma \in \Gamma$.

Proposition 3. *Let $z \in \mathcal{H}/\Gamma$ be an elliptic point. Then the stabilizer Γ_z of z in Γ is a finite cyclic group.*

Proof. Let $g \in \mathrm{SL}_2(\mathbb{R})$ such that $g \cdot i = z$. Then $g^1 \Gamma_z g$ fixes i, and hence included in the stabilizer of i in $\mathrm{SL}_2(\mathbb{R})$. This stabilizer is the group $\mathrm{SO}_1(\mathbb{R}) \simeq \mathbb{R}/2\pi\mathbb{Z}$. Any discrete subgroup of this compact group is finite and cyclic. $\lhd$

Proposition 4. *Let $\gamma \in \mathbb{R}^{2\times 2}$ be entire over $\mathbb{Z}$ and or finite order. Then the order of γ is either 2, 3, 4, or 6. (The order of γ in $\mathrm{PGL}_2(\mathbb{Z})$ is either 2 or 3).*

Proof. Both eigenvalues of γ are entire over $\mathbb{Z}$ and the norm is ± 1, so that the eigenvalues are $\pm e^{\pm i\theta}$ for some $\theta \in \mathbb{R}$. This implies that $\mathrm{Tr}\theta = 2\cos\theta$. Since this is also an integer, the only possibilities for the characteristic polynomial of γ are $x^2 \pm 1$, $x^2 \pm x \pm 1$, and $(x \pm 1)^2$. $\lhd$

2 Quaternions and complex-multiplication points

2.1 Quadratic fields inside quaternion algebras

Let B be a quaternion algebra over $\mathbb{Q}$. For any quadratic field $K \subset B$ with non-trivial automorphism σ, we know (by Skolem-Noether) that there exists an element $j \in B \smallsetminus 0$ such that, for all $x \in K$, $jx = \sigma(x)j$, and $j^2 = \beta \in \mathbb{Q}$. (Moreover, j is determined up to multiplication by $K^\times$). This gives the following map $B \hookrightarrow K^{2\times 2}$: $x \in K \mapsto \begin{pmatrix} x & 0 \\ 0 & \sigma(x) \end{pmatrix}$, $j \mapsto \begin{pmatrix} 0 & j^2 \\ 1 & 0 \end{pmatrix}$. This implies that $x + jy \in B \mapsto \begin{pmatrix} x & j^2\sigma(y) \\ y & \sigma(x) \end{pmatrix}$ and we easily check that this is an algebra homomorphism. This map extends to a splitting $B \otimes_{\mathbb{Q}} K \simeq K^{2\times 2}$.

Proposition 5. *Let $L = \mathbb{Q}[\sqrt{D}]$ be a quadratic extension of $\mathbb{Q}$ and $B/\mathbb{Q}$ be a quaternion algebra such that $B \subset L^{2\times 2}$. Then B contains a sub-field isomorphic to L.*

Proof. Let $\{i, j\}$ be a quaternionic basis of B over $\mathbb{Q}$: that is, $i^2 = c, j^2 = d \in \mathbb{Q}$, and $\mathrm{Tr}\,i = \mathrm{Tr}\,j = \mathrm{Tr}\,ij = 0$. Since $L^{2\times 2}$ is split over L, it is isomorphic to $(1, c/L)$, and has therefore a quaternionic basis $\{i, \varepsilon\}$ with $\varepsilon^2 = 1$. Since $\{i, j\}$ is another quaternionic basis of L, we have $j \in L[i] \cdot \varepsilon$, or $j = a\varepsilon$ with $a \in L[i]$. Moreover, we see that $d = j^2 = a\varepsilon a\varepsilon = a\overline{a}\varepsilon^2 = N_{L[i]/L}(a) \in \mathbb{Q}$.

We now prove the following lemma: let $z \in L[i]$ such that $N_{L[i]/L}(z) \in \mathbb{Q}$. Then $z \in \mathbb{Q}[i]^\times \cdot \mathbb{Q}[i\sqrt{D}]^\times$. We write $z = x + y\sqrt{D}$ with $x, y \in \mathbb{Q}[i]$. Since $N_{L[i]/L}(z) = (x +_y \sqrt{D})(\overline{x} + \overline{y}\sqrt{D}) \in \mathbb{Q}$, we see that $(x\overline{y} + \overline{x}y) = 0$. This means that $y/x \in i\mathbb{Q}$, or that $y = itx$ with $t \in \mathbb{Q}$. We then have $z = x + y\sqrt{D} = x(1 + i\sqrt{D}\,t)$ as required.

Applying this lemma to a, we see that we may write $uj = (p + i\sqrt{D}\,q)\varepsilon$ with $u \in \mathbb{Q}[i]^\times$, which means that $(uj)^2 = (p^2 - cDq^2)$. Consequently:

$$B \simeq \left(\frac{c,\, p^2 - cDq^2}{\mathbb{Q}}\right) \simeq \left(\frac{p^2c, c^2q^2D - p^2c}{\mathbb{Q}}\right) \simeq \left(\frac{\frac{p^2}{cq^2}, D - \frac{p^2}{cq^2}}{\mathbb{Q}}\right). \tag{1}$$

In this last basis, we then have $i^2 + j^2 = D$, so that $\mathbb{Q}[i+j] \simeq L \subset B$ as required. $\lhd$

2.2 Complex multiplication points

Let B be an indefinite quaternion algebra over $\mathbb{Q}$. We fix a real quadratic $K \supset \mathbb{Q}$ and choose one of the two embeddings $K \subset \mathbb{R}$. The construction of 2.1 then defines an unique map $\eta : B \to \mathbb{R}^{2\times 2}$. (Note that the image of jK is well-defined!). Let also $\mathcal{O}$ be an order of B.

For any $z \in \mathbb{C}$, we write $\Lambda(z)$ for the lattice $\eta(\mathcal{O}) \cdot \binom{z}{1}$ of $\mathbb{C}^2$. Let $A(z)$ be the polarized abelian surface $\mathbb{C}^2/\Lambda(z)$.

We say that z has *complex multiplication* by $L \subset B$ if it is the fixed point of $\eta(L)$, or equivalently if $\eta(L) \cdot \Lambda(z) = \Lambda(z)$.

Théorème 6. *Let $z \in \mathbb{C}$. The following are equivalent.*

(i) The point z has complex multiplication (by an imaginary quadratic field L).

(ii) The abelian surface $A(z)$ is isogenous to the square of an elliptic curve E, having complex multiplication (by L).

(iii) The ring $\operatorname{End}_{\mathbb{Q}}(A)$ is isomorphic to $L^{2\times 2}$.

(iv) The ring of QM-automorphisms $\operatorname{End}_B(A)$ is not reduced to $\mathbb{Q}$.

Proof. (ii) $\Rightarrow$ (iii). If $A(z) \sim E \times E$ then $\operatorname{End}_{\mathbb{Q}}(A(z)) \simeq \operatorname{End}_{\mathbb{Q}}^{2\times 2}$.

(iii) $\Rightarrow$ (ii). By Falting's proof of the Tate conjecture for abelian varieties over number fields, we know that, for ℓ prime,

$$\operatorname{Hom}_{\mathbb{Q}}(A, E \times E) \otimes \mathbb{Z}_\ell \quad \simeq \quad \operatorname{Hom}_{\mathrm{Gal}}(T_\ell(A), T_\ell(E) \times T_\ell(E)).$$

The assumption (iii) means that the right-hand side contains an isomorphism ι. The image of ι on the left-hand side is an isogeny.

(iii) $\Rightarrow$ (ii), elementary proof. Since $\operatorname{End}_{\mathbb{Q}}(A)$ is not a division algebra, A is not simple. This means that there exists an isogeny $A \sim E_1 \times E_2$, where E_1, E_2 are elliptic curves. If $E_1 \nsim E_2$ then $\operatorname{End}_{\mathbb{Q}} A \simeq \operatorname{End}_{\mathbb{Q}} E_1 \times \operatorname{End}_{\mathbb{Q}} E_2$, which is at most the product of two quadratic fields and therefore does not contain the quaternion algebra B. This proves that E_1 is isogenous to E_2, so that $A \sim E_1^2$.

(iv) $\Rightarrow$ (i). Let $L = \operatorname{End}_B A(z)$ and assume that $L \neq \mathbb{Q}$. For any $\lambda \in L \smallsetminus \mathbb{Q}$, the multiplication-by- λ map defines a map $m_\lambda : \mathbb{C}^2 \to \mathbb{C}^2$, stabilizing $\Lambda(z)$ (by the universal property of the universal cover of $A(z)$). By the usual properties of abelian varieties, m_λ is a $\mathbb{C}$-linear map. Since $m_\lambda(z) \in \eta(\mathcal{O}) \cdot z$, there exists $c \in \mathcal{O}$ such that $m_\lambda(z) = \eta(c)z$. Moreover, since λ is a B-endomorphism, m_λ commutes with all elements of $\eta(\mathcal{O})$, which implies that c lies in the center of B. Since B is a central simple $\mathbb{Q}$-algebra, this means that $c \in \mathbb{Q}$. In other words, z is fixed by the homographic action of λ. We just showed that z has complex multiplication by L.

(i) $\Rightarrow$ (iv), not-working proof. We write $X = \eta(\mathcal{O}^{\times +}) \smallsetminus \mathcal{H}$ for the Shimura curve and $\mathcal{A} \to X$ for the relative abelian surface with quaternionic multiplication by $\mathcal{O}$.

Let $\iota : \{z\} \hookrightarrow X$ be the injection of the point z. We then know that $A(z) = \mathcal{A} \times_{X,\iota} \{z\}$ is the fibre at z of the surface $\mathcal{A}$.

Assume that z has complex multiplication by a ring R. This means that there exists $\lambda \in H \smallsetminus \mathbb{Q}$ such that $\eta(\lambda) \cdot z = z$. Write $\gamma = \eta(\lambda) \in \mathbb{R}^{2\times 2}$; then $\gamma \circ \iota = \iota$, Let $\mathcal{A}_\gamma = \mathcal{A} \times_X \gamma$ be the pull-back of $\mathcal{A}$ along γ, and $A_\gamma = A(z) \times_{\mathcal{A}} \mathcal{A}_\gamma$. Since $\gamma \circ \iota = \iota$, A_γ is the fibre of $\mathcal{A}_\gamma$ above z, and therefore isogenous (as a B-QM surface) to $A(z)$.

Therefore, the scalar $\lambda \in H \smallsetminus \mathbb{Q}$ defines an endomorphism m_λ of $A(z)$. We see that m_λ has the same characteristic polynomial as λ, which means that m_λ is an embedding of R in B.

(i) $\Rightarrow$(iv). Assume that z has complex multiplication by an element $x \in B \smallsetminus \mathbb{Q}$. Since $\operatorname{Im} z > 0$, $L = \mathbb{Q}(x)$ is imaginary quadratic over $\mathbb{Q}$. Write $\eta(x) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then $x \cdot \binom{z}{1} = (cz + d)\binom{z}{1}$, so that $u = (cz + d)$ is an endomorphism of $\Lambda(z)$. Moreover, since u is a homothety, it commutes to B, so that it is a B-endomorphism of $A(z)$. Finally, since L is imaginary, $L \neq K$, therefore $c \neq 0$ and $u \notin \mathbb{R}$.

(iii) $\Rightarrow$ (iv). By Prop. 5, since $B \subset L^{2\times 2}$, B contains a sub-field L' isomorphic to L. Write $L' = \mathbb{Q}[\sqrt{D}]$: then the element $\sqrt{D} \in B$ is diagonalizable over $\mathbb{Q}$, and therefore of the form $\begin{pmatrix} \sqrt{D} & \\ & -\sqrt{D} \end{pmatrix}$ in some basis of L^2. This shows that there exists maps $L \subset B \subset L^{2\times 2}$ such that the composition is the map $x \mapsto \begin{pmatrix} x & \\ & \sigma(x) \end{pmatrix}$, where σ is the non-trivial automorphism of $L/\mathbb{Q}$. We now see that the L-homothety matrices commute with all elements of B, so that $\operatorname{End}_B A = L$.

(iv) $\Rightarrow$ (iii) Let $R = \operatorname{End}_{\mathbb{Q}} A \supset B$. Then $C = \operatorname{End}_B A$ is the commutant of B in R. Since B is central simple, if $R = B$ then $C = \mathbb{Q}$, which is impossible. Hence $R \neq B$. $\lhd$

Let $z \in X(\mathcal{O})$ be a CM point by the imaginary quadratic field $L \subset B$. We say that z has *complex multiplication by* $\mathcal{A} = L \cap \mathcal{O}$. For any quadratic order $\mathcal{A}$ over $\mathbb{Z}$, we write $\mathrm{CM}(\mathcal{O}, \mathcal{A})$ for the set of points of $X(\mathcal{O})$ having complex multiplication by $\mathcal{A}$.

Proposition 7. *A point $z \in X(\mathcal{O})$ is elliptic iff it has complex multiplication by a imaginary quadratic order isomorphic to one of the two quadratic orders $\mathbb{Z}[\sqrt{-1}]$ or $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$.*

Proof. The elements $\gamma \in \mathcal{O}$ fixing $z \in \mathcal{H}/\mathcal{O}$ are entire over $\mathbb{Z}$ and of finite order, and therefore of order 2, 3, 4 or 6 in an imaginary quadratic field. $\lhd$

Proposition 8. *Let $\mathcal{A}, \mathcal{A}' \subset \mathcal{O}$ be two imaginary quadratic orders. The CM points associated with $\mathcal{A}$ and $\mathcal{A}'$ coincide iff $\mathcal{A}'$ is conjugated to $\mathcal{A}$ by an inner automorphism of $\mathcal{O}$: $\mathcal{A}' = x^{-1}\mathcal{A}x$ for $x \in \mathcal{O}^{\times +}$.*

Proof. Assume $\mathcal{A}' = x^{-1}\mathcal{A}x$. Let z be a fixed point of $\mathcal{A}$: $\eta(a)z = z$ for $a \in A$. Then, for $a' = x^{-1}ax \in \mathcal{A}'$, $\eta(a')(\eta(x^{-1})z) = \eta(x^{-1})z$, so that $x^{-1}z$ has complex multiplication by $\mathcal{A}'$.

Conversely, assume that two quadratic orders $\mathcal{A}$, $\mathcal{A}'$ have conjugate fixed points $z, z' = \sigma z$. Replacing $\mathcal{A}'$ by $\sigma\mathcal{A}'\sigma^{-1}$, we may assume that $z = z'$. We then use Prop. 1 to conclude. $\lhd$

2.2.1 Examples.

Let B_6 be the quaternion algebra over $\mathbb{Q}$ ramified at the primes 2 and 3: for example, $B_6 = \left(\frac{2,3}{\mathbb{Q}}\right)$. Let $i, j \in B_6$ such that $i^2 = 2$, $j^2 = 3$, $ij + ji = 0$. A maximal order of B_6 is $\mathcal{O} = \langle 1, i, \frac{1+i+j}{2}, \frac{j+ij}{2} \rangle$. We fix the real quadratic field $K = \mathbb{Q}(\sqrt{2}) \subset B_6$ which gives the embedding

$$\eta : B_6 \longrightarrow \mathbb{R}^{2\times 2}, i \longmapsto \begin{pmatrix} \sqrt{2} & \\ & -\sqrt{2} \end{pmatrix}, j \longmapsto \begin{pmatrix} & 3 \\ 1 & \end{pmatrix}, ij \longmapsto \begin{pmatrix} & -3\sqrt{2} \\ \sqrt{2} & \end{pmatrix}. \tag{2}$$

Let $\alpha = \frac{i+3ij}{2}$; then we check that $\alpha^2 = -13$, so that $\mathbb{Q}(\alpha) \simeq \mathbb{Q}(\sqrt{-13}) \subset B_6$. We have $\eta(\alpha) = \frac{\sqrt{2}}{2}\begin{pmatrix} 1 & -9 \\ 3 & -1 \end{pmatrix}$, so that the fixed point of $\mathbb{Q}(\alpha)$ is the image in $X(\mathcal{O})$ of $z(\alpha) = \frac{1+\sqrt{-26}}{3}$.

Let $\beta = \frac{i+ij}{2}$; then $\beta^2 = -1$, so that $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{-1}) \subset B_6$. We have $\eta(\beta) = \frac{\sqrt{2}}{2}\begin{pmatrix} 1 & -3 \\ 1 & -1 \end{pmatrix}$, so that the fixed point of $\mathbb{Q}(\beta)$ is the image in $X(\mathcal{O})$ of $z(\beta) = 1 + \sqrt{-2}$.

Unramified case. Let $B_1 = (1, 1/\mathbb{Q}) = \mathbb{Q}^{2\times 2}$ be the split quaternion algebra over $\mathbb{Q}$. We write $i = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$, $j = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$, $ij = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$, so that $i^2 = j^2 = 1$ and $(ij)^2 = -1$. Let $\mathcal{O}(N) = \langle 1, \frac{1+i}{2}, \frac{N+1}{2}j, \frac{j+ij}{2} \rangle$. We check that $\mathcal{O}(N)$ is an order of B_1. Its image $\eta(\mathcal{O}(N))$ is the congruence group $\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), c \equiv 0 \pmod{N} \right\}$. Therefore, the Shimura curve $X(\mathcal{O}(N))$ is the classical modular curve $X_0(N)$.

Let $d \in \mathbb{Z}$ and $\delta = \frac{d+1}{2}i + \frac{d-1}{2}ij \in \mathcal{O}$. The fixed point of $\eta(\delta) = \begin{pmatrix} & d \\ 1 & \end{pmatrix}$ in $\mathcal{H}$ is $z = \sqrt{d}$, which is imaginary if $d < 0$.

3 In characteristic p: supersingular points

Let A be an abelian surface defined over the field k, with quaternionic multiplication by the indefinite algebra B, *i.e.* equipped with an (injective) morphism $B \hookrightarrow R = \operatorname{End} A \otimes \mathbb{Q}$.

Théorème 9. *Let A be an abelian surface over k, with QM by the indefinite quaternion algebra B. Then either* *(i)* *A is isogenous to the square* E^2 *of an elliptic curve, or*

(ii) *A is simple and* $\operatorname{End}_{\mathbb{Q}} A = B$.

If A is not simple, then A is isogenous to a product $E_1 \times E_2$ of two elliptic curves. If $E_1 \nsim E_2$ then since $R = \operatorname{End}_{\mathbb{Q}} E_1 \times \operatorname{End}_{\mathbb{Q}} E_2$, we have at least one injection $B \hookrightarrow \operatorname{End}_{\mathbb{Q}} E_i$, so that the curve E_i is supersingular. However, in this case, the endomorphism ring of E_1 is the quaternion algebra $B_{p,\infty}$ ramified at $\{p, \infty\}$. Since $B_{p,\infty}$ is a definite quaternion algebra, we have $B \neq B_{p,\infty}$, which is impossible. This proves that $E_1 \sim E_2$.

We therefore have $A \sim E^2$ and $R = \operatorname{End}_{\mathbb{Q}} A = (\operatorname{End}_{\mathbb{Q}} E)^{2\times 2}$. Let $C = \operatorname{End}_{\mathbb{Q}} E$. If $C = \mathbb{Q}$ then $R = \mathbb{Q}^{2\times 2}$ is a (split) quaternion algebra over $\mathbb{Q}$ and there exists a map $B \to R$ iff $B = R$. If C is an imaginary quadratic field then it must split B. The last case is when C is the quaternion algebra $B_{p,\infty}$. We can show that, for any indefinite quaternion algebra B and any prime p, there exists an embedding $B \hookrightarrow (B_{p,\infty})^{2\times 2}$.

If A is simple, then its endomorphism algebra $R = \operatorname{End}_{\mathbb{Q}} A$ is a simple algebra. Let K be the center of R. Since $\dim A = 2$, the field K is an extension of $\mathbb{Q}$ of degree 1, 2 or 4.

If $[K : \mathbb{Q}] = 4$ then $R = K$ and R is commutative, which is impossible since $B \subset R$.

If $K = \mathbb{Q}$ then, since R is central simple over $\mathbb{Q}$, it is a quaternion algebra over $\mathbb{Q}$, hence $R = B$.

If K is a real quadratic field, then R is a quaternion algebra over K, containing B and therefore $B \otimes K$. Since A is simple, R is not split over K. Therefore, K does not split B, and R contains a real quadratic extension K' of K, which is therefore a totally real quartic extension of $\mathbb{Q}$. By [Mumford, Corollary p. 191], this implies that $4 \mid \dim A$, which is impossible.

Assume that K is an imaginary quadratic field. Then since R is a quaternion algebra over K containing B, we can show that $R = B \otimes_{\mathbb{Q}} K$.

We can show that this last case may only happen when the base field k has characteristic $p > 0$. $\operatorname{End}_{\mathbb{Q}} A$ contains a CM quartic field L. If $p = 0$ then A would have its endomorphism ring equal to the CM field L; this impossible since $\operatorname{End}_{\mathbb{Q}} A$ is not commutative.

Let $\mathfrak{q}$ be a place of K that does *not* divide p. XXX (by Honda-Tate?) Then $\mathfrak{q}$ is split in R: $R \otimes_K K_{\mathfrak{q}} \simeq K_{\mathfrak{q}}^{2\times 2}$. Since R is a division algebra, it is not split at all places of K, and is therefore ramified at the two places $\mathfrak{p}, \mathfrak{p}'$ dividing p. This means that the discriminant of R over K is $\mathfrak{p}\mathfrak{p}' = p$.

Assume that p does not divide the discriminant of $B/\mathbb{Q}$. Then the embedding $B \hookrightarrow R$, when tensoring by $\mathbb{Q}_p$, gives an embedding

$$B \otimes_{\mathbb{Q}} \mathbb{Q}_p = \mathbb{Q}_p^{2\times 2} \quad \hookrightarrow \quad R \otimes_{\mathbb{Q}} \mathbb{Q}_p = R \otimes_K (K_{\mathfrak{p}} \oplus K_{\mathfrak{p}'}). \tag{3}$$

Since the algebra $\mathbb{Q}_p^{2\times 2}$ has nilpotent elements while $R_{\mathfrak{p}} \oplus R_{\mathfrak{p}'}$ does not, this is a contradiction.

Therefore, p divides $\operatorname{disc} B/\mathbb{Q}$. This means that $B \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a division algebra. The Tate module $T_p(A)$ has dimension 0, 1 or 2. The map $B \hookrightarrow \operatorname{End}_{\mathbb{Q}}(A)$ then gives a map $\rho : B \otimes \mathbb{Q}_p \to \operatorname{End}_{\mathbb{Q}_p}(T_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$. If $T_p(A) \neq 0$, then $\rho(1) = 1$ and ρ is therefore injective. This gives an embedding $B_p \hookrightarrow \mathbb{Q}_p^{i\times i}$ for $i \leqslant 2$, which is impossible.