Appendix A. The role of the splitting field

This appendix contains some more information about the fields of definition of Shimura congruence curves of prime power level.

THEOREM 6. *Under the assumptions of Lemma 8, but with the possible exception of the case* $\Delta = \Delta(3,4,6)$, $M(S)$ *is the* splitting field *of* p *in* k, *that is the fixed field of all* $\sigma \in \mathrm{Gal}\, k/\mathbb{Q}$ *fixing the prime ideals* $\mathfrak{p}_j \mid p$. *The action of the absolute Galois group on these principal congruence subgroup Shimura curves is the same as the action on the level ideals: if the principal congruence subgroup* $\Delta(\mathfrak{p}^n)$ *is the surface group of* $S := S_{\mathfrak{p}^n}$, $\Delta(\sigma(\mathfrak{p}^n))$ *is the surface group* $\Delta(\mathfrak{p}^n)_\sigma$ *of* S^σ. *The field of moduli* $M(S)$ *coincides with the field of moduli* $M(\mathcal{D})$ *of the maximal regular dessin on* S.

This splitting field can also be considered as the smallest subfield of k (of degree g) in which p splits in g prime ideals (in this splitting field necessarily of residue class degree 1).

PROOF. 1. With Lemma 7, the result clearly extends from $\mathfrak{p}$ to all prime power levels $\mathfrak{p}^n$, so we will consider only the case $n = 1$. Another simplification comes from Lemma 1: since Δ is maximal, we have in fact $M(\mathcal{D}) = M(S)$. So it is sufficient to care about $M(S)$.

2. As a preparatory step, we need to learn more about the full automorphism group $G := \Delta/\Delta(\mathfrak{p})$ of $S := S_{\mathfrak{p}}$. All triangle groups in question are either the norm 1 groups Φ mentioned in Lemma 8 or extensions of them of degree 2 or 4. In a few cases, Φ is not a triangle group itself but a quadrangle group. The extensions are generated by integer elements $\delta \in A$ of totally positive norm $\nu \in k$, either a prime dividing the discriminant $D(A)$ or a non–square unit of k. The arithmetic in A implies that δ normalizes congruence subgroups $\Delta(\mathfrak{p})$ as well. If q denotes the norm $N(\mathfrak{p})$ and if Δ is generated by Φ and δ, then $\Phi/\Delta(\mathfrak{p}) \cong \mathrm{PSL}(2,\mathbb{F}_q)$ and $\Delta/\Delta(\mathfrak{p}) \cong \mathrm{PSL}(2,\mathbb{F}_q) \times C_2$ or $\cong \mathrm{PGL}(2,\mathbb{F}_q)$ depending on the alternative whether the (reduced quaternion) norm $N(\delta) \bmod \mathfrak{p}$ is a square in $\mathbb{F}_q$ or not. If Δ is an index 4 extension of Φ, the quotient $\Delta/\Delta(\mathfrak{p})$ is $\cong \mathrm{PSL}(2,\mathbb{F}_q) \times C_2 \times C_2$ or $\cong \mathrm{PGL}(2,\mathbb{F}_q) \times C_2$ by a similar argument (we learned this idea from A. Džambić).

3. By the arguments already used in the proof of Lemma 8, we know that the quasiplatonic surfaces $S_{\mathfrak{p}_j}$, $j = 1,\ldots,g$, form a family $\mathcal{F}$ invariant under the action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}})$, so the splitting number g is an upper bound for the length of the Galois orbit of S. We can suppose that all these surfaces are equipped with the dessins induced by the maximal triangle group $\Delta \triangleright \Phi \triangleright \Delta(\mathfrak{p}_j)$ of signature (r,s,t). Let $\mathfrak{p}$ be one of these prime ideals. Let G be the automorphism group of $S := S_{\mathfrak{p}}$, generated by the elements g_0, g_1, g_∞ of respective orders r,s,t, images of the canonical generators $\gamma_0, \gamma_1, \gamma_\infty$ of Δ under the canonical epimorphism

$$h \,:\, \Delta \,\to\, \Delta/\Delta(\mathfrak{p}) \,\cong\, G\,.$$

If g_1, say, has a fixed point $P \in S$ and acts in suitable local coordinates on a neighbourhood of P like

$$g_1 \,:\, z \,\mapsto\, \zeta_s^v \cdot z \quad ,$$

we call ζ_s^v the *multiplier* of g_1 in P. Clearly, v is coprime to s. The collections of all pairs

$$(\zeta_r^u, n_{r,u})\,, \quad (\zeta_s^v, n_{s,v})\,, \quad (\zeta_t^w, n_{t,w})$$

are called the *multiplier data* of (G, g_0, g_1, g_∞) on S where we denote by $n_{r,u}$ the number of all fixpoints of g_0 on S with multiplier ζ_r^u, and so on.

4. As next step we show how the action of the absolute Galois group on the family $\mathcal{F}$ induces an action on the multiplier data. For all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}})$ the multiplier data of $(G^\sigma, g_0^\sigma, g_1^\sigma, g_\infty^\sigma)$ arise from the original ones by an obvious action of σ on the multipliers, see [**4**] or [**3**]. We can simplify the consideration of this Galois action on the multiplier data in two ways. First, we can neglect all multipliers with (say) $r = 2$ because $\mathrm{Gal}(\overline{\mathbb{Q}})$ acts trivially on $\zeta_2 = -1$. Second, we can exclude all primes p from the consideration in our theorem which divide one of the entries of the signature of Δ: a case–by–case analysis of all 19 triangle groups in question (see Table (3) of [**5**]) shows that this possibility occurs only if p and the discriminant ideal $D(A)$ of the algebra have a nontrivial common divisor or – much more often – if the splitting number of p in k is $g = 1$, so Corollary 2 applies. Instead of a tedious list we give two typical examples.

a) $\Delta = \Delta(2, 5, 6)$ with $k = \mathbb{Q}(\sqrt{5})$. Here, 2 divides the discriminant of the algebra, 3 is inert and 5 is ramified.

b) $\Delta = \Delta(2, 5, 30)$ with $k = \mathbb{Q}(\cos\frac{\pi}{15})$, the maximal real subfield of $\mathbb{Q}(\zeta_{15})$, is a bit more complicated. The prime 3 divides the discriminant $D(A)$. The Galois group of $\mathbb{Q}(\zeta_{15})/\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/15\mathbb{Z})^* \cong \{\pm 1 \bmod 15\} \times \{1, 2, 4, 8 \bmod 15\}$, and k is the fixed field of the first factor, and therefore

$$\mathrm{Gal}(k/\mathbb{Q}) \;\cong\; (\mathbb{Z}/15\mathbb{Z})^*/\{\pm 1\} \;\cong\; \{1, 2, 4, 8 \bmod 15\} \quad .$$

This second factor is generated by the Frobenius automorphism for the prime 2, so this prime is inert in k. Finally, the prime 5 is totally ramified already in the subfield $\mathbb{Q}(\zeta_5)$ and inert in the subfield $\mathbb{Q}(\zeta_3)$, hence it has in $\mathbb{Q}(\zeta_{15})$ the decomposition $5\mathbb{Z}[\zeta_{15}] = \mathfrak{P}^4$ with one prime ideal $\mathfrak{P} < \mathbb{Z}[\zeta_{15}]$ of residue degree 2. Because the splitting number of 5 is $g = 1$ in $\mathbb{Q}(\zeta_{15})$, it is also 1 in its subfield k.

The primes not dividing the signature entries have the advantage that they cannot belong to *parabolic* generators of $\mathrm{SL}(2, \mathbb{F}_q)$ or $\mathrm{GL}(2, \mathbb{F}_q)$; these are the only ones having eigenvalues of multiplicity 2. So, for the other primes p our generators g_i (that is g_0, g_1 or g_∞) are non–parabolic, therefore g_i is conjugate in G to $g_i^{\pm 1}$ but to no other power of g_i – an easy consequence of the structure of $\mathrm{SL}(2, \mathbb{F}_q)$ and $\mathrm{GL}(2, \mathbb{F}_q)$, compare the eigenvalues of their matrices and the respective arguments already used in [**4**] and [**2**]. By construction of (say) $g_i = g_\infty = h(\gamma_\infty)$ by means of the canonical epimorphism h, the fixpoint $u \in \mathbb{H}$ of γ_∞ gives at least one fixpoint $P = \Delta(\mathfrak{p})u \in S = \Delta(\mathfrak{p})\backslash\mathbb{H}$ with multiplier ζ_t. Now suppose that g_∞ fixes another point $Q \in S$, then this is a fixed point of the same order because Δ is maximal and so the orders of the generators of G (the signature entries) are pairwise different. So, Q and P are both face centers of the dessin (or vertices of the same colour in the cases $i = 0, 1$). By the transitivity of G there is an automorphism $a \in G$ with $a(P) = Q$, therefore $a^{-1} g_\infty a$ fixes P as well, hence is conjugate to a power of g_∞, and we know that here $g_\infty^{\pm 1}$ are the only possible powers. Since the multiplier of g_∞ in Q is the same as that of $a^{-1} g_\infty a$ in P, it has to be $\zeta_t^{\pm 1}$. The only possible contribution of g_∞ to the multiplier data are therefore the pairs

$$(\zeta_t, n_{t,1}) \qquad \text{and} \qquad (\zeta_t^{-1}, n_{t,-1}) \quad .$$

In the following, we will therefore always assume (without loss of generality, see above) that p is coprime to r, s, t. As a consequence, p is unramified in all cyclotomic fields in question, hence also unramified in k, see the next step of the proof.

5. By the same proof as in [**4**] we can moreover see that $n_{t,1} = n_{t,-1}$: consider the canonical representation ψ of G on the space of holomorphic differentials of S. Since g_∞ is conjugate to g_∞^{-1}, and since

$$\operatorname{tr}\psi(g_\infty) \;=\; \operatorname{tr}\psi(g_\infty^{-1}) \;=\; \operatorname{tr}\psi(g_\infty)^{-1} \;=\; \overline{\operatorname{tr}\psi(g_\infty)}\,,$$

$\psi(g_\infty)$ has a real trace. On the other hand, Eichler's trace formula

$$\operatorname{tr}\psi(g_\infty) \;=\; 1 + n_{t,1}\,\frac{\zeta_t}{1-\zeta_t} + n_{t,-1}\,\frac{\zeta_t^{-1}}{1-\zeta_t^{-1}}$$

gives a real value if and only if $n_{t,1} = n_{t,-1}$, so the multiplier system is invariant under complex conjugation. Obviously, the action of $\mathrm{Gal}(\overline{\mathbb{Q}})$ on the multiplier data corresponds therefore to the action on $\mathbb{Q}(\cos\frac{2\pi}{r}, \cos\frac{2\pi}{s}, \cos\frac{2\pi}{t})$, and this is precisely the center field k of the quaternion algebra A for all maximal arithmetic triangle groups except $\Delta(3,4,6)$. This can again be seen via a case–by–case analysis along the lines of Takeuchi's Table (3) in [**5**]. Two consequences are important: first, $k < \mathbb{Q}(\zeta_r, \zeta_s, \zeta_t)$, therefore (by the assumptions justified in step 4 of the proof) p is also unramified in k; in other words, the exponent $e = 1$ in the prime decomposition of Lemma 8. Second, on S^σ the contribution of the Galois conjugate generator g_∞^σ with $\sigma(\zeta_t) = \zeta_t^w$ to the multiplier data is $(\zeta_t^w, n_{t,1})$, $(\zeta_t^{-w}, n_{t,1})$. Together with the analogous facts for the other generators and with $\zeta_t + \zeta_t^{-1} = 2\cos(\frac{2\pi}{t})$ the action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}})$ on the multiplier data gives an orbit of length $[k:\mathbb{Q}]$.

6. In general, this orbit length is however not the orbit length of the action of $\mathrm{Gal}(\overline{\mathbb{Q}})$ on the family $\mathcal{F}$ of the Shimura congruence curves $S_{\mathfrak{p}_j}$, $j = 1, \ldots, g$: if we consider again the canonical homomorphism $h : \Delta \to G = \Delta/\Delta(\mathfrak{p}) = \mathrm{Aut}\,S$, we get in fact at least $[k:\mathbb{Q}]$ different epimorphisms $\sigma \circ h$, but their kernels coincide if and only if they differ by composition with an automorphism of G. (Here we use again the hypothesis that Δ is maximal, so we cannot pass to other homomorphisms by permutation of the generators.) Since we need only a lower bound for the length of the Galois orbit (remember step 3 above), it is sufficient to study these automorphisms on its commutator subgroup $[G,G] = \mathrm{PSL}(2,\mathbb{F}_q)$ or its extension $\mathrm{PGL}(2,\mathbb{F}_q)$ – the generators of the possible C_2 factors are anyway irrelevant for the Galois action, see step 4. The automorphisms of these matrix groups over $\mathbb{F}_q$ are composed by

- matrix conjugations leaving eigenvalues and traces invariant – so they leave invariant the multipliers – and
- Galois conjugations by $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ acting on the matrix coefficients and hence also on the eigenvalues.

If $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}})$ induces this second kind of automorphism of G, it sends therefore a generator $g_i \in G$, $i = 0, 1, \infty$, to another element conjugate to some power $g_i^{\pm w}$ where w is some p–power (here and in the following neglecting possible C_2 factors, see above).

7. This is true in the same way for the g_i as matrices over $\mathbb{F}_q$ and for the g_i as automorphisms of S. In the fist version, σ induces an action on their eigenvalues

in the finite fields $\mathbb{F}_{p^m}$, in the second version an analogous action

$$\zeta_i + \zeta_i^{-1} \;\mapsto\; \zeta_i^w + \zeta_i^{-w} \;, \quad w \quad \text{a } p\text{–power},$$

where ζ_i denotes the multiplier of g_i . Clearly, if σ fixes k elementwise, it has this behaviour (with $w = \pm 1$). Recall from number theory in cyclotomic fields that the *Frobenius subgroup* of $\mathrm{Gal}(\mathbb{Q}(\zeta_i)/\mathbb{Q})$ consisting of all

$$\sigma \;:\; \zeta_i \;\mapsto\; \zeta_i^w \;, \quad w \quad \text{a } p\text{–power},$$

is precisely the maximal subgroup fixing the prime ideals in the prime decomposition of the (unramified!) rational prime p . Its fixed field is the splitting field of p in $\mathbb{Q}(\zeta_i)$. Using this fact for all three cyclotomic fields $\mathbb{Q}(\zeta_i)$, the restriction to k is an exercise in Galois theory and shows

$$\{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}) \mid S \cong S^\sigma\} \;\leq\; U_p \;:=\; \{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}) \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}$$

(U_p depending only on k and p , not on the choice of $\mathfrak{p}$ among the $\mathfrak{p}_j$ because k is abelian). The orbit of $\mathrm{Gal}(\overline{\mathbb{Q}})$ on the family $\mathcal{F}$ has therefore at least length $|\mathrm{Gal}(\overline{\mathbb{Q}}) : U_p|$, and since the splitting field $K_p \leq k$ of p is the fixed field of U_p , this group index is the field degree $[K_p : \mathbb{Q}] = g$. Together with the upper bound for the Galois orbit given in Lemma 8 we see therefore that K_p is in fact the field of moduli – hence also the minimal field of definition – of S .

8. As a side result, we see also that the multiplier data determine uniquely the curves of the family $\mathcal{F}$. Therefore, Proposition 3 of [**3**] shows that the actions of $\mathrm{Gal}(\overline{\mathbb{Q}})$ on $\mathcal{F}$, their multiplier data, and their corresponding prime ideals $\mathfrak{p}_j$ are compatible. □

Remark 3. *Step 5 of the proof above fails for* $\Delta = \Delta(3,4,6)$ *because the centre field* $k = \mathbb{Q}(\sqrt{6}) \neq \mathbb{Q}(\cos\frac{2\pi}{r}, \cos\frac{2\pi}{s}, \cos\frac{2\pi}{t}) = \mathbb{Q}$ *. Moreover, the minimal cyclotomic field containing* k *is generated by the 24–th root of unity* ζ_{24}*, hence has degree* 4 *over* k *. Therefore, no group commensurable with* Δ *can contain a torsion element* γ *of order* $m \neq 2,3,4,6$ *because otherwise we would have a cyclotomic subfield* $k(\gamma) \cong k(\zeta_m) < A$ *, and this can have at most degree* 2 *over* k *because* A *cannot contain larger commutative subfields.*

Is it possible that in this case all $S_\mathfrak{p}$ *are defined over* $\mathbb{Q}$ *? No: by the quadratic reciprocity law, rational primes* p *split in* k *if and only if* $p \equiv \pm 1$ *or* $\pm 5 \bmod 24$ *. The first example* $p = 5$ *,* $\mathfrak{p} = (1 \pm \sqrt{6})\mathcal{O}_k$ *gives two Galois conjugate curves of genus* 16 *with field of moduli* k *, see the (quite different) proof in* [**1**].

References

[1] Conder, M.D.E., Jones, G.A., Streit, M., Wolfart, J.: *Galois actions on regular dessins of small genera*, Revista Mat. Iberoamericana 29 (2013), 163–181.

[2] Feierabend, F.: *Galois–Operationen auf verallgemeinerten Macbeath–Hurwitz Kurven,* PhD thesis, Frankfurt 2008.

[3] Jones,G.A., Streit, M., Wolfart, J., *Wilson's map operations on regular dessins and cyclotomic fields of definition,* Proc. London Math. Soc. 100 (2010), 510–532.

[4] Streit, M., *Field of definition and Galois orbits for the Macbeath–Hurwitz curves,* Arch. Math. 74 (2000) 342–349.

[5] Takeuchi, K., *Commensurability classes of arithmetic triangle groups,* J. Fac. Sci. Univ. Tokio, Sect. 1A Math. (1) **24** (1977), 201–212.