Appendix B

Fields of Low Characteristic

Certain propositions about \( C(r, d) \) that are trivial when \( \text{char}(K) = 0 \) or \( \text{char}(K) > k \) become false or, if true, need extra arguments in low non-zero characteristics. This Appendix contains proofs of these properties.

**Lemma B.0.1.** Suppose \( d \in K^* \) and \( a \in K^* \). Then

\[
\hat{\varphi}(a) := \begin{cases} 
[0, a, 0, 0, 4a^{-2}d] & \text{Tetrahedron}, \\
[0, a, 0, 0, 12a^{-1}d, 0] & \text{Octahedron}, \\
[0, a, 0, 0, 0, \frac{144d}{r}, 0, 0, 0, -a^{-1}(144d)^2, 0] & \text{Icosahedron}
\end{cases}
\]

is an element of \( C(r, d)(K) \). In particular \( C(r, d)(K) \neq \emptyset \).

**Proof.** This is verified by calculation.

**Proposition B.0.2.** Suppose \( K \) is a field and \( 2, d \in K^* \). If \((X, Y, Z) \in D(r, d) - (0, 0, 0)\), there is a \( \varphi \in C(r, d)(K) \) so that \( \pi(\varphi) = (X, Y, Z) \).

**Proof.** If \( Z = 0 \), we let \( \varphi := \hat{\varphi}(-X/Y) \), where \( \hat{\varphi} \) is the function defined in Lemma B.0.1. One checks that \( \pi(\varphi) = (X, Y, Z) \).

If \( Z \neq 0 \), define

\[
\varphi := [Z, 0, \frac{Y}{Z}, \frac{2X}{Z}, \ldots],
\]

where the omitted terms are uniquely determined by the first \( k - 3 \) defining equations of \( C(r, d) \). The coefficients of \( \varphi \) can be expressed as elements in the ring \( \mathbb{Z}[X, Y, Z, Z^{-1}] \). With the help of PARI we get the algebraic identities

\[
\tau_4(\varphi) = 0, \quad 7\tau_6(\varphi) = -360 \left( \frac{X^2 + Y^3}{Z^5} \right), \\
7\tau_{12}(\varphi) = 3110400 \left( \frac{X^2 + Y^3}{Z^5} \right)^2,
\]

when \( r = 5 \), and similar identities when \( r = 3, 4 \). This shows that \( \varphi \) is a ‘generic’ lift of the element \((X, Y, Z)\). The result follows.
Proposition B.0.3. Suppose $K$ a field and $d \in K^*$ then

$$\varphi \in C(r,d) \Rightarrow \lambda g \cdot \varphi \in C(r,d'),$$

where $d' = \lambda^{6-r} \det(g)^{-6} d$.

Proof. The claim about multiplication by $\lambda \in K^*$ is clear by examining the defining equations of $C(r,d)(K)$. Furthermore, any $g \cdot f$ can be written as $g \cdot f = \lambda g' \cdot f$ with $g' \in SL_2(K)$ and $\lambda \in K^*$ satisfying $\lambda^{6-r} = \det(g)^6$. Therefore we can assume $g \in SL_2(K)$.

We are left to show that if $g \in SL_2(K)$ and $\varphi \in C(r,d)(K)$ then $g \cdot \varphi \in C(r,d)$. The subsets of the equations defining $C(r,d)$ that are equivalent to the vanishing of a polynomial combination of covariants of $\varphi$, necessarily remain valid by the definition of a covariant. This is true for all equations, except the equations derived from the coefficients of the 4th covariant $\tau_4(\varphi)$, and the icosahedral equation labelled $D_4^*$. The equations obtained by requiring that $\tau_4$ vanish remain valid after an $SL_2(K)$ substitution because of the covariance of $\tau_4$. However, there is an added complication since the equations for $C(r,d)$ are obtained from the coefficients of $\tau_4(f)$ after dividing out by their content. Let $V$ be the algebraic set defined by these equations.

Note that

$$\begin{pmatrix} \kappa & 0 \\ 0 & \kappa^{-1} \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & \nu \\ 0 & 1 \end{pmatrix},$$

where $\kappa \in K^*$ and $\nu \in K$, generate $SL_2(K)$. By inspection $V$ is closed under the action of the first two generators. A calculation (e.g. with the help of a computer package) shows that it is also closed under the action of the last generator.

Finally, we must check the equations remain closed under $SL_2(K)$-substitutions if we also require that $D_4^*$ is satisfied in the icosahedral case. This is also done by checking the claim on the generators (B.1) of $SL_2(K)$.

Lemma B.0.4. Suppose $d \in K^*$ and $\varphi \in C(r,d)(\bar{K})$. Then there is a $g \in SL_2(\bar{K})$ so that $a_0(g \cdot \varphi) = 0$. If $N \in K^*$, there is a $g \in SL_2(K)$ so that $g \cdot \varphi = [0, 1, 0, \ldots]$.

Proof. Let $f := f(\varphi)$. We can find $g \in SL_2(\bar{K})$ so that the binary form $g \cdot f$ has a zero at $\infty$. Since $\varphi \mapsto f(\varphi)$ is $SL_2(\bar{K})$-equivariant we have $a_0(g \cdot \varphi) = 0$.

If $N \in K^*$, $f$ has no multiple roots, as the discriminant of $f$ is non-zero. Therefore, by equivariance, $a_1(g \cdot \varphi) \neq 0$. Twisting with an $SL_2(K)$ matrix of the shape $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ allows us to suppose $g \cdot \varphi = [0, 1, 0, \ldots]$. \hfill $\square$
Lemma B.0.5. Suppose $N, d \in K^*$. Then $C(r, d)(\bar{K})$ is a homogeneous $SL_2(\bar{K})$-space and $C(r)(\bar{K})$ is a homogeneous $GL_2(\bar{K})$-space.

Proof. Suppose $\varphi \in C(r, d)(\bar{K})$. By Lemma B.0.4, we can assume that $\varphi = [0, 1, 0, \ldots]$. However, as $N \in K^*$, the missing coefficients are determined by the defining equations of $C(r, d)$. We have shown that there is a single element of $C(r, d)$ to which every $\varphi \in C(r, d)$ is $SL_2(\bar{K})$-equivalent. This means that $C(r, d)(\bar{K})$ is a homogeneous $SL_2(\bar{K})$-space. As a corollary $C(r)(\bar{K})$ is a homogeneous $GL_2(\bar{K})$-space.

Remark B.0.6. Lemma B.0.5 is not true without some restrictions on the characteristic of $K$. For instance, if $K$ has char$(K) = 2$ then $[0, 1, 0, 0, 1]$ and $[0, 1, 0, 1, 0]$ are elements of $C(3, 1)(K)$. These lie in distinct $SL_2(\bar{K})$-orbits, since being of the shape $[0, *, 0, *, 0]$ is an $SL_2(\bar{K})$-invariant property.

Proposition B.0.7. Suppose $K$ is a field and $N \in K^*$. Suppose $(X, Y, Z) \in D(r, d) - (0, 0, 0)$. If $\varphi \in C(r, d)(K)$ and $\pi(\varphi) = (X, Y, Z)$ then there is a unique parabolic $g \in SL_2(K)$ so that

$$g \cdot \varphi := \begin{cases} [Z, 0, Y, 2X, \ldots] & \text{if } Z \neq 0, \\ [0, -X/Y, 0, \ldots] & \text{if } Z = 0, \end{cases}$$

where the omitted terms are uniquely determined by the defining equations of $C(r, d)$.

Proof. (Existence) Since $N \in K^*$, there is a parabolic $g \in SL_2(K)$ so that the $\varphi$ has the shape $[* , 0 , \ldots]$ if $Z \neq 0$, and $[0, *, 0, \ldots]$ if $Z = 0$. Since $\pi(\varphi) = \pi(g \cdot \varphi) = (X, Y, Z)$, the initial coefficients of $\varphi$ agree with the coefficients in the announcement of the proposition. The defining equations of $C(r, d)$ determine the rest of $\Omega_r$.

(Uniqueness) Suppose $\varphi$ has the canonical form given. Since $N \in K^*$, there is no non-zero parabolic $g \in SL_2(K)$ that fixes $\varphi$.

Lemma B.0.8. If $N, d \in K^* \neq 0$ and $\varphi \in C(r, d)$ then $\#\Gamma(\varphi) = 2N$. Furthermore, if $\varphi$ corresponds to the coefficients of one of the forms chosen in § 4.3, then the explicit description of the group given in § 4.3 is the group $\Gamma(\varphi)(\bar{K})$.

Proof. Since $N \in K^*$, the space $C(r)(\bar{K})$ is a homogeneous $GL_2(\bar{K})$-space by Lemma B.0.5. This means that we can assume that $\varphi$ corresponds to one of the Klein forms mentioned in § 4.3. Let $\Gamma'$ denote the group of symmetries mentioned in § 4.3, and $\Gamma := \Gamma(\varphi)$ the full group of symmetries. Clearly $\Gamma' \subset \Gamma(\varphi)$. Indeed, the set of equations witnessing the truth of the statement $\Gamma' \subset \Gamma(\varphi)$ in $\bar{Q}$ can be written as a set of polynomial equations in the ring generated by $Z$ and the entries of elements of $\Gamma'$. These identities remain valid in the field $K$. 


APPENDIX B. FIELDS OF LOW CHARACTERISTIC

Suppose that \( g \in \Gamma(\varphi) \). We will show that \( g \in \Gamma' \). Let \( f := f(\varphi) \). Calculating the discriminant we see that the roots of \( f \) are distinct if \( N, d \in K^* \). Since \( \Gamma' \) is transitive on the roots of \( f \), we can multiply \( g \) by an element of \( \Gamma' \) and assume that \( g \) fixes the root at \( \infty \). Therefore, \( g = \left( \begin{array}{cc} \kappa & \nu \\ 0 & \kappa^{-1} \end{array} \right) \) for some \( \kappa \in K^* \), \( \nu \in K \). Since \( \varphi = [0, *, 0, \ldots] \) and \( N \in K^* \) we calculate that \( \nu = 0 \). The matrix \( g \) is diagonal and we deduce that \( g \in G' \). Conclusion: \( \Gamma(\varphi) = \Gamma' \).

Finally, we must show that \( \#\Gamma' = 2N \). I.e. that \( \Gamma' \) has no kernel when we reduce from \( \text{SL}_2(\overline{\mathbb{Q}}) \) to \( \text{SL}_2(\overline{K}) \). Let \( f := f(\varphi) \). Suppose \( g \in \Gamma'(\overline{\mathbb{Q}}) \) is not \( \pm I \). Then \( g \) induces a non-trivial permutation of the roots of \( f \in \overline{\mathbb{Q}}[x, y] \). As \( N, d \in \overline{K} \), we have \( \text{disc}(f) \neq 0 \), so the roots of \( f \) remain distinct in \( \overline{K} \). Therefore the kernel is contained in \( \{\pm I\} \). As \( 2 \in \overline{K} \), the matrix \(-I\) is not in the kernel. Conclusion: \( \#\Gamma(\varphi)(\overline{K}) = \#\Gamma(\varphi)(\overline{\mathbb{Q}}) = 2N \).

Remark B.0.9. Consider \( \varphi = [0, 144, 0, 0, 0, 0, 0, 0, 0, -144, 0] \). We have \( f := f(\varphi) = 1728d \, xy(x^{10} + 11x^5y^5 - y^{10}) \)

Suppose \( K \) is a field with \( \text{char}(K) = 11 \). Then \( f \) has distinct roots, as the discriminant is non-zero. However, \( \Gamma(f) \) contains the cyclic group of order 11 generated by \( g := \left( \begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right) \). This means that \( \Gamma(f) \neq \Gamma(\varphi) \). Set \( \varphi' := g \cdot \varphi \). Then \( \varphi, \varphi' \) are distinct elements of \( C(5, d) \) with \( f(\varphi) = f(\varphi') \).