JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Yuval Z. FLICKER

Conjugacy classes of finite subgroups of $\mathrm{SL}(2, F)$, $\mathrm{SL}(3, \bar{F})$

Tome 31, n° 3 (2019), p. 555-571.

<http://jtnb.centre-mersenne.org/item?id=JTNB_2019__31_3_555_0>

Journal de Théorie des Nombres
de Bordeaux **31** (2019), 555–571

Conjugacy classes of finite subgroups of $\mathrm{SL}(2, F)$, $\mathrm{SL}(3, \bar{F})$

par Yuval Z. FLICKER

Résumé. Soit F un corps. Nous déterminons les sous-groupes finis G de $\mathrm{SL}(2, F)$ dont le cardinal $|G|$ n'est pas divisible par la caractéristique de F, à conjugaison près. Dans le cas où $F = \bar{F}$ est séparablement clos, nous montrons (via des arguments de la théorie des représentations des groupes finis) que deux sous-groupes isomorphes de $\mathrm{SL}(2, F)$ sont conjugués. Nous obtenons le même résultat pour les sous-groupes finis irréductibles de $\mathrm{SL}(3, \bar{F})$. L'extension du cas séparablement clos au cas rationnel repose naturellement sur la cohomologie galoisienne. Plus précisément, nous calculons le premier groupe de cohomologie galoisienne du centralisateur C de G dans le SL en question, modulo l'action du normalisateur. Les résultats obtenus ici dans le cas semisimple simplement connexe sont différents des résultats déjà connus dans le cas du groupe adjoint $\mathrm{PGL}(2)$. Enfin, nous déterminons le corps de définition d'un tel sous-groupe fini G de $\mathrm{SL}(2, \bar{F})$, c'est-à-dire le corps minimal F_1, tel que $\overline{F_1} = \bar{F}$ et tel que le groupe fini G s'injecte dans $\mathrm{SL}(2, F_1)$.

Abstract. Let F is a field. We determine the finite subgroups G of $\mathrm{SL}(2, F)$ of cardinality $|G|$ prime to the characteristic of F, up to conjugacy. When $F = \bar{F}$ is separably closed, using representation theory of finite groups we show that isomorphic subgroups of $\mathrm{SL}(2, F)$ are conjugate. We show this also for irreducible finite subgroups of $\mathrm{SL}(3, \bar{F})$. The extension of the separably closed to the rational case is naturally based on Galois cohomology: we compute the first Galois cohomology group of the centralizer C of G in the SL, modulo the action of the normalizer. The results we obtain here in the semisimple simply connected case are different than those already known in the case of the adjoint group $\mathrm{PGL}(2)$. Finally, we determine the field of definition of such a finite subgroup G of $\mathrm{SL}(2, \bar{F})$, that is, the minimal field F_1 with $\overline{F_1} = \bar{F}$ such that the finite group G embeds in $\mathrm{SL}(2, F_1)$.

Manuscrit reçu le 19 février 2018, révisé le 8 septembre 2019, accepté le 28 septembre 2019.
2010 *Mathematics Subject Classification.* 14G05, 14G27, 14G25, 14E08.
Mots-clefs. Galois cohomology, $\mathrm{SL}(2, F)$, $\mathrm{SL}(3, F)$, algebraic classification, rational classification, representation theory.
Partially supported by the Simons Foundation grant #317731 and the Aliyah and Absorption Ministry Kamea B grant.

1. Introduction

Let F be a field. Denote by $\bar{F}$ a separable algebraic closure of F. The finite subgroups considered below are only those which have order indivisible by $\operatorname{char} F$. In other characteristics, linearly reductive finite subgroup *schemes* are classified in [9]. It is well-known (see, e.g., [7]) that the finite subgroups G of $\mathrm{SL}(2,\bar{F})$ are the cyclic group $C_r = \mathbb{Z}/r$, the binary dihedral group BD_{4r}, and the binary Platonic groups $BT_{24} = 2A_4 = \mathrm{SL}(2,3)$, $BO_{48} = 2S_4$, $BI_{120} = 2A_5 = \mathrm{SL}(2,5)$. Their orders are r, $4r$, 24, 48, 120. So $\operatorname{char} F \neq 2$ unless we consider C_r with odd r. It is also known (see, e.g., [8]) that the finite subgroups of $\mathrm{SL}(3,\bar{F})$ are (the families (A), (B), (C), (D) and) of type (C′), (D′), (E), ..., (J). *We determine in the case of* SL(2) *the finite subgroups of the group of* rational *points* $\mathrm{SL}(2,F)$ *up to conjugacy.* When $F = \bar{F}$ is separably closed, we show that isomorphic finite subgroups of $\mathrm{SL}(2,\bar{F})$ are conjugate. This follows from representation theory of finite groups. We show this also in the case of $\mathrm{SL}(3,\bar{F})$, for *irreducible* finite subgroups, and leave the questions of rationality in this dimension to another work. Note that $\langle \mathrm{diag}(1,\omega,\omega^2)\rangle$ and $\langle \omega I\rangle$, where ω is a primitive 3rd root of 1 in F and I is the identity element of $\mathrm{SL}(3,F)$, are isomorphic (to the cyclic group of order 3), but they are not conjugate in $\mathrm{SL}(3,\bar{F})$. Such rationality questions (over F) lead naturally to Galois cohomology, see [16]. The reduction of the separably closed to the rational case is naturally based on the first Galois cohomology group of the centralizer C of G in the SL, modulo the action of the normalizer. Such a question had been considered in the case of PGL(2) by Beauville [1]. We consider the semisimple simply connected SL rather than the adjoint PGL. We also determine the *field of definition* of the given finite subgroup G of $\mathrm{SL}(2,\bar{F})$, namely the minimal field F_1 with $\overline{F_1} = \bar{F}$ such that the group $\mathrm{SL}(2,F_1)$ contains the finite group G.

Acknowledgments. I warmly thank Ron Solomon and J.-P. Serre for useful correspondence, and Tokyo University IPMU for hospitality when some of this work was done.

2. Fields of definition of finite subgroups of $\mathrm{SL}(2,\bar{F})$

The question in this section is to find which of the subgroups of $\bar{S} = \mathrm{SL}(2,\bar{F})$ embed in $S = \mathrm{SL}(2,F)$ for a given field F, or alternatively, given a subgroup G of $\bar{S}$, in which S does it embed. This information is illuminating, but not required for the rest of this paper.

Proposition 2.1.

(1) *S contains C_r ($r \geq 3$) if and only if F contains $\zeta + \zeta^{-1}$ for some primitive rth root $\zeta = \zeta_r$ of 1 in $\bar{F}$. The group C_r is uniquely defined up to conjugacy in S.*

(2) *S contains* $Q_8 = BD_{4\cdot 2}$ *if and only if there are* $a, b \in F$ *with* $a^2 + b^2 = -1$, *thus for all* F *with* $\operatorname{char} F > 0$.

(3) (*Example 1*) *If* $F = \mathbb{F}_q$, $q = p^f$ *odd, then the* 2*-Sylow subgroup of* $S = \mathrm{SL}(2, q)$ *is* Q_8 *if* $q \equiv \pm 3 \pmod 8$, *and*

$$BD_{4\cdot 2^r},\ 2^{r+2} || (q^2-1), \quad \textit{if} \quad q \equiv \pm 1 \pmod 8.$$

(4) *S contains* $BD_{4\cdot r}$, $r \geq 2$, *if and only if*
   (a) F *contains* $\alpha = \zeta + \zeta^{-1}$ *for some primitive* $2r^{\text{th}}$ *root* $\zeta = \zeta_{2r}$ *of* 1 *in* $\bar{F}^\times$, *and*
   (b) $-1 \in N_{E/F}E^\times$, $E = F(\zeta)$, *namely when* $\zeta \notin F^\times$, *there are* x, y *in* F *with* $-1 = x^2 - \alpha xy + y^2$.

   (*Example 2*) *Suppose* $F = \mathbb{F}_q$, $q = p^f$ *odd. If* S *contains* BD_{4r}, *and* $2^k | r$, *then* $2^{k+2} | (q^2 - 1)$ *and* (4a). *If* $2^{k+2} | (q^2-1)$ *and* (4a), *then* S *contains* BD_{4r}, $2^k || r$. *Thus when* $q \equiv \pm 3 \pmod 8$, $k \leq 1$. *If* F *contains* $\mathbb{F}_q$ *with* $2^{k+2} | (q^2-1)$ *and* (4a), *then* $S \supset BD_{4r}$, $2^k || r$.

(5) *S contains* $2A_4$ *if and only if* -1 *is a sum of two squares in* F, *in particular if* $\operatorname{char} F > 2$.

(6) *S contains* $2S_4 = BO_{48}$ *if and only if* -1 *is a sum of two squares in* F *and* $\sqrt{2} \in F$.

(7) *S contains* $2A_5$ *if and only if* -1 *is a sum of two squares in* F *and* 5 *is a square in* F.

Proof. (1). Suppose $C_r \hookrightarrow S$ and $h \in S$ generates the image of C_r. Then the eigenvalues of h are ζ, ζ^{-1}, and $\operatorname{tr} h = \zeta + \zeta^{-1}$ lies in F. Conversely, if $\alpha = \zeta + \zeta^{-1}$ lies in F, then $h = \left(\begin{smallmatrix} \alpha & 1 \\ -1 & 0 \end{smallmatrix}\right) \in S$. The characteristic polynomial of h, $x^2 - \alpha x + 1$, has roots ζ, ζ^{-1}, which are distinct (as $\zeta = \zeta^{-1}$ implies $\zeta^2 = 1$, but $r \geq 3$ by assumption), hence h is diagonalizable in $\bar{S}$ and has order r, so $C_r = \langle h \rangle \subset S$.

To see that C_r is uniquely defined up to conjugacy in S, note that if b is an element of S with eigenvalues ζ, ζ^{-1}, then it is conjugate to h in $\bar{S}$. So there is $g \in \bar{S}$ with $h = g^{-1}bg$. Then $h = \sigma(g)^{-1}b\sigma(g)$ for every $\sigma \in \mathrm{Gal}(\bar{F}/F)$. Hence $g_\sigma = g\sigma(g)^{-1}$ lies in the centralizer of b in $\bar{S}$. This is a torus, say T, over F. Hence the cocycle $\{\sigma \mapsto g_\sigma\}$ lies in $\ker[H^1(F,T) \to H^1(F,S)]$. But $H^1(F,T)$ is trivial (as is $H^1(F,S)$), so there is some t in $T(\bar{F})$ with $g_\sigma = t\sigma(t)^{-1}$, thus $g\sigma(g)^{-1} = t\sigma(t)^{-1}$ for all $\sigma \in \mathrm{Gal}(\bar{F}/F)$. Consequently $t^{-1}g = \sigma(t^{-1}g)$, namely $t^{-1}g = s \in S$, so $g = ts$ and $h = s^{-1}t^{-1}bts = s^{-1}bs$.

(2). Recall that $Q_8 = \langle i, j;\, i^2 = -I = j^2,\, j^{-1}ij = i^{-1} \rangle$. By matrix multiplication, $s = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{SL}(2,F)$ satisfies $s^2 = -I$ if and only if $d = -a$ and $a^2 + bc = -1$. If $a = 0$ then $d = 0$ and $s = \left(\begin{smallmatrix} 0 & e \\ -1/e & 0 \end{smallmatrix}\right)$. If ζ_4 lies in F, take $i = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, $j = \operatorname{diag}(\zeta_4, -\zeta_4)$; then $Q_8 \subset S$. If not, in a suitable basis $i = \left(\begin{smallmatrix} 0 & e \\ -1/e & 0 \end{smallmatrix}\right)$ and $j = \left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right)$. As $ij = \left(\begin{smallmatrix} ec & -ea \\ -a/e & -b/e \end{smallmatrix}\right)$ lies in the ring Q_8 (as i, j

do) its square is $-I$, so $b=e^2c$, and $1=\det j=-a^2-e^2c^2$. Conversely, if $a, b\in F$, $a^2+b^2=-1$, then $\langle \left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}a&b\\b&-a\end{smallmatrix}\right)\rangle$ is a copy of Q_8 in $\mathrm{SL}(2,F)$.

Example. $F=\mathbb{Q}(\sqrt{-2})$, $a=\sqrt{-2}$, $b=1$. Any F with $\operatorname{char}F>0$, e.g., $F=\mathbb{F}_7$, $a=3$, $b=2$.

(3). Let $F=\mathbb{F}_q$ be a finite field of odd order $q=p^f$. We determine the 2-Sylow subgroup of $S=\mathrm{SL}(2,q)$ using [13, Theorem 6.11, p. 189]. It asserts that if P is a p-group containing at most one subgroup of order p, then either P is cyclic, or else $p=2$ and P is a generalized quaternion group. Using this with $p=2$, noting that the only element of order 2 in S is $-I$, and that there are a and b with $-1=a^2+b^2$ in any finite field, we see that S contains the quaternion group Q_8 generated by $\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}a&b\\b&-a\end{smallmatrix}\right)$. Hence the 2-Sylow is a generalized quaternion group. The order of $\mathrm{SL}(2,q)$ is $q(q^2-1)$, so the order of a 2-Sylow subgroup of $\mathrm{SL}(2,q)$ is $2^k||(q^2-1)$, meaning the biggest power 2^k of 2 dividing q^2-1. If q is congruent to 3 or 5 modulo 8, which means that $p\equiv\pm3 \pmod 8$ and f is odd, then $8||(q^2-1)$, $k=3$, the 2-Sylow is Q_8, and S contains no element of order 8. If $q\equiv\pm1 \pmod 8$, which means that p has this property or f is even, then $2^{k+2}|(q^2-1)$, $k\geq2$, the 2-Sylow is $BD_{2^{k+2}}$, $k\geq 2$, strictly bigger than Q_8, and S contains an element of order 2^{k+1}.

A self-sufficient proof is as follows. If $q\equiv 1 \pmod 4$ and $2^{r+2}||(q^2-1)$, $r\geq1$, then $2^{r+1}||(q-1)$, $2||(q+1)$. As $\mathbb{F}_q$ is cyclic of order $q-1$, it contains ζ of order 2^{r+1}. Put $d=\operatorname{diag}(\zeta,\zeta^{-1})$. Then $T=\langle d, i\rangle$, with matrix i as in (2), is a Sylow 2-subgroup of S with $d^{2^r}=i^2=-I$ and $i^{-1}di=d^{-1}$. This T is a generalized quaternion group.

If $q\equiv -1 \pmod 4$, let E be a field of order q^2 containing F. Then the multiplicative group $E_1=E^\times$ acts as F-linear transformations on the 2-dimensional F-space $(E,+)$, so $E_1\subset \mathrm{GL}(2,F)$. The group E_1 is cyclic of order q^2-1. Denote a generator by y. Hence E_1 contains a cyclic subgroup T_1 of order 2^{r+2}. The subgroup $\{y^{n(q-1)}; 0\leq n<q+1\}$ of E_1 is of order $(q^2-1)/(q-1)=q+1$; it is contained in S. Hence, a cyclic subgroup T_2 of T_1 of order 2^{r+1} is contained in S. Clearly E is the centralizer ring for T_2 inside the ring $\mathrm{Mat}(2,F)$ of 2×2-matrices with entries in F. Hence $E_1=C_S(T_2)$. Let T be a Sylow 2-subgroup of S containing T_2. Since $T\cap E_1=T_2$, T is non-abelian and $-I$ is the only element of T of order 2. Let j be in $T-T_2$. If t is a generator of T_2 with eigenvalues λ, λ^{-1}, then $j^{-1}tj$ must have the same eigenvalues. So $j^{-1}tj=t^{-1}$, since j does not centralize T_2. In particular, the centralizer of j in T_2 is $\{-I,I\}$. So j^2 is in $\{-I, I\}$. Since j does not have order 2, $j^2=-I$. It follows that $T=\langle t, j\rangle$ is a generalized quaternion group of order 2^{r+2}.

(4). The case of $r=2$ is (2), where $\alpha=0$. Now $C_{2r}\subset BD_{4r}\subset S$ implies $\alpha=\zeta+\zeta^{-1}\in F$ by (1), for $\zeta=\zeta_{2r}$. The group BD_{4r} is generated by

h (with $h^r = -I$) and g with $ghg^{-1} = h^{-1}$ and $g^2 = -I$. If $\zeta \in F$, then $h = \mathrm{diag}(\zeta, \zeta^{-1})$ and $g = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ generate BD_{4r}, and $-1 \in N_{E/F}E^\times$ as $E = F(\zeta)$ is F. If $\zeta \notin F$, then $h = \left(\begin{smallmatrix} \alpha & 1 \\ -1 & 0 \end{smallmatrix}\right)$ still lies in S. Its eigenvalues are ζ, ζ^{-1}. Thus the normalizer of h is $C \cup gC$, where C is the centralizer of h. By matrix multiplication, $g = \left(\begin{smallmatrix} x & y \\ y-\alpha x & -x \end{smallmatrix}\right)$ with $-1 = x^2 - \alpha xy + y^2 = (x - \zeta y)(x - \zeta^{-1} y)$. Thus -1 is a norm from the quadratic extension $E = F(\zeta)$ of F. Note that $g^2 = -I$. Conversely, if $\alpha = \zeta + \zeta^{-1} \in F$ and there are x, $y \in F$ with $-1 = x^2 - \alpha xy + y^2 = (x - \zeta y)(x - \zeta^{-1} y)$, then $BD_{4r} = \langle h, g \rangle \subset S$.

Example. If $r = 4$, $\zeta = \zeta_8 = \frac{1+i}{\sqrt{2}}$, $\alpha = \sqrt{2}$. If $F = \mathbb{F}_7$, $r = 4$, $h = \left(\begin{smallmatrix} 3 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, $j = \left(\begin{smallmatrix} 2 & 1 \\ 2 & -2 \end{smallmatrix}\right)$, $jhj^{-1} = h^{-1}$.

(5). If S contains $2A_4 = Q_8 : C_3 = BT_{24}$, then it contains Q_8, so -1 is a sum of two squares in F by (2). Conversely, following Serre [17, 10.2.3], if $-1 = a^2 + b^2$ is a sum of two squares in F, we define I, i, j, k in the algebra $M(2, F)$ of 2×2 matrices over F by

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad j = \begin{pmatrix} a & b \\ b & -a \end{pmatrix}, \quad k = \begin{pmatrix} b & -a \\ -a & -b \end{pmatrix}.$$

Since $i^2 = j^2 = k^2 = -I$, $ijk = -I$, this defines an isomorphism of $M(2, F)$ with the quaternion algebra $Q(F) = \langle i, j; i^2 = j^2 = (ij)^2 = -I \rangle$ over F, thus a splitting of $Q(F)$ over any field F where -1 is a sum of squares. Let

$$Q = Q_8 = \{\pm I, \pm i, \pm j, \pm k\} \subset \mathrm{SL}(2, F)$$

be the quaternion group, consisting of 8 elements. The set

$$X = \left\{ \frac{1}{2}(\pm I \pm i \pm j \pm k) \right\} \subset \mathrm{SL}(2, F)$$

consists of 16 elements. The matrices in X normalize Q. The set $Y = Q \cup X$ is a subgroup of $\mathrm{SL}(2, F)$ of order 24. It is the semidirect product of the normal subgroup Q with its complement the cyclic group C_3 of order 3 generated by $\frac{1}{2}(-1 + i + j + k)$. It is isomorphic to $\mathrm{SL}(2, 3) = 2A_4$.

Note that -1 is a sum of two squares in $\mathbb{F}_p$: if $p > 2$, there are $(p+1)/2$ elements in $\mathbb{F}_p$ of the form $-a^2$, and $(p+1)/2$ elements of the form $1 + b^2$, and $(p+1)/2 + (p+1)/2 > p$.

(6). If S contains $2S_4 = BO_{48}$, then it contains $2A_4 = Q_8 : C_3$ as a subgroup of index 2, so -1 is a sum of two squares in F by (5). Its 2-Sylow subgroup is $BD_{4\cdot 4}$, which contains C_8. Hence $\zeta_8 + \zeta_8^{-1} = \sqrt{2}$ (i.e., $(\zeta_8 + \zeta_8^{-1})^2 = 2$) lies in F. Note that $2S_4/Q_8 = S_3$. The group BO_{48} is presented in [7, (BO_{48}) of Subsection 3.2] as generated by BT_{24} and $w_4 = \mathrm{diag}(\zeta_8, \zeta_8^{-1})$ in $\bar{S}$, thus by t and w_4. As $\zeta_8 = (1+i)/\sqrt{2}$, if i and $\sqrt{2}$ lie in F, this gives a presentation also in S.

If 2 is a square in F, and -1 is a sum of two squares (and not necessarily a square), then S contain $2S_4$. Under this assumption on F, first we note that $\mathrm{PSL}(2,F)$ contains S_4. Indeed, put $s = I + i$. Then $s^2 = 2i$, $sis^{-1} = i$, $sjs^{-1} = k$, $sks^{-1} = -j$. Hence s normalizes Y of (5). The image σ of s in $\mathrm{PGL}(2,F)$ then normalizes $Y/\{\pm I\} = A_4$. The group generated by $Y/\{\pm I\}$ and σ is isomorphic to S_4. If $2 = c^2$ with $c \in F$, then s/c has determinant 1, so S_4 is contained in $\mathrm{PSL}(2,F)$.

Next, we note that if $\mathrm{PSL}(2,F)$ contains S_4, then $\mathrm{SL}(2,F)$ contains $2S_4$. The opposite direction is clear. So, suppose $H \subset \mathrm{PSL}(2,F)$ with $H \simeq S_4$. Let G be the full pre-image of H in $\mathrm{SL}(2,F)$ for the natural projection map $\mathrm{SL}(2,F) \to \mathrm{PSL}(2,F)$ (quotient by the center $Z = Z(\mathrm{SL}(2,F)) = \{\pm I\}$). We are assuming $\operatorname{char} F \neq 2$. Then Z is a normal (central) subgroup of G and $G/Z = H \simeq S_4$. Let T be a Sylow 2-subgroup of G. Then $-I$ is the unique involution of T, and T/Z is dihedral of order 8. So, T is the generalized quaternion group of order 16. Hence, $G \simeq 2S_4$.

Indeed, let $A = [H,H] \simeq A_4$ and let $E = [T/Z, T/Z] \subset A$. Then E is a Klein 4-group and the pre-image of E in $[G,G]$ is $Q \simeq Q_8$. Let X be a Sylow 3-subgroup of A, so that $A = EX$. Let Y be a Sylow 3-subgroup of $[G,G]$. Then

$$[G,G] = Q : Y \simeq 2A_4 \simeq \mathrm{SL}(2,3)$$

and $G = [G,G]T$ with $T \cap [G,G] = Q$ and with T a generalized quaternion group. It is not hard to prove that G is unique up to isomorphism and $G \simeq 2S_4$.

In short, $\mathrm{PSL}(2,F)$ contains S_4 if and only if $\mathrm{SL}(2,F)$ contains $2S_4$.

(7). If S contains $2A_5$, then it contains its subgroup $2A_4$, hence -1 is a sum of two squares in F. Also, $2A_5$ contains an element h of order 5, whose eigenvalues are

$$\zeta = \frac{-1 + u\sqrt{5}}{4} + vi\frac{\sqrt{5 + u\sqrt{5}}}{2\sqrt{2}}, \qquad u, v \in \{\pm 1\},$$

so $\operatorname{tr} h = \zeta + \zeta^{-1} = \frac{-1+u\sqrt{5}}{2}$ lies in F, as does $\sqrt{5}$.

Conversely, assume 5 is a square in F, and -1 is a sum of two squares. We construct a group R in $\mathrm{SL}(2,F)$ isomorphic to $\mathrm{SL}(2,5) = 2A_5$, following Serre [17, 10.2.3], who attributes the construction to Coxeter [4]. Consider the 8 matrices $x + yi + zj + wk$, where

$$(x, y, z, w) = \frac{1}{2}(0, \pm 1, \pm t, \pm t')$$

with $t = \frac{1+\sqrt{5}}{2}$ and $t' = \frac{1-\sqrt{5}}{2}$. Permuting these (x, y, z, w) by even permutations, we obtain a set T of $8 \times 12 = 96$ matrices. They are of order 3 (resp. 4, 5, 6, 10) if their x-component is $-\frac{1}{2}$ (resp. 0, $-t/2$ or $-t'/2$, $\frac{1}{2}$, $t/2$ or $t'/2$). Put $R = Y \cup T$, where Y is the group $Q : C_3 = \mathrm{SL}(2,3)$ of (5) above. See also [3, p. 2]. □

Remark 2.2.

(1) Part (1) holds vacuously for $r = 2$. Indeed, if $\operatorname{char} F \neq 2$ then there is a unique element, $-I$, of order 2 in $S = \mathrm{SL}(2, F)$. It generates the center $Z = \langle -I \rangle$ of S. If $\operatorname{char} F = 2$, each $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$, $a \in F^\times$, has order 2.

(2) In (5), we cannot argue that S contains also the normalizer $2S_4 = N_{\bar{S}}(Q_8)$ of Q_8 in $\bar{S} = \mathrm{SL}(2, \bar{F})$, as by (6) F would have to contain $\sqrt{2}$ too. Thus the construction of the normalizer of $A = Q_8$ in the proof of [7, Proposition 2.3] is not purely rational over F.

(3) The condition on F for $\mathrm{PGL}(2, F)$ to contain A_4 (there are a, b in F with $-1 = a^2 + b^2$ if $\operatorname{char} F \neq 2$; there is $c \in F$ with $c^2 + c = 1$ if $\operatorname{char} F = 2$), S_4 ($\operatorname{char} F \neq 2$ and there are a, b in F with $-1 = a^2 + b^2$), A_5 (there are a, b, c in F with $-1 = a^2 + b^2$ and $c^2 + c = 1$) is given already in [15, Remarque in 2.5].

(4) The examples of case (3) and the second half of (4) of the proposition (concerning subgroups of finite groups) are of course well-known, and are given simply for completeness, as examples, as the proof is short. References include [5, Chapter XII], [11], [14], and recently [2]. These texts might be of interest to group theorists. For our rationality considerations we give a complete but short treatment. In any case the case of finite field F is just an example of the proposition, which considers a general field.

3. Isomorphic finite subgroups of $\mathrm{SL}(2, \bar{F})$ are conjugate

We now determine the conjugacy classes of finite subgroups of $\mathrm{SL}(2, \bar{F})$.

Proposition 3.1. *Any two finite irreducible isomorphic subgroups of the group* $\mathrm{SL}(2, \bar{F})$*, with cardinality prime to* $\operatorname{char} \bar{F}$*, are conjugate.*

3.1. The cyclic C_r. The cyclic group C_r (which is reducible) is generated by an element of order r, diagonalizable, with eigenvalues $\zeta_r^{\pm 1}$. So there is a single conjugacy class of groups $C_r = \mathbb{Z}/r$ in $\mathrm{SL}(2, \bar{F})$ if $r \neq 0$ in $\bar{F}$. When $r = 2$, the only element of order 2 in $\mathrm{SL}(2, \bar{F})$ is $-I$.

3.2. The binary dihedral $BD_{4 \cdot 2} = Q_8$. This is the quaternion group of 8 elements $\langle i, j; i^2 = j^2 = (ij)^2 = -I \rangle$. By matrix multiplication, an $s = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2, \bar{F})$ with $s^2 = -I$ has $a + d = 0$ and $a^2 + bc = -1$. If $a = 0$, then $d = 0$ and $s = \left(\begin{smallmatrix} 0 & b \\ -1/b & 0 \end{smallmatrix}\right)$. We may choose the basis so that $i = w$, $w = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. If j too has the form $\left(\begin{smallmatrix} 0 & b \\ -1/b & 0 \end{smallmatrix}\right)$, as $(ij)^2 = -I$ we have $b = \pm i$, and Q_8 is the group generated by $i = w$ and $j = \operatorname{diag}(i, -i)$, and $ij = y = \operatorname{diag}(i, -i)w$. If not, still with $i = w$, $j = \left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right)$, and as $ij = \left(\begin{smallmatrix} c & -a \\ -a & -b \end{smallmatrix}\right)$ lies in the ring Q_8 (as i, j do) its square is $-I$, so $c = b$, and $1 = \det j = -a^2 - b^2$. Note that we cannot have $i = y$, with $y = \left(\begin{smallmatrix} a & b \\ b & -a \end{smallmatrix}\right)$, and $j = \left(\begin{smallmatrix} c & d \\ d & -c \end{smallmatrix}\right)$, as then $(ij)^2 \neq -I$. Hence one of i, j has the form y. Now with a suitable choice of a basis, i will be taken to be y, then j has to be w or $-w$, the only element in the normalizer of $\langle y\rangle$, modulo $\langle y\rangle$, and $\langle y, w\rangle$ is a copy of Q_8 in $\mathrm{SL}(2, F)$, unique up to conjugation.

Here is another way to see this. There are 5 conjugacy classes in Q_8. They are I, $-I$, $\{\pm i\}$, $\{\pm j\}$, $\{\pm ij\}$. Hence there are 5 irreducible representations of Q_8, 4 of them of dimension 1, factorizing through the quotient $C_4 = \langle i\rangle$, mapping i to 1, -1, i, $-i$, and one irreducible faithful two dimensional representation (sum of dimensions is $4 \times 1^2 + 2^2 = 8 = |Q_8|$).

3.3. The binary dihedral $BD_{4\cdot r}$, $r \geq 3$. The cyclic subgroup $C_{2r} = \langle h\rangle$ of the binary dihedral group

$$BD_{4\cdot r} = \langle h,\ w;\ h^r = -I = w^2,\ whw^{-1} = h^{-1}\rangle,\ r \geq 3,$$

is diagonal, up to conjugacy, by 3.1. The w solving the equation are $\pm\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ if r is odd, and also the product of this with $\mathrm{diag}(\zeta_4, \zeta_4^{-1})$ if r is even, so $BD_{4\cdot r}$ is uniquely determined by C_{2r}, as its normalizer in $\mathrm{SL}(2, \bar{F})$.

3.4. $2A_4 = \mathrm{SL}(2,3) = BT_{24}$. This group ([12, p. 288]) has 3 irreducible two-dimensional representations, (ψ, ξ_1, ξ_2 in [6, p. 228]), obtained from each other by twisting with the 3 1-dimensional representations, which take at u of order 3 the value ω (= 3rd root of 1), so only one representation can be into $\mathrm{SL}(2, \bar{F})$.

3.5. $2S_4 = BO_{48}$. $2S_4$ is not in [3], since it is a solvable group. I could not find a character table in the literature, so let us work out this well known case. A Sylow 2-subgroup is the generalized quaternion group of order 16, $BD_{16} = \langle d(\zeta), a(i)\rangle$, where ζ is a primitive 8th root of 1, $d(x) = \mathrm{diag}(x, 1/x)$, $a(x) = \left(\begin{smallmatrix} 0 & x \\ -1/x & 0 \end{smallmatrix}\right)$. There are 3 classes of elements in $2S_4$ outside $2A_4$, intersecting BD_{16} in the BD_{16}-classes in $BD_{16} - Q_8$: 2 classes of elements of order 8: $\{d(\zeta), d(1/\zeta)\}$, $\{d(\zeta^3), d(\zeta^5)\}$, and one class of elements of order 4: $\{a(\zeta^j);\ j = 1, 3, 5, 7\}$ (so we got 8 elements of $BD_{16} - Q_8$; conjugate by the elements of order 3 in $2S_4$ to get the 24 elements of $2S_4 - 2A_4$). Also, there are 5 $2S_4$-classes inside $2A_4$: one each of elements of order 1, 2, 3, 4, and 6 (these classes consist of 1, 1, 6, 8, 8 elements; see [12, p. 288] for $2A_4 = \mathrm{SL}(2,3)$). So there are 8 characters of $2S_4$, five of which descend to characters of S_4 (as there are 5 conjugacy classes in S_4, three of them in S_3). So there are 3 faithful characters of $2S_4$. Their degrees squared have to add up to 24. So we get character degrees 2, 2 and 4. The characters of $2A_4 = \mathrm{SL}(2,3)$ of degree 2 which do not give representations in $\mathrm{SL}(2, \bar{F})$ (but in $\mathrm{GL}(2, \bar{F})$; χ_6, χ_7 in [12, p. 288]) are not invariant in $2S_4$. So they induce up to a character of degree 4. The character χ_5 of $2A_4$ of degree 2 which does map into $\mathrm{SL}(2, \bar{F})$ lifts to a character of degree 2 of $2S_4$. The other character of $2S_4$ of degree 2 comes from tensoring the first representation with the nontrivial degree 1 representation $2S_4/2A_4 \twoheadrightarrow S_4/A_4 \twoheadrightarrow \langle -I \rangle$. As $\langle -I \rangle$ is a subgroup of $2S_4$, the image of the second representation is the same as that of the first.

3.6. $2A_5 = \mathrm{SL}(2,5) = BI_{120}$. By [6, p. 228], $\mathrm{SL}(2,q)$, $q = 5$, has two representations of degree 2, η_1 and η_2. Conjugation by $2S_5$ permutes them. Indeed, if two representations are twists by an automorphism, then their images in SL are conjugate: if η_1 is one representation and α is the automorphism, then η_1 and $\eta_2 = \eta_1 \circ \alpha$ have the same image.

3.7. Isomorphic finite subgroups of $\mathrm{PGL}(2,\bar{F}) = \mathrm{SO}(3,\bar{F})$ are conjugate. Let us consider the analogous question for $\mathrm{PGL}(2,\bar{F})$.

Proposition 3.2. *Any two finite irreducible isomorphic subgroups of the group* $\mathrm{PSL}(2,\bar{F})$*, with cardinality prime to* $\mathrm{char}\,\bar{F}$*, are conjugate.*

Proof. We need to consider 3-dimensional representations of A_4, S_4, A_5. From [12, p. 287], S_4 has a unique 3-dimensional representation χ_4 in $\mathrm{SL}(3,\bar{F})$ (and another, χ_5, in $\mathrm{GL}(3,\bar{F})$, obtained by twisting with the sign character, whose value at the transpositions is -1, not 1). Its restriction to the index 2 subgroup A_4 is irreducible. By [12, p. 288], A_5 has two 3-dimensional representations, but they are obtained from each other by conjugation in S_5, so their images are equal. □

4. Isomorphic finite subgroups of $\mathrm{SL}(2,F)$ up to conjugacy

In this section (assuming $\mathrm{char}\,F$ does not divide the order of the group in question) we parametrize the conjugacy classes in $\mathrm{SL}(2,F)$ of isomorphic subgroups of $\mathrm{SL}(2,F)$.

Theorem 4.1. *Up to conjugacy,* $\mathrm{SL}(2,F)$ *contains a single subgroup isomorphic to $C_r = \mathbb{Z}/r$. The subgroups (up to conjugacy) isomorphic to each of $Q_8 = BD_{4\cdot 2}$, $2S_4 = BO_{48}$ and $2A_5 = BI_{120}$, in* $\mathrm{SL}(2,F)$*, are parametrized by $F^\times/F^{\times,2}$. The same holds for $2A_4 = BT_{24}$ if F contains $\sqrt{2}$, namely if S contains $2S_4$. If not, the conjugacy classes in* $\mathrm{SL}(2,F)$ *of $2A_4$ are parametrized by a quotient of $F^\times/F^{\times,2}$ by a subgroup of cardinality two. If $\mu_{2r}(F)$ has cardinality $2r$, then the subgroups of type $BD_{4\cdot r}$, $r \geq 3$, are parametrized, up to conjugacy in* $\mathrm{SL}(2,F)$*, by $F^\times/F^{\times,2}\mu_{2r}(F)$. The same holds also when ζ_{2r} does not lie in $F^\times$, but then the cardinality of μ_{2r} is a proper divisor of $2r$.*

Proof. This follows using the proposition below. The centralizer of C_r is $\mathbb{G}_m = \mathrm{GL}(1)$ if $r \geq 3$, and $S = \mathrm{SL}(2)$ if $r = 2$. We have $H^1(F,\mathbb{G}_m) = \{0\}$, $H^1(F,S) = \{0\}$. The first sentence of the theorem follows. The centralizer of each of the other subgroups is the center $C_2 = \mu_2 = \{\pm I\}$ of S. We have $H^1(F,\mu_2) = F^\times/F^{\times,2}$ ([16, II.1.2 Corollary]: $x \mapsto x^2$ defines a short exact sequence $1 \to \mu_2 \to \mathbb{G}_m \to \mathbb{G}_m \to 1$, hence a long exact sequence

$\{\pm 1\} \to F^\times \to F^\times \to H^1(F, \mu_2) \to H^1(F, \mathbb{G}_m) = 1)$. The normalizer of $BD_{4\cdot 2} = Q_8$ in $\mathrm{SL}(2, \bar{F})$ is $2A_4 = Q_8 : C_3$. By Proposition 2.1, S contains Q_8 if and only if it contains its normalizer $2A_4$. If the normalizer N of $G \subset \mathrm{SL}(2, F)$ in $\mathrm{SL}(2, \bar{F})$ lies in $\mathrm{SL}(2, F)$, it acts trivially on $H^1(F, C)_0$. The claim about Q_8 follows. The normalizer of $2S_4$ is $2S_4$. That of $2A_4$ is $2S_4$. That of $2A_5$ is $2A_5$. Using the proposition below, the claims about $2S_4$ and $2A_5$ follow, as the normalizer is just the group. As for the claim about $2A_4$, the normalizer $N = 2S_4$ of $2A_4$ in $\mathrm{SL}(2, \bar{F})$ lies in $\mathrm{SL}(2, F)$ if $\sqrt{2} \in F$. If not, the conjugacy classes in $\mathrm{SL}(2, F)$ of $2A_4$ are parametrized by a quotient of $F^\times/F^{\times,2}$ by a subgroup of cardinality 2.

Consider the remaining case of $BD_{4\cdot r}$, $r \geq 3$. Its centralizer C in $\mathrm{SL}(2)$ is μ_2, so $H^1(F, C)_0 = H^1(F, C) = F^\times/F^{\times,2}$. Its normalizer is $BD_{8\cdot r}$. Suppose $\zeta = \zeta_{2r} \in F$. Fix the embedding

$$i : BD_{4\cdot r} = \langle a, b;\, a^r = b^2 = -I,\, bab^{-1} = a^{-1}\rangle \hookrightarrow \mathrm{SL}(2, F),$$

with $i(a) = \mathrm{diag}(\zeta, \zeta^{-1})$ and $i(b) = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. The embeddings in $\mathrm{SL}(2, F)$ of subgroups isomorphic to $BD_{4\cdot r}$ (up to conjugation by $\mathrm{SL}(2, F)$) are the conjugates of i by $\mathrm{diag}(\beta, 1/\beta)$, where $\beta^2 = \alpha \in F^\times/F^{\times,2}$. The powers of $i(a)$ are not affected by conjugation by $\mathrm{diag}(\beta, 1/\beta)$, but $i(b)$ becomes

$$\mathrm{Int}(\mathrm{diag}(\beta, 1/\beta))i(b) = \left(\begin{smallmatrix} 0 & \alpha \\ -1/\alpha & 0 \end{smallmatrix}\right).$$

The normalizer is

$$BD_{8\cdot r} = \langle c, b;\, c^{2r} = b^2 = -I,\, bcb^{-1} = c^{-1}\rangle.$$

It acts on $H^1(F, \mu_2)$ by multiplication by the cocycle

$$\sigma \mapsto \rho^{-1}\sigma(\rho), \quad \rho = \mathrm{diag}(\nu, \nu^{-1}), \quad \nu = \zeta_{4r}.$$

This cocycle corresponds to the class of $\zeta = \nu^2$ in $F^\times/F^{\times,2}$, which generates $\mu_{2r}(F)$.

Suppose now $\zeta = \zeta_{2r} \notin F$. We still have $\alpha = \zeta + \zeta^{-1} \in F$, as $BD_{4r} \subset \mathrm{SL}(2, F)$. Fix the embedding

$$i : BD_{4\cdot r} = \langle a, b;\, a^r = b^2 = -I,\, bab^{-1} = a^{-1}\rangle \hookrightarrow \mathrm{SL}(2, F),$$

with $i(a) = \left(\begin{smallmatrix} \alpha & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $i(b) = \left(\begin{smallmatrix} x & y \\ y-\alpha x & -x \end{smallmatrix}\right)$. Then there is some $\eta = \left(\begin{smallmatrix} a & b \\ -\zeta^{-1} & -\zeta b \end{smallmatrix}\right)$ with $1 = ab(\zeta^{-1} - \zeta)$ so that

$$i(a) = \eta\,\mathrm{diag}(\zeta, \zeta^{-1})\eta^{-1}, \quad i(b) = \eta\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)\eta^{-1},$$

with $x = \zeta^{-1}a^2 + \zeta b^2$ and $y = a^2 + b^2$. The embeddings in $\mathrm{SL}(2, F)$ of subgroups isomorphic to $BD_{4\cdot r}$ (up to conjugation by $\mathrm{SL}(2, F)$) are the conjugates of i by $\eta\,\mathrm{diag}(\beta, 1/\beta)\eta^{-1}$, where $\beta^2 = \alpha \in F^\times/F^{\times,2}$. The powers of $i(a)$ are not affected by conjugation by $\eta\,\mathrm{diag}(\beta, 1/\beta)\eta^{-1}$, but $i(b)$ becomes

$$\mathrm{Int}(\eta)\,\mathrm{Int}(\mathrm{diag}(\beta, 1/\beta))i(b) = \mathrm{Int}(\eta)\left(\begin{smallmatrix} 0 & \alpha \\ -1/\alpha & 0 \end{smallmatrix}\right).$$

The normalizer is

$$BD_{8\cdot r} = \langle c,\, b;\, c^{2r} = b^2 = -I,\, bcb^{-1} = c^{-1}\rangle.$$

It acts on $H^1(F, \mu_2)$ by multiplication by the cocycle

$$\sigma \mapsto \mathrm{Int}(\eta)(\rho^{-1}\sigma(\rho)), \quad \rho = \mathrm{diag}(\nu, \nu^{-1}), \quad \nu = \zeta_{4r}.$$

This cocycle corresponds to the class of $\zeta = \nu^2$ in $E^\times/E^{\times,2}$, $E = F(\zeta)$, which generates $\mu_{2r}(E)$. As $\zeta \notin F$, the cardinality of $\mu_{2r}(F)$ is a proper divisor of $2r$. $\square$

Example 4.2. The subgroups $G = 2A_5 = \mathrm{SL}(2,5)$ and $G^x = x^{-1}Gx$ of $\mathrm{SL}(2,q)$, $q \equiv \pm 1 \pmod 5$, are not conjugate if $x \in \mathrm{GL}(2,q)$, $\det x \notin F^{\times,2}$, e.g., when $q = 9$, in $\mathrm{SL}(2,9) = 2A_6$.

Let F be a field, and S an algebraic group over F. Denote by $S(F)$ the group of F-points of S. Let G be a subgroup of $S(F)$; fix an embedding $e : G \hookrightarrow S(F)$. Let $\bar{F}$ be a fixed separable closure of F, and $\mathrm{Gal}(\bar{F}/F)$ the Galois group. Put $G^g = g^{-1}Gg$. Denote by $\mathrm{Conj}(G, S(F))$ the (pointed, by G) set $\{G^g \subset S(F);\, g \in S(\bar{F})/S(F)\}$ of subgroups of $S(F)$ which are conjugate to G in $S(\bar{F})$, modulo conjugacy by $S(F)$.

Let $C = \mathrm{Cent}_S(G)$ be the centralizer of G in S, $H^1(F, C)_0$ the kernel of the natural map $H^1(F, C) \to H^1(F, S)$ where

$$H^i(F, S) = H^i(\mathrm{Gal}(\bar{F}/F), S(\bar{F})),$$

and N the normalizer of G in $S(\bar{F})$. In the rest of this section, following [1] we prove the following.

Proposition 4.3. *There is a natural isomorphism*

$$H^1(F, C)_0/N \xrightarrow{\sim} \mathrm{Conj}(G, S(F))$$

of pointed sets.

To describe the set $\mathrm{Conj}(G, S(F))$, consider the set $\mathrm{Emb}_e(G, S(F))$ of embeddings $j : G \hookrightarrow S(F)$ which are conjugate in $S(\bar{F})$ to e, thus $j = \mathrm{Int}(g)e : G \hookrightarrow S(F)$, where

$$\mathrm{Int}(g)\rho = g\rho g^{-1} : h \mapsto g\rho(h)g^{-1}, \quad g \in S(\bar{F}),$$

modulo conjugacy by $S(F)$. The image map

$$\mathrm{im} : \mathrm{Emb}_e(G, S(F)) \to \mathrm{Conj}(G, S(F)),$$

sending an embedding to its image, is onto.

The normalizer N of G in $S(\bar{F})$ acts on G by automorphisms, hence on $\mathrm{Emb}_e(G, S(F))$. Two embeddings with the same image are obtained from each other by an automorphism of G, which has to be given by an element of N if the two embeddings are conjugate to each other by $S(\bar{F})$. Hence im defines an isomorphism

$$\mathrm{Emb}_e(G, S(F))/N \xrightarrow{\sim} \mathrm{Conj}(G, S(F)).$$

Note: if N is contained in $S(F)$ then it acts trivially on $\mathrm{Emb}_e(G, S(F))$.

Lemma 4.4. *The pointed set* $\mathrm{Emb}_e(G, S(F))$ *is canonically isomorphic to* $H^1(F, C)_0$.

Proof. Put $X = \{g \in S(\bar{F});\ g^{-1}\sigma(g) \in C(\bar{F}) \text{ for all } \sigma \in \mathrm{Gal}(\bar{F}/F)\}$. The group $S(F)$ acts on X by left multiplication, and $C(\bar{F})$ acts on X by right multiplication. The kernel of $H^1(F, C) \to H^1(F, S)$ is identified in [16, Chapter I, 5.4, Corollary 1] with the quotient on the left by $S(F)$ of the set of $\mathrm{Gal}(\bar{F}/F)$-invariant elements of $S(\bar{F})/C(\bar{F})$. The latter set is, by definition, $X/C(\bar{F})$, so $H^1(F, C)_0 = S(F)\backslash X/C(\bar{F})$.

For every $g \in X$, the conjugate embedding $\mathrm{Int}(g)e = geg^{-1}$ lies in $\mathrm{Emb}_e(G, S(F))$. Each element $j \in \mathrm{Emb}_e(G, S(F))$ has the form $\mathrm{Int}(g)e$ for some $g \in S(\bar{F})$. For each $\sigma \in \mathrm{Gal}(\bar{F}/F)$, $\sigma(g)$ again conjugates e to j. Hence $g^{-1}\sigma(g) \in C(\bar{F})$, and $g \in X$. So the map $g \mapsto geg^{-1}$, $X \to \mathrm{Emb}_e(G, S(\bar{F}))$ is onto. Two elements, g and g', in X, give the same embedding in $\mathrm{Emb}_e(G, S(F))$, if and only if g' lies in $S(F)gC(\bar{F})$. So this map descends to a canonical bijection $S(F)\backslash X/C(\bar{F}) \xrightarrow{\sim} \mathrm{Emb}_e(G, S(\bar{F}))$. □

Proof of Proposition 4.3. The isomorphism of the lemma can be presented explicitly as follows. A class in the kernel $H^1(F, C)_0$ is represented by a 1–cocycle $\mathrm{Gal}(\bar{F}/F) \to C(\bar{F})$ which becomes a coboundary in $S(\bar{F})$, hence it takes the form $\sigma \mapsto g^{-1}\sigma(g)$ for some $g \in X$. To this class associate the embedding geg^{-1}.

Now an element n of N acts on $\mathrm{Emb}_e(G, S(F))$ by $j \mapsto j \circ \mathrm{Int}(n)$. If $j = geg^{-1}$, this amounts to replacing g by gn, hence the 1–cocycle $\varphi : \sigma \mapsto g^{-1}\sigma(g)$ by $n^{-1}\varphi\sigma(n)$. This defines an action of N on $H^1(F, C)$ which preserves $H^1(F, C)_0$. In conclusion, the map $g \mapsto gGg^{-1}$ reduces to an isomorphism $H^1(F, C)_0/N \xrightarrow{\sim} \mathrm{Conj}(G, S(F))$ of pointed sets. □

5. Isomorphic irreducible finite subgroups of $\mathbf{SL(3, \bar{F})}$ are conjugate

Theorem 5.1. *Any two finite irreducible isomorphic subgroups of* $\mathrm{SL}(3, \bar{F})$ *with cardinality prime to* $\mathrm{char}\,\bar{F}$ *and to* 3 *are conjugate.*

5.1. (J) PSL(2, 7), order $\mathbf{2^3 \cdot 3 \cdot 7}$. $\mathrm{PSL}(2, 7)$, order 168, [12, p. 289], has two 3-dimensional representations, obtained from each other by first conjugating by $\mathrm{PGL}(2, 7)$, which contains $\mathrm{PSL}(2, 7)$ as a normal subgroup of index 2. So they have the same image.

5.2. (I) $3A_6$, the Valentiner group, order $2^3 \cdot 3^3 \cdot 5$.

Proposition 5.2. *There are* 4 *irreducible representations of* $3A_6$ *of degree* 3. *The group* $\mathrm{Aut}(A_6)/A_6 = \mathbb{Z}/2 \times \mathbb{Z}/2$ *permutes them. Hence there is a single copy* (*up to conjugacy*) *of* $3A_6$ *in* $\mathrm{SL}(3, \bar{F})$.

Proof. The [3] presents the character tables for the simple groups in order of their size. So A_6 is the third group in the Atlas. Character tables for all the decorated versions of A_6 are tabulated. The little diagram at the end of the discussion of this item (bottom of 2nd page) shows that the table for $3G$, $G = A_6$, is the third one down in the left hand column. It lists five characters with degrees 3, 3, 6, 9, 15. The sum of their squares is $9+9+36+81+225 = 360$, not 1080. There are the non-faithful characters, which are the characters of A_6 at the top of column 1, of degrees 1, 5, 5, 8, 8, 9, 10. The sum of their squares is $360 = |A_6|$. Also, the table for $3A_6$ only treats the representations whose restriction to $Z = Z(3A_6) = \langle z \rangle$ map z to ωI, ω being a primitive 3rd root of 1 in $\bar{F}$. So there is another set of characters with the same degrees 3, 3, 6, 9, 15, where z is mapped to $\omega^2 I$. In other words, there are 4 irreducible representations of $3A_6$ of degree 3.

Now $\mathrm{Aut}(A_6)/A_6$ ist eine Kleinsche Vierergruppe (un petit groupe de quatre) permuting these 4 characters. To see this, note that $\mathrm{Aut}(A_6)$ has three subgroups of index 2. One is S_6. Another is $\mathrm{PGL}(2, 9)$. The third is the Mathieu group M_{10}. Consider the action of each of the outer automorphisms on the relevant conjugacy classes: the two central classes and the two classes of elements of order 5. From [10, Table 6.3.1], we see that the M_{10}-automorphism centralizes $Z(3A_6)$, while the other two invert it. Also, the $\mathrm{PGL}(2, 9)$-automorphism centralizes a cyclic group of order 5, while $N_{S_6}(C_5) \simeq F_{20}$, the Frobenius group of order 20, in which all elements of order 5 are conjugate. The group A_6 has cyclic Sylow 5-subgroups of order 5. One is $P = \langle (12345) \rangle$. The normalizer $N_{A_6}(P)$ in A_6 of P is dihedral D_{10} of order 10, meaning that (12345) is conjugate in A_6 to $(54321) = (12345)^{-1}$. But (12345) is not conjugate in A_6 to $(13524) = (12345)^2$, which is a representative of the other class.

In S_6, all 5-cycles are conjugate: For a symmetric group, cycle type determines conjugacy class. So in A_6 there are $n_5 = |A_6|/|N_{A_6}(C_5)| = 6 \cdot 5 \cdot 4 \cdot 3/2 \cdot 5 = 2^2 3^2$ 5-Sylow subgroups. Hence there are $4 \cdot 4 \cdot 9$ elements of order 5, $8 \cdot 9 = 72$ in each of the two conjugacy classes of elements of order 5 in A_6. The group PGL(2,9) contains an element, say $t \notin A_6$, which commutes with the element (12345) in $A_6 = \mathrm{PSL}(2, 9)$. Then, of course, t also commutes with $(13524) = (12345)^2$. So, every element of $\mathrm{PGL}(2, 9)$ leaves invariant (under conjugation) the conjugacy class, $(12345)^{A_6}$ (which consists of 72 elements), and also the conjugacy class, $(13524)^{A_6}$. On the other hand, S_6 interchanges these two A_6-classes. So up to conjugacy we have only one image in $\mathrm{SL}(3, \bar{F})$. □

Scholium 5.3. In 1861, Emile Mathieu wrote a beautiful paper describing a new simple group of order $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$, which is a sharply 5-transitive subgroup of S_{12}. This group is called M_{12} in his honor. The stabilizer of one point is also a simple group, called M_{11}. The stabilizer of two points is the group M_{10} which is not simple but contains A_6 as a normal simple subgroup of index 2. In 1873, Mathieu published a paper on M_{24}.

5.3. (H) $A_5 = \mathrm{PSL}(2,5) = \mathrm{SL}(2,4)$, order $2^2 \cdot 3 \cdot 5$. This group has two irreducible 3-dimensional representations ([12, p. 288]). Conjugation by $S_5 = \mathrm{PGL}(2,5)$ (equality, as $S_5 = \mathrm{Aut}(A_5)$, $\mathrm{PGL}(2,p) = \mathrm{Aut}(\mathrm{PSL}(2,p))$ for all primes p) permutes these two representations, so A_5 has a unique embedding in $\mathrm{SL}(3,\bar{F})$, up to conjugation. (By [3, 1st case, p. 36], table at the bottom has $2G$, $G = A_5$; $2A_5$ has no faithful 3-dimensional representations. See also Linear representation theory of double cover of alternating group in `https://groupprops.subwiki.org/wiki/`.)

5.4. (G) The Hessian group H, order $2^3 \cdot 3^4$.

Proposition 5.4. *There are* 6 *irreducible* 3*-dimensional representations of the Hessian group* H *in* $\mathrm{SL}(3,\bar{F})$*. Their images are conjugate to each other under* $\mathrm{SL}(3,\bar{F})$*.*

Proof. The Hessian group H is a subgroup of $\mathrm{SL}(3,\bar{F})$ which has a normal subgroup A with $H/A = \mathrm{SL}(2,3)$. This gives one faithful representation $\rho_0 : H \hookrightarrow \mathrm{SL}(3,\bar{F})$. In fact, the normalizer of A in $\mathrm{SL}(3,\bar{F})$ is H ([8, Corollary 3.6(3)]). We proceed to determine all faithful 3-dimensional representations ρ of H. Such ρ is faithful on A. A 3-dimensional faithful representation of A is nontrivial on $Z = \langle \omega I \rangle$, ω being a primitive 3rd root of 1 in $\bar{F}$. There are 11 conjugacy classes in $A = \langle S, T \rangle$, 8 of 3 elements each: these are the classes of

$$S = \mathrm{diag}(1,\omega,\omega^2), \quad S^{-1}, \quad S^jT, \quad S^jT^{-1} \quad (j = 0,\,1,\,2),$$

where $T = \left(\begin{smallmatrix} 0&1&0\\ 0&0&1\\ 1&0&0 \end{smallmatrix}\right)$, and 3 classes of a single element each: $\omega^j I$ $(j = 0,\,1,\,2)$. Hence there are 11 irreducible representations of A: the trivial, 4 pairs of 1-dimensional representations $C_3 = A/E_j \to Z$ (the kernel E_j $(1 \le j \le 4)$ is as in Proposition 3.2 in [8]) determined by where ω goes to in $Z = \langle \omega I \rangle$; and 2 3-*dimensional ones*, as $27 = 3^2 + 3^2 + 9 \times 1$. The latter are the natural embedding $\rho_A = \rho_0|A$ of A in $\mathrm{SL}(3,\bar{F})$, and its composition with $\omega \mapsto \omega^{-1}$. Hence there is exactly one copy of A inside $\mathrm{SL}(3,\bar{F})$ up to conjugacy, and any faithful representation of A in $\mathrm{SL}(3,\bar{F})$ is conjugate to $\rho_A = \rho_0|A$.

If ρ_1 is any extension of ρ_A to H, then $\rho_1(hah^{-1}) = \rho_0(hah^{-1})$ for all $a \in A$ and $h \in H$. Hence $\rho_1(h)^{-1}\rho_0(h)$ lies in the centralizer Z of A in $\mathrm{SL}(3,\bar{F})$ for all $h \in H$, namely there is a character $\chi : H/A \to Z$ with $\rho_1 = \chi\rho_0$ on H. Such a character on $H/A = \mathrm{SL}(2,3) = Q_8 : C_3$ is trivial on the quaternion normal subgroup Q_8 of $\mathrm{SL}(2,3)$, the two nontrivial characters are denoted by χ_2, χ_3 in [12, p. 288]. This gives a total of 6 irreducible 3-dimensional representations. However, the image of χ_2, χ_3 is $Z \subset H$, and $\bar{H} = H$, where $h \mapsto \bar{h}$ is the automorphism of H defined by $\omega \mapsto \omega^2$. So up to conjugation in $\mathrm{SL}(3, \bar{F})$, the image of H in $\mathrm{SL}(3, \bar{F})$ is independent of the faithful representation used to embed H in $\mathrm{SL}(3, \bar{F})$. □

Scholium 5.5. To put the last paragraph in general perspective, let us recall some results in representation theory from [12]. Corollary 6.17 of [12] asserts: if $A \trianglelefteq H$ are finite groups, and $\rho \in \operatorname{Irr} H$ (= set of irreducible representations of H) is such that $\vartheta = \rho|A$ lies in $\operatorname{Irr} A$, then $\beta \otimes \rho$, $\beta \in \operatorname{Irr}(H/A)$, are irreducible, distinct for distinct β, and are all the irreducible constituents of $\vartheta^H = \operatorname{Ind}_A^H \vartheta$.

Chapter 11 of [12] starts by observing that if $\theta \in \operatorname{Irr} A$, $A \trianglelefteq H$, is invariant under H, namely $\theta^h : a \mapsto \theta(h^{-1}ah)$ is equivalent to θ for all $h \in H$, then for each irreducible constituent χ of θ^H there is $e(\chi) \in \mathbb{Z}_{>0}$ with $\chi_A = e(\chi)\theta$. Thus if θ extends to H (i.e., $e(\chi) = 1$ for some χ), then by [12, Corollary 6.17] the $e(\chi)$ are the degrees of the irreducible characters of H/A.

To determine when such a θ extends, recall that a function $\rho : H \to \mathrm{GL}(n, F)$ such that for all g, $h \in H$ there is $\alpha(g, h) \in F$ with $\rho(g)\rho(h) = \alpha(g, h)\rho(gh)$, is called a *projective* F-representation of H of degree n. The function $\alpha : H \times H \to F$ is called the *factor set* of ρ. It is uniquely determined by ρ, and nonzero. Equivalently, the composition ρ^* of ρ with the projection $g \mapsto g^*$, $\mathrm{GL}(n, F) \to \mathrm{PGL}(n, F)$, is a homomorphism.

Then Theorem 11.2 of [12] asserts: if $\theta \in \operatorname{Irr} A$, $A \trianglelefteq H$, is H-invariant, then there is a projective representation ρ of H with $\rho(aha') = \theta(a)\rho(h)\theta(a')$ for all a, $a' \in A$, $h \in H$. Any other projective representation ρ_1 of H satisfying this identity has the form $\rho_1 = \mu\rho$ for some character (that is, a multiplicative function) $\mu : H/A \to \bar{F}^\times$.

Finally Theorem 11.7 of [12] clarifies that θ extends to a representation ρ of H iff its factor set is trivial in $H^2(H/A, \bar{F}^\times)$.

Now in our case $H^2(H/A, \bar{F}^\times)$ is trivial, so the invariant irreducible representation ρ_A extends to a representation ρ of H in $\mathrm{GL}(3, \bar{F})$, where H is a group which induces the action of the normalizer $N = N_{\mathrm{SL}(3,\bar{F})}(A)$ of A in $\mathrm{SL}(3, \bar{F})$, namely for each $h \in H$ there is $y \in N$ with $a^h = a^y$, for all $a \in A$. As

$$C_{\mathrm{SL}(3,\bar{F})}(A) = Z(\mathrm{SL}(3, \bar{F})) = Z,$$

we have $H/Z = N/Z$. The subgroup AQ_8 of order $3^3 \cdot 2^3$ of H is isomorphic to the analogous group in N. If we take $H \subset \mathrm{SL}(3, \bar{F})$, then ρ is the embedding that extends ρ_A, the other representations are the twist with μ of order 3 and with its square, and those obtained on applying $\omega \mapsto \omega^{-1}$. If we take $H = A : \mathrm{SL}(2, 3)$, it has a faithful representation into $\mathrm{GL}(3, \bar{F})$, but not into $\mathrm{SL}(2, 3)$; the same for its twists and conjugates.

5.5. (E), (F) The subgroups $A : Q_8$, $A : C_4$ of H, orders $2^3 \cdot 3^3$, $2^2 \cdot 3^3$. The last sentence of the proof of the proposition of (G) applies to the subgroups (E), (F) too, as the image of H depends only on the image of A, which is uniquely defined up to conjugation.

Theorem 5.6. *Up to conjugacy,* $\mathrm{SL}(3, F)$ *contains at most one subgroup isomorphic to* $A = \langle S, T\rangle$, $A : \langle R\rangle$, $A : C_4$, $A : Q_8$, *the Hessian group* H (*with* $H/A = \mathrm{SL}(2, 3)$), A_5, *the Valentiner group* $3A_6$, $\mathrm{PSL}(2, 7)$, *provided that* $\mathrm{char}\, F$ *does not divide the order of the group in question, and* F *contains a* (*primitive*) 3*rd root of* 1.

Proof. As in the case of Theorem 4.1, this is just a corollary of Proposition 4.3 and Theorem 5.1. The centralizer of each of these groups in $\mathrm{SL}(3, F)$ is the center $C_3 = Z = \mathbb{Z}/3 = \langle \omega I\rangle$ of $\mathrm{SL}(3, F)$. As $H^1(F, \mathbb{G}_m) = \{0\}$, $H^1(F, \mathrm{SL}(3)) = \{0\}$ and $H^1(F, Z) = \{0\}$. As

$$1 \to Z \to \mathrm{SL}(3) \to \mathrm{PGL}(3) \to 1$$

is exact, so

$$Z \to \mathrm{SL}(3, F) \to \mathrm{PGL}(3, F) \to H^1(F, \mathbb{Z}/3) \to H^1(F, \mathrm{SL}(3)) = \{0\}$$

is exact, and $\mathrm{PSL}(3, F) = \mathrm{SL}(3, F)/\langle \omega I\rangle$, as the center of $\mathrm{SL}(3, F)$ is $\langle \omega I\rangle$. □

The groups in the Theorem of type (C′), (D′), (E), (F), (G), make a tower, each group contained in the next. The infinite reducible or decomposable families (A), (B), (C), (D), can be similarly analyzed. But note that the isomorphic subgroups $Z = \langle \omega I\rangle$ and $\langle S = \mathrm{diag}(1, \omega, \omega^2)\rangle$ are not conjugate in $\mathrm{SL}(3, \bar{F})$.

References

[1] A. BEAUVILLE, "Finite subgroups of $\mathrm{PGL}_2(K)$", in *Vector bundles and complex geometry*, Contemporary Mathematics, vol. 522, American Mathematical Society, 2010, p. 23-29.

[2] J. N. BRAY, D. F. HOLT & C. M. RONEY-DOUGAL, *The maximal subgroups of the low-dimensional finite classical groups*, London Mathematical Society Lecture Note Series, vol. 407, Cambridge University Press, 2013, xiv+438 pages.

[3] J. H. CONWAY, R. T. CURTIS, S. P. NORTON, R. A. PARKER & R. A. WILSON, *Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups*, Clarendon Press, 1985.

[4] H. S. M. COXETER, "The binary polyhedral groups and other generalizations of the quaternion group", *Duke Math. J.* **7** (1940), p. 367-379.

[5] L. E. DICKSON, *Linear Groups* (*with an exposition of the Galois field theory*), B. G. Teubner, 1901.

[6] L. DORNHOFF, *Group Representation Theory. Part A*: *Ordinary Representation Theory*, Pure and Applied Mathematics, vol. 7, Marcel Dekker, 1971.

[7] Y. Z. FLICKER, "Finite subgroups of $\mathrm{SL}(2, \bar{F})$ and automorphy", preprint.

[8] ———, "The finite subgroups of $\mathrm{SL}(3, \bar{F})$", preprint.

[9] ———, "Linearly reductive finite subgroup schemes of $\mathrm{SL}(3)$", preprint.

[10] D. Gorenstein, R. Lyons & R. Solomon, *The Classification of the Finite Simple Groups. Part I, Chapter A: Almost simple K-groups*, Mathematical Surveys and Monographs, vol. 40, American Mathematical Society, 1998, xvi+419 pages.

[11] B. Huppert, *Endliche Gruppen I*, Grundlehren der mathematischen Wissenschaften, vol. 134, Springer, 1967.

[12] I. M. Isaacs, *Character Theory of Finite Groups*, Pure and Applied Mathematics, vol. 69, Academic Press Inc., 1976, xii+304 pages.

[13] ———, *Finite Group Theory*, Graduate Studies in Mathematics, vol. 92, American Mathematical Society, 2008, xi+350 pages.

[14] H. H. Mitchell, "Determination of the ordinary and modular ternary linear groups", *American M. S. Trans.* **12** (2011), p. 207-242.

[15] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15** (1972), p. 259-331.

[16] ———, *Galois cohomology*, Springer, 1997, x+210 pages.

[17] ———, *Finite Groups: An Introduction*, Surveys of Modern Mathematics, vol. 10, International Press., 2016, ix+179 pages.

Yuval Z. Flicker
Ariel University, Ariel 40700, Israel
The Ohio State University, Columbus OH43210, USA
E-mail: yzflicker@gmail.com