Tits's construction of the Ree groups

Tits's construction of the Ree groups

Arjeh M. Cohen
CWI
Kruislaan 413
1098 SJ AMSTERDAM

§0 Introduction. Following Tits [3], we present a construction of the Ree groups (of the first kind), i.e., the groups of Lie type ${}^2G_2(F)$, where F is a field of characteristic 3 having an automorphism whose square is the Frobenius map $x \mapsto x^3$ on F. (Thus, if F is a finite field, it has order $q = 3^{2m+1}$ for some natural number m.) For any such field F, the corresponding group is defined as a subgroup of the projective linear group PGL(7,F) stabilizing a specified set of projective points, on which it acts as a doubly transitive permutation group. We shall also discuss its normal structure. The merit of the construction is that no knowledge of Lie algebras or any other theory beyond some elementary facts from number theory, linear algebra and group theory is required. A disadvantage of the construction is that quite a few computational checks are involved of formulae that seem to have come out of the blue. This is at least partly due to the lack of (sufficient) geometry in these notes. The geometry behind it all, as well as an identification of the groups constructed here with the "classical" Ree groups can be found in Tits [3]. We mention here that from the intricate classification of finite groups of Ree type, finished by Bombieri [1] in 1980, it immediately follows that for finite fields F "our groups" are isomorphic to the "classical" Ree groups.
I am grateful to Professor Tits for elucidating parts of the text in [3], some helpful comments on an earlier version of these notes, and for supplying Formulae (1.2) below. These formulae were checked on a computer by A.E. Brouwer.

For the duration of these notes, we let F stand for a field of characteristic 3 with a nontrivial automorphism σ whose square σ^2 is the Frobenius map 3. (When applied to an element of F, these maps appear in the exponent; this justifies the notation for the Frobenius map.) If F is finite of order 3^{2m+1}, then $\sigma = 3^{m+1}$. Finally, F^* denotes the multiplicative group of F.

§1 The construction. For $x,y,z \in F$, denote by $\gamma(x,y,z)$ the projective point whose homogeneous coordinates are $(x,y,z,1,u,v,w)$, where

(1.1a) $$u = x^2y + xz + y^\sigma - x^{\sigma+3},$$

(1.1b) $$v = x^\sigma y^\sigma + z^\sigma + xy^2 - yz - x^{2\sigma+3},$$

and

(1.1c) $$w = -z^2 - xv - yu.$$

Furthermore, put $\gamma_0 = \gamma(0,0,0)$, and let ∞ be the projective point whose homogeneous coordinates are $(0,0,0,0,0,0,1)$. Set $\Gamma_\infty = \{\gamma(x,y,z) \mid x,y,z \in F\}$ and $\Gamma = \Gamma_\infty \cup \{\infty\}$. The group ${}^2G_2(F)$ is defined as the group of all (nonsingular) projective linear transformations leaving Γ invariant. Elements of the group $PGL(7,F)$ of all projective linear transformations are thought of as matrices, determined up to a nonzero scalar factor, operating from the left on column vectors.

We end this section with some useful formulae. If $(x,y,z,1,u,v,w)$ are the homogeneous coordinates of $\gamma(x,y,z)$, then

(1.2a) $$v^{\sigma+1} + (w^2y-v^2u-vwz)^{\sigma^{-1}}w - uw^\sigma = 0$$

(1.2b) $$(uxz+u^2-x^2w)^{\sigma^{-1}}v - u^\sigma z + (uwz+w^2x-u^2v)^{\sigma^{-1}}y = 0$$

(1.2c) $$y^\sigma - u + (v+yz-y^2x)^{\sigma^{-1}}x = 0$$

(1.2d) $$v^{\sigma+2} + (uwz+w^2x-u^2v)^{\sigma^{-1}}w^2 - (uv+zw)w^\sigma = 0$$

These formulae can be verified by applying σ to both sides of the equations and subsequently replacing u,v,w by expressions in x,y,z using (1.1). These verifications are both tedious and straightforward.

§2 <u>The subgroups</u> B, U, H, <u>and</u> G <u>of</u> ${}^2G_2(F)$. For $a,b,c \in F$ there is a unique projective linear transformation $t_{a,b,c}$ in ${}^2G_2(F)$ extending the map on Γ given by

(2.1) $$\begin{cases} \gamma(x,y,z) \mapsto \gamma(x+a, a^\sigma x+y+b, (a^{\sigma+1}-b)x+ay+z+c) \\ \infty \mapsto \infty \end{cases}$$

It is, again, straightforward to check this, so the proof is omitted.

Given a,b,c,d,e,f we have the following multiplication rule.

(2.2) $t_{a,b,c}t_{d,e,f} = t_{a+d,b+e+a^{\sigma}d,f+c+a^{\sigma+1}d-bd+ea}$

Thus $U := \{t_{a,b,c} | a,b,c \in F\}$ is a subgroup of $^2G_2(F)$ fixing ∞ and regular on Γ_∞. Its center Z(U) coincides with its ~~commutator~~ subgroup $[U',U]$; where $U' = [U,U]$

(2.3) $Z(U) = [U',U] = \{t_{0,0,c} | c \in F\}$. <u>In particular</u>, <u>U is nilpotent</u>.

Next, for $k \in F\backslash\{0\}$, let h_k be the projective linear transformation whose matrix is of diagonal form with diagonal entries $(k,k^{\sigma+1},k^{\sigma+2},1,k^{\sigma+3},k^{2\sigma+3},k^{2\sigma+4})$. Then

(2.4) $h_k\,\gamma(x,y,z) = \gamma(kx,k^{\sigma+1}y,k^{\sigma+2}z)$ $(x,y,z \in F)$,

so $H := \{h_k | k \in F^*\}$ is a subgroup of $^2G_2(F)$ fixing ∞, γ_0, and normalizing U. Thus B = UH is a subgroup of $^2G_2(F)$ fixing ∞. It is readily seen that [B,B] = U. In fact, we need the following slightly stronger statement later on. Let B' be a subgroup of B properly containing $\langle h_{-1},U\rangle$. Then

(2.5) $[B',B'] = U$.

<u>Proof</u>: Use (2.3) and $[h_k,t_{a,b,c}] = h_k t_{a,b,c} h_k^{-1} t_{a,b,c}^{-1} \in t_{((k-1)a,(k^{\sigma+1}-1)b-(k^{\sigma}-1)a^{\sigma+1},0)}Z(U)$ for all $a,b \in F$ and $k \in F^*\backslash\{\pm1\}$ such that $h_k \in B'$ to derive $U \leqslant [B',B']$. Since $B'/U \cong H/(U \cap H)$ is abelian, the converse inclusion also holds. Hence (2.5).

Finally, denote by ω the involutory projective linear transformation determined by the permutation $(e_x,e_v)(e_y,e_u)(e_t,e_w)$ of the standard basis $e_x,e_y,e_z,e_t,e_u,e_v,e_w$ of F^7, and set $G = \langle B,\omega\rangle$, the group generated by B and ω. We claim

(2.6) G <u>is a subgroup of</u> $^2G_2(F)$.

<u>Proof</u>. In view of the above and since $\omega(\infty) = \gamma_0$, we need only show that ω preserves $\Gamma_\infty\backslash\{\gamma_0\}$ in order to establish this claim. First of all, we assert that if (x,y,z,1,u,v,w) represents the point $\gamma(x,y,z)$ of $\Gamma_\infty\backslash\{\gamma_0\}$, then $w \neq 0$.
For suppose w = 0, then by (1.2a), we get v = 0, and hence, by (1.2b) either u = 0 or z = 0. Thus $z^2 = uy = 0$ in view of (1.1c).

Hence $u = 0$ thanks to (1.2c). It follows, again by (1.2c), that $y^\sigma = (y^2x)^{\sigma-1}x$, so that either $y = 0$ or $y = x^{\sigma+1}$. Consequently, by (1.1b), $x = y = z = 0$, which is in conflict with $\gamma(x,y,z) \neq \gamma_0$. This proves that $w \neq 0$, indeed.

In order to finish the proof of (2.6), notice that for $\gamma(x,y,z) \in \Gamma_\infty\setminus\{\gamma_0\}$, we have

$$(2.7) \qquad \omega\,\gamma(x,y,z) = \gamma\left(\frac{v}{w}, \frac{u}{w}, \frac{z}{w}\right).$$

From (1.2a), (1.2d), and (1.1c), the defining equations (1.1) for $\gamma\left(\frac{v}{w}, \frac{u}{w}, \frac{z}{w}\right) \in \Gamma_\infty$ follow.

Later on we shall use that ω normalizes H, or, more precisely,

$$(2.8) \qquad \omega\, h_k \omega^{-1} = h_{k^{-1}} \qquad (k \in F^*).$$

§3 <u>Some geometry</u>. We recall that a quadratic form Q on F^7 is a homogeneous polynomial on F^7 (in the variables x,y,z,t,u,v,w, say) of degree 2. The <u>quadric associated with</u> Q is the set of projective points whose homogeneous coordinates $p = (x,y,z,t,u,v,w)$ satisfy $Q(p) = 0$. (Notice that this definition is indeed independent of the choice of homogeneous coordinates.) The quadric determines Q up to a scalar multiple. In view of (1.1c) and a quick check for ∞, all points of Γ are easily seen to belong to the quadric associated with Q_0, where

$$(3.1) \qquad Q_0(p) = tw + xv + yu + z^2 \qquad (p = (x,y,z,t,u,v,w) \in F^7).$$

The converse also holds:

<u>The quadric associated with</u> Q_0 <u>is the only quadric containing</u> Γ.

<u>Proof</u>. The set A of points of Γ defined over the ground field $\mathbb{F}_3$ consists of $3^3 + 1 = 28$ points. On the other hand, the vector space of all quadratic forms on F^7 has a natural basis Φ consisting of the 28 monomials on F^7 of degree 2 (with coefficient 1). Consider the 28×28-matrix whose rows (columns) are indexed by the elements of A (resp. Φ) and whose a,φ entry for $a \in A$, $\varphi \in \Phi$ is $\varphi(a)$. Straightforward computation yields that the rank of this matrix is 27. This means that there is a unique quadric containing A. Hence (3.2).

There is a standard way to obtain an inner product from the quadratic form Q_0, namely

$$(p,q) \mapsto Q_0(p+q) - Q_0(p) - Q_0(q) \qquad (p,q \in F^7).$$

Given a subset X of F^7, we denote by $X^\perp$ the subset of F^7 consisting of all vectors perpendicular to X with respect to this inner product. Recall that $e_x, e_y, e_z, e_t, e_u, e_v, e_w$ denote the standard basis of F^7, and observe that e_t, e_w are homogeneous coordinates for γ_0, ∞, respectively.

The linear subspaces $\{x = y = u = 0\}$, $\{x = z = v = 0\}$ and $\{y = u = v = 0\}$ of F^7 are exceptional in the sense that they contain "more" points of Γ than an "average" 4-dimensional subspace could have. The following statement is based on this phenomenon.

(3.3) <u>Let</u> (p,p') <u>be an ordered pair of nonzero vectors in</u> $\{e_t,e_w\}^\perp$ <u>such that for each</u> $\lambda \in F$ <u>there is a point in</u> Γ <u>whose homogeneous coordinates are</u> $\lambda p + \lambda^\sigma p' + e_t + we_w$ <u>for some</u> $w \in F$. <u>Then</u> (p,p') <u>is one of</u> (e_z,e_v), (e_y,e_u), <u>up to nonzero scalar multiplications of both</u> p <u>and</u> p'.

<u>Proof</u>. Write $p = (x,y,z,0,u,v,0)$ and $p' = (x',y',z',0,u',v',0)$. Then, for $\lambda \in F$, the projective point with homogeneous coordinates $\lambda p + \lambda^\sigma p' + e_t + we_w$ for some $w \in F$ belongs to Γ if and only if (1.1a) and (1.1b) are satisfied for this vector, i.e., if and only if the following two formulae hold.

(3.4a)
$$\begin{cases} \lambda u + \lambda^\sigma(u'-y^\sigma) - \lambda^3(x^2y+y'^\sigma) - \lambda^{\sigma+2}(x^2y'-xx'y) \\ - \lambda^{2\sigma+1}(x'^2y-xx'y') - \lambda^{3\sigma}x'^2y' - \lambda^2xz - \lambda^{\sigma+1}(x'z+xz') \\ + \lambda^{\sigma+3}(x^{\sigma+3}) - \lambda^{2\sigma}x'z' + \lambda^{4\sigma}x^\sigma x'^3 \\ + \lambda^6x'^\sigma x^3 + \lambda^{3\sigma+3}x'^{\sigma+3} \qquad = 0 \end{cases}$$

(3.4b)
$$\begin{cases} \lambda v + \lambda^\sigma(v'-z^\sigma) - \lambda^{2\sigma}(x^\sigma y^\sigma-y'z') - \lambda^{\sigma+3}(x'^\sigma y^\sigma+y'^\sigma x^\sigma) - \lambda^6x'^\sigma y'^\sigma \\ - \lambda^3(xy^2+z'^\sigma) - \lambda^{\sigma+2}(x'y^2-xyy') - \lambda^{2\sigma+1}(xy'^2-x'yy') \\ - \lambda^{3\sigma}x'y'^2 + \lambda^2yz + \lambda^{\sigma+1}(y'z+z'y) + \lambda^{2\sigma+3}x^{2\sigma+3} \\ + \lambda^{5\sigma}x^{2\sigma}x'^3 - \lambda^{\sigma+6}x^{\sigma+3}x'^\sigma - \lambda^{4\sigma+3}x^\sigma x'^{\sigma+3} \\ + \lambda^9x'^{2\sigma}x^3 + \lambda^{3\sigma+6}x'^{2\sigma+3} \qquad = 0 \end{cases}$$

The hypothesis of (3.3) implies that these two equations hold for all $\lambda \in F$. By a standard result in algebra, cf. Bourbaki [2] §5, this implies that the coefficients of most monomials occurring in the left hand sides, viewed as polynomials in λ and λ^σ, vanish. In the case of small fields, however, a little caution is in order. (Recall that $F \neq \mathbb{F}_3$.) If $F = \mathbb{F}_{27}$, then $\sigma = 9$, so that, for instance, $\lambda^{4\sigma} = \lambda^{\sigma+1}$. Nevertheless, in each of the equations (3.4), the monomials $\lambda, \lambda^2, \lambda^3, \lambda^\sigma, \lambda^{2\sigma+3}$, and $\lambda^{3\sigma+6}$ do not occur in more than one "guise" over any field F under consideration, so their coefficients vanish. Thus,
$u = v = yz = x^2y+y'^\sigma = xy^2+z'^\sigma = u'-y = v'-z^\sigma = x^{2\sigma+3} = x'^{2\sigma+3} = 0.$
It immediately follows that either $p = ze_z$ and $p' = z^\sigma e_v$, or $p = ye_y$ and $p' = y^\sigma e_u$, according as $y = 0$ or $z = 0$. This settles (3.3).

§4 The structure of $^2G_2(F)$. The group of all projective linear transformations preserving the quadric accociated with Q_0, is a classical group of Lie type $B_3(F)$. It will be denoted PGO(7,F). As a direct consequence of (3.2), we have

(4.1) $^2G_2(F)$ is a subgroup of PGO(7,F).

This observation and (3.3) enable us to determine $^2G_2(F)$.

(4.2) The stabilizer in $^2G_2(F)$ of γ_0 and ∞ coincides with H.

Proof. First of all, notice that ω interchanges γ_0 and ∞, and hence normalizes the stabilizer in question.
Suppose $g \in {}^2G_2(F)$ stabilizes both γ_0 and ∞. Then we may view g as a nonsingular matrix fixing e_t and transforming e_w to a scalar multiple of itself. In view of (4.1), the set $\{e_t,e_w\}^\perp$ is also preserved by g. Hence, g preserves the set of all ordered pairs (p,p') of vectors in F^7 with the property that for each $\lambda \in F$ there is $w \in F$ such that $\lambda p + \lambda^\sigma p' + e_t + we_w$ represents a point of Γ. But the latter set has only two elements according to (3.3). These two elements behave differently under ω, as

$$\omega(e_z,e_v) = (e_z,e_x),$$

while

$$\omega(e_y,e_u) = (e_u,e_y).$$

Thus, $g(e_y,e_u)$ cannot be equal to $(\lambda e_z,\mu e_v)$ for some $\lambda,\mu \in F$, [for otherwise, $\omega g\omega(e_y) = \omega g(e_u) = \omega(\mu e_v) = \mu e_x$; but $\omega g\omega$ stabilizes both γ_0 and ∞, so, according to (3.3) should map e_y to a nonzero scalar multiple of e_y or e_z, a contradiction]. It follows that g fixes the projective points with homogeneous coordinates e_z,e_v, e_y,e_u and, as $e_x = \omega(e_v)$, also e_x. In other words, g has diagonal form, with diagonal, say,

$$(\alpha,\beta,\gamma,1,\zeta,\eta,\theta).$$

Now, H is contained in the stabilizer of γ_0 and ∞, so after multiplication by $h_{\alpha^{-1}}$, a member of H, we may assume that $\alpha = 1$. By (1.1) applied to $g\gamma_{(1,0,0)}$, we get $\zeta = \eta = \theta = 1$. The same argument for $\omega g\omega$ yields $\beta = \gamma = 1$, whence $g = 1 \in H$.
The conclusion is that H is indeed the stabilizer in ${}^2G_2(F)$ of γ_0 and ∞. This finishes the proof of (4.2).

The importance of (4.2) lies in the following immediate consequence

(4.3) $G = {}^2G_2(F) = B \cup U\omega B$, <u>with uniqueness of expression at the right hand side</u>. <u>In particular</u>, ${}^2G_2(F)$ <u>is a doubly transitive permutation group of</u> Γ <u>with point stabilizer</u> B <u>and two point stabilizer</u> H.

In particular,

(4.4) <u>If</u> F <u>is finite of order</u> $q = 3^{2m+1}$, <u>then</u> $|U| = q^3$ <u>and</u> $|H| = (q-1)$, <u>so</u> $|B| = q^3(q-1)$ <u>and</u> $|{}^2G_2(F)| = q^3(q^3+1)(q-1)$.

§5 The normal structure of ${}^2G_2(F)$.

Let N be the subgroup of $G = {}^2G_2(F)$ generated by U and all its conjugates. We first show that N comprises quite a lot of G. Consider the following identities in G.

(5.1a) $\omega t_{0,0,1}\omega = t_{-1,0,-1}\omega t_{-1,1,-1}$,

(5.1b) $\omega t_{1,1,0}\omega = t_{1,1,0}\omega t_{1,-1,0}h_{-1}$.

These identities are easily verified by use of (2.1), (2.4) and (2.7). In fact, the permutations of Γ on both hand sides of either equation (5.1) have the same images on ∞, γ_0, and $\gamma(1,0,0)$, so that they must be equal according to (4.2).

Now, (5.1a) shows that ω belongs to N, and this, together with (5.1b) results in $h_{-1} \in N$. Since N is normal in G, we also obtain that $h_{k^2} = h_k \omega h_{k^{-1}} \omega$ is in N for every $k \in F^*$. Thus, N contains U, ω and the subgroup of H generated by all h_{k^2} for $k \in F^*$ and h_{-1}. In view of (4.3) this yields

(5.2) G = HN, <u>and</u> $G/N \cong F^*/F'$, <u>where</u> F' <u>is a subgroup of</u> F* <u>containing all nonzero squares and</u> -1.

(The second part of the statement follows from the first part by the First Isomorphism Theorem.) From this, we derive

(5.3) $[G,G] = N = [N,N]$.

<u>Proof</u>. Since $[B,B] = U$ (cf. (2.5)), we have $U \subseteq [G,G]$. As $[G,G]$ is normal in G, it follows that $N \subseteq [G,G]$. But G/N is abelian by (5.2), so $N \supseteq [G,G]$, and the first equality is established. As for the second equality, by (2.5) applied to $B' = B \cap N$, we have that $U \subseteq [N,N]$. Since $[N,N]$ is characteristic in N and N is normal in G, the group $[N,N]$ is normal in G, too, so that $N \subseteq [N,N]$, whence $N = [N,N]$, and we are done.

We are now in a position to prove the main result of this section.

(5.4) N <u>is a simple group</u>. <u>Thus, any nontrivial normal subgroup of</u> G <u>must contain</u> N.

<u>Proof</u>. Let M be a nontrivial normal subgroup of N. As N is doubly transitive on Γ (it contains U, ω and all conjugates), M must be transitive. This means that $N = M(B \cap N)$, implying $G = NH = MB$ (cf. 5.2). Hence, if $g \in G$, there are $m \in M$ and $b \in B$ with $g = mb$, so that $gUg^{-1} = mUm^{-1} \subseteq MUM = UM$ (as U is normal in B and contained in N). This shows that any conjugate of U is contained in UM. Therefore, N = UM, and, by the First Isomorphism Theorem, $N/M \cong U/U \cap M$. But the right hand side represents a nilpotent group (cf. (2.3)) while, due to (5.3), the left hand side is its own commutator subgroup.
This can only happen if $N/M \cong \{1\}$, i.e., M = N.

Since -1 is not a square in F and the subgroup of F* of all squares has index 2 if F is finite, it follows that

(5.5) <u>If</u> F is <u>finite</u>, <u>then</u> G <u>is simple</u>.

§6 References

[1] Bombieri, E., Thompson's problem ($\sigma^2 = 3$), Inventiones Math. 58 (1980) 77-100.

[2] Bourbaki, N., Algèbre, Chap. 7, Hermann, Paris.

[3] Tits, J., Les groupes simples de Suzuki et de Ree, Séminaire Bourbaki, 210, 1960/61.

§7 Exercises. Show that

(7.1) There exist fields F as described in §1 such that F^* does not coincide with its subgroup generated by -1 and the nonzero squares.

(7.2) For each pair of points of Γ with homogeneous coordinates p,q, respectively, we have $p \notin \{q\}^{\perp}$.

(7.3a) Each pair of points of Γ is fixed by a unique involution in G. Given such a pair γ,δ denote by $\ell_{\gamma,\delta}$ the set of points fixed by the corresponding involution. Thus $\gamma,\delta \in \ell_{\gamma,\delta}$.

(7.3b) G is transitive on the set $\{\ell_{\gamma,\delta} \mid \gamma,\delta \in \Gamma,\ \gamma \neq \delta\}$.

(7.3c) The stabilizer in G of $\ell_{\gamma,\delta}$ is doubly transitive on the set $\ell_{\gamma,\delta}$, and contains a subgroup isomorphic to the projective special linear group PSL(2,F).

(7.4) Determine ${}^2G_2(F)$ for $F = \mathbb{F}_3$. Prove that ${}^2G_2(F) \cong \mathrm{Aut}\ PSL(2,8)$ in this case.

2 december 1983