RESOLVENTS OF CERTAIN LINEAR GROUPS IN A FINITE FIELD

L. CARLITZ

1. Introduction. Let $F_q = GF(q)$ denote the finite field of order $q = p^n$, where p is a prime. Consider the group Γ of linear transformations

$$x' = (ax + b)/(cx + d) \tag{1.1}$$

with coefficients $a, b, c, d \in F_q$ and of determinant 1. The order of Γ is $\frac{1}{2}q(q^2 - 1)$ or $q(q^2 - 1)$ according as q is odd or even, i.e., according as $p > 2$ or $p = 2$. Put

$$J = J(x) = Q^{\frac{1}{2}(q+1)}L^{-\frac{1}{2}(q^2-q)} \qquad (p > 2), \tag{1.2}$$

where

$$L = x^q - x, \; Q = (x^{q^2} - x)/(x^q - x) = L^{q-1} + 1; \tag{1.3}$$

when $p = 2$ the factor $\frac{1}{2}$ in the exponents in the right member of (1.2) is omitted. It is familiar that L is the product of distinct linear polynomials $x + a$ and Q is the product of distinct irreducible quadratics $x^2 + ax + b$. Moreover (**1**, p. 4) J is an absolute and fundamental invariant of Γ, that is, every absolute invariant is a rational function of J. The equation

$$J(x) = y, \tag{1.4}$$

where y is an indeterminate, is normal over $F_q(y)$ with Galois group Γ.

If we put $u = L^{\frac{1}{2}(q-1)}$ or L^{q-1} according as $p > 2$ or $p = 2$, then (1.2) and (1.4) imply

$$(u^2 + 1)^{\frac{1}{2}(q+1)} = yu^q \qquad (p > 2), \tag{1.5}$$

$$(u + 1)^{q+1} = yu^q \qquad (p = 2), \tag{1.6}$$

resolvents of degree $q + 1$. The principal object of the present paper is to construct resolvents of lower degree when they occur. It is well known (see for example (**2**, p. 287)) that Γ can be represented as a permutation group of degree $\leqslant q$ only when

$$q = 5, 7, 9, 11, \tag{1.7}$$

in which case the degree is 5, 7, 6, 11, respectively. Resolvents are constructed for the minimum degree in each case. For example when $q = 5$ the quintic resolvent is

$$t^5 - 2t^3 = J, \tag{1.8}$$

while for $q = 7$ we get

$$w^7 + 4w^5 - 4w^4 = J. \tag{1.9}$$

Received October 8, 1955.

When $q = 4$, (1.6) is a quintic. In this case we construct a sextic resolvent

$$t^6 + t^5 = J. \tag{1.10}$$

Incidentally when $q = 9$, we again get the equation (1.10). However it should be observed that in the one case (1.10) has group $\mathfrak{A}_5$ while in the other the group is $\mathfrak{A}_6$.

Finally in §7 we consider briefly the ternary linear group. For $q = 2$ the group is of order 168 and we construct a resolvent of degree 8. In this case the resolvent of degree 7 is easily found (compare the case $q = 4$).

For the discussion of the corresponding problems in the classical case the reader is referred to (**3**, Ch. 13; **5**; **7**).

2. $q = 5$. In this case Γ is icosohedral and has a tetrahedral subgroup generated by

$$x' = -x, \qquad x' = \frac{x+2}{x-2}. \tag{2.1}$$

This gives rise to the 12 functions

$$\pm x, \pm \frac{1}{x}, \pm \frac{x+2}{x-2}, \pm \frac{x-2}{x+2}, \pm 2\frac{x+2}{x-2}, \pm 2\frac{x-2}{x+2}. \tag{2.2}$$

Applying the second of (2.1) to $(x^4 + 1)/x^2$ we get

$$t = T/L^2, \tag{2.3}$$

where

$$T = T(x) = x^{12} + 2x^8 + 2x^4 + 1. \tag{2.4}$$

Since $x^4 + 1 = (x^2 + 2)(x^2 - 2)$, it is clear that T is the product of six irreducible quadratics. Consequently

$$Q = TU, \tag{2.5}$$

where U is a polynomial of degree 6; we find that

$$U = U(x) = x^8 - x^4 + 1. \tag{2.6}$$

Since the function (2.3) belongs to a tetrahedral subgroup of Γ, it must satisfy an equation of degree 5 with coefficients in $F_5(J)$. While this equation can be found by the method of undetermined coefficients it is easier to make use of the identity

$$T^2(x) - U^3(x) = 2L^4, \tag{2.7}$$

which can be verified without difficulty. Incidentally (2.7) is one of a set of five identities obtained by replacing x by $x + c$, $c = 0, 1, 2, 3, 4$. Using (2.3), (2.6), (2.7) we get

$$t^5 - 2t^3 = J. \tag{2.8}$$

This proves

THEOREM 1. *For* $q = 5$, (1.4) *admits the quintic resolvent* (2.8).

It may be noted that Garrett **(6)** has proved that a quintic equation in a field of characteristic 5 can in general be reduced to the form

$$z^5 + az^2 + b = 0. \tag{2.9}$$

Replacing t by $1/z$ in (2.8), we evidently get an equation of the form (2.9).

3. $q = 7$. The group Γ is now the simple group $LF(2, 7)$ of order 168. We require a subgroup $\mathfrak{S}_4$ of order 24. Such an octahedral subgroup is generated by

$$s_1 = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}, \quad s_2 = \begin{pmatrix} 3 & 4 \\ 1 & 4 \end{pmatrix}, \quad s_3 = \begin{pmatrix} 0 & 3 \\ 1 & -2 \end{pmatrix}. \tag{3.1}$$

The transformations s_1, s_2 generate a dihedral subgroup $\mathfrak{D}_4$ of order 8; a function belonging to $\mathfrak{D}_4$ is

$$\xi = (x^2 + 2x - 2)^4/L. \tag{3.2}$$

Applying s_3 to ξ we find that

$$t = T^4/L^3, \tag{3.3}$$

where

$$T = (x^2 + 2x - 2)(x^2 + 4x - 1)(x^2 + x - 4) = x^6 - x^3 - 1 \tag{3.4}$$

belongs to the group $\mathfrak{S}_4$. Consequently t satisfies an equation of degree 7. It is however more convenient to find the equation of degree 7 satisfied by

$$w = t - 4 = W/L^3, \tag{3.5}$$

where

$$W = T^4 - 4L^3. \tag{3.6}$$

We observe first that $W|Q$. To prove this let $\alpha^6 = -1$, $\alpha \in GF(7^2)$. Then by (3.4), $T(\alpha) = -\alpha^3 - \alpha$, which implies $T^4(\alpha) = 3\alpha^3$; also $L^3(\alpha) = (\alpha^7 - \alpha)^3$, so that

$$W(\alpha) = 3\alpha^3 + 4\alpha^3 = 0.$$

This implies $x^6 + 1|W(x)$. Now applying the substitution s_1, we find that W is a product of distinct irreducible quadratics, in particular it is clear that $W|Q$. Also (3.6) implies $(W, T) = 1$. We have accordingly

$$Q = TWU, \tag{3.7}$$

where U is a polynomial of degree 12.

Returning to (3.5) we now construct the equation of degree 7 satisfied by w. This is evidently of the form

$$w^7 + a_1w^6 + \ldots + a_6w = bJ$$

or what is the same thing

$$W^7 + a_1W^6L^3 + \ldots + a_6WL^{18} = bQ^4. \tag{3.8}$$

It follows immediately from (3.7) that $a_4 = a_5 = a_6 = 0$; also $b = 1$. Since

$W = x^{24} - 4x^{21} + \ldots$, comparison of coefficients yields $a_1 = 0$, $a_2 = 4$, $a_2 + a_3 = 0$. Thus (3.8) reduces to

$$W^7 + 4W^5L^6 - 4W^4L^9 = Q^4. \tag{3.9}$$

In terms of w this is

$$w^7 + 4w^5 - 4w^4 = J. \tag{3.10}$$

This proves

THEOREM 2. *For $q = 7$ (1.4) admits the resolvent (3.10) of degree seven.*

If we substitute from (3.7), (3.9) becomes

$$W^3 + 4WL^6 - 4L^9 = T^4U^4. \tag{3.11}$$

Next using (3.6) we get

$$T^8 + 2T^4L^3 + 3L^6 = U^4. \tag{3.12}$$

In terms of T above, (3.12) becomes

$$(T^4 - 4L^3)^4 (T^{12} + 2T^8L^3 + 3T^4L^6) = Q, \tag{3.13}$$

from which the equation for t follows at once:

$$(t - 4)^4 (t^3 + 2t^2 + 3t) = J. \tag{3.14}$$

This equation can also be obtained directly from (3.10).

Concerning the polynomials T, U, W we may state

THEOREM 3. *The polynomials T, U, W satisfy* (3.6), (3.7), (3.11), (3.12).

4. $q = 11$. The group Γ is now the simple group $LF(2, 11)$, of order 660. We require a subgroup $\mathfrak{A}_5$ of order 60. Such an icosahedral subgroup is generated by (see for example (**4**, p. 479))

$$s_1 = \begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix}, \quad s_2 = \begin{pmatrix} 3 & 1 \\ 1 & -3 \end{pmatrix} \tag{4.1}$$

of period 5 and 2, respectively. Note that

$$s_1 s_2 = \begin{pmatrix} 1 & 4 \\ 1 & -3 \end{pmatrix}, \tag{4.2}$$

which is of period 3. It is easily seen that $(x^2 + 1)/(x - 3)$ is invariant under s_2 and next that $(x^{10} + 1)/(x^5 - 1)$ is invariant under (4.1). A little computation now shows that

$$t = T^2/L^5, \tag{4.3}$$

where

$$T = x^{30} + 5x^{25} + 5x^{20} + 5x^{10} - 5x^5 + 1, \tag{4.4}$$

belongs to $\mathfrak{A}_5$. Notice that T is a product of distinct irreducible quadratics, so that $T|Q$.

https://doi.org/10.4153/CJM-1956-062-6 Published online by Cambridge University Press

In the next place application of s_1 to the quadratic $x^2 - 5x + 2$ gives $H_1 = x^{10} + 5x^5 - 1$. Applying $s_2 s_1^3$ to $x^2 - 5x + 2$ we get $x^2 - 4x + 2$ and this gives $H_2 = x^{10} - 2x^5 - 1$. If we put

$$H = H_1 H_2 = x^{20} + 3x^{15} - x^{10} - 3x^5 + 1 \tag{4.5}$$

we find that

$$h = H^3/L^5 \tag{4.6}$$

also belongs to $\mathfrak{A}_5$. Note that H, like T, is a product of distinct irreducible quadratics. Moreover it is not difficult to verify that T and H satisfy the relation

$$T^2 - H^3 = L^5; \tag{4.7}$$

in terms of t and h this is

$$t - h = 1. \tag{4.8}$$

(For the polynomials corresponding to T, H and L in the classical case, see **(5**, p. 54**)**. The differentiation method used there is however not applicable here.)

Since (4.7) implies $(T, H) = 1$, it follows that

$$Q = THU, \tag{4.9}$$

where U is a polynomial of degree 30. It is also easily verified that

$$u = U/L^5 \tag{4.10}$$

belongs to the group $\mathfrak{A}_5$. Thus each of the functions t, h, u satisfies an equation of degree 11, which we shall now set up. We notice first that

$$U = T^2 + 4L^5. \tag{4.11}$$

To prove (4.11) put $\phi(x) = (U - T^2)/L^5$ and let β be a number in some extension of F_q such that β and its conjugates under $\mathfrak{A}_5$ are distinct; we may, for example, take β as the root of an irreducible polynomial of the third degree. Then since $\phi(x)$ is invariant under $\mathfrak{A}_5$ we have $\phi(\beta_i) = \phi(\beta)$, where β_i is any conjugate of β under $\mathfrak{A}_5$. Then $\phi(x) - \phi(\beta)$ vanishes for 60 distinct values of x; since $\deg \phi(x) < 60$ it follows that $\phi(x)$ is constant. Comparison of coefficients now yields (4.11). Incidentally (4.7) can be proved in a similar way.

Making use of (4.11) it is not difficult to find the equation of degree 11 satisfied by u. This equation is of the form

$$u^{11} + a_1 u^{10} + \ldots + a_{10} u = J$$

or what is the same thing

$$U^{11} + a_2 U^{10} L^5 + \ldots + a_{10} U L^{50} = Q^6. \tag{4.12}$$

Since $U | Q$ we have $a_6 = \ldots = a_{10} = 0$. Also since all terms in Q have exponents divisible by 10, it is clear that $a_1 = 0$. Thus (4.12) becomes

$$U^5 + a_2 U^3 L^{10} + \ldots + a_5 L^{25} = T^6 H^6. \tag{4.13}$$

Using (4.7) and (4.11) we may rewrite (4.13) in terms of T; the resulting

https://doi.org/10.4153/CJM-1956-062-6 Published online by Cambridge University Press

relation is of degree 10 and must therefore be an identity in T. Comparing coefficients we readily find that

$$a_2 = 6,\ a_3 = 3,\ a_4 = 3,\ a_5 = a_6.$$

Thus (4.12) becomes

$$U^{11} + 6U^9L^{10} + 3U^8L^{15} + 3U^7L^{20} + 6U^6L^{25} = Q^6, \tag{4.14}$$

and therefore

$$u^{11} + 6u^9 + 3u^8 + 3u^7 + 6u^6 = J. \tag{4.15}$$

We may rewrite (4.14) as

$$U^5 + 6U^3L^{10} + 3U^2L^{15} + 3UL^{20} + 6L^{25} = T^6H^6$$

and remark that the left member is

$$\begin{aligned}(U - 5L^5)^2(U^3 - U^2 + 4U + 2)\\ = (U - 5L^5)^2(U - 4L^5)^3\\ = (T^2 - L^5)^3T^6 = H^6T^6,\end{aligned}$$

by (4.7) and (4.11), which is correct. Conversely we may obtain (4.14) by retracing these steps.

In view of the above it is convenient to rewrite (4.15) as

$$u^6(u - 5)^2(u - 4)^3 = J. \tag{4.16}$$

The corresponding equations for t and h are

$$t^3(t - 1)^2(t + 4)^6 = J \tag{4.17}$$

and

$$h^2(h + 1)^3(h + 5)^6 = J. \tag{4.18}$$

We may state

THEOREM 4. *For* $q = 11$, (1.4) *admits the resolvents* (4.16), (4.17), (4.18) *of degree* 11.

THEOREM 5. *The polynomials* T, H, U *satisfy* (4.7), (4.9), (4.11) *and* (4.14).

5. $q = 4$. When $q = 4$, the equation (1.6) becomes

$$(u + 1)^5 = yu^4, \tag{5.1}$$

where $u = (x^4 - x)^3$. Thus (5.1) is a quintic resolvent of (1.4). The group in this case is $\mathfrak{A}_5$. We shall construct a sextic resolvent. This can be done most rapidly by making use of an irreducible quadratic, say

$$P = x^2 + x + \phi, \tag{5.2}$$

where $\phi^2 + \phi + 1 = 0$, $\phi \in F_4$. Now put

$$t = \frac{Q}{L^2P}. \tag{5.3}$$

https://doi.org/10.4153/CJM-1956-062-6 Published online by Cambridge University Press

It is easily verified that t belongs to the dihedral group $\mathfrak{D}_5$ of order 10 generated by

(5.4) $$s_1 = \begin{pmatrix} 1 & \phi^2 \\ \phi & \phi^2 \end{pmatrix}, \quad s_2 = \begin{pmatrix} 1 & \phi^2 \\ 1 & 1 \end{pmatrix}.$$

Thus t must satisfy an equation of degree 6. Indeed from (5.2)

$$\begin{aligned} P^2 + P &= x^4 + x + 1 = L + 1, \\ Q &= L^3 + 1 = (P^2 + P + 1)^3 + 1 = P^6 + P^5 + P^3 + P. \\ &= P^6 + P(P^2 + P + 1)^2, \end{aligned}$$

so that

(5.5) $$Q = P^6 + PL^2.$$

Using (5.3), (5.5) becomes

$$Q = \left(\frac{Q}{L^2 t}\right)^6 + \frac{Q}{t},$$

which reduces to

(5.6) $$t^6 + t^5 = \frac{Q^5}{L^{12}} = J.$$

This proves

THEOREM 6. *For* $q = 4$, (1.4) *admits the resolvent* (5.6) *of degree* 6 *as well as the resolvent* (5.1) *of degree* 5.

We remark that if x denotes any solution of the equation $J(x) = y$ then the solutions of $t^5 + t = y$ are the six irreducible quadratics

$$x^2 + x + \phi,\ x^2 + x + \phi^2,\ x^2 + \phi x + 1,\ x^2 + \phi x + \phi,\ x^2 + \phi^2 x + 1,\ x^2 + \phi^2 x + \phi^2.$$

6. $q = 9$. The group Γ is now of order 60. We require a subgroup of index 6. Such an icosahedral subgroup $\mathfrak{A}_5$ is generated by

(6.1) $$s_1 = \begin{pmatrix} 0 & 1 \\ -1 & 1 + \sigma \end{pmatrix}, \quad s_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

where $\sigma^2 = -1$. It is easily verified that

$$s_1^5 = s_2^2 = (s_1 s_2)^3 = 1,$$

so that $\mathfrak{A}_5$ is indeed the icosahedral group.

Using (6.1) we find that

(6.2) $$u = U^5/L^6,$$

where

(6.3) $$U = x^{12} - x^{10} + x^6 - x^2 - 1,$$

https://doi.org/10.4153/CJM-1956-062-6 Published online by Cambridge University Press

belongs to $\mathfrak{A}_5$. Since U is a product of 6 distinct irreducible quadratics, we have

(6.4) $$Q = TU,$$

where T is a polynomial of degree 60. Moreover

(6.5) $$t = T/L^6$$

also belongs to $\mathfrak{A}_5$. Consequently we have a relation of the form $U^5 - T = cL^6$, or what is the same thing

(6.6) $$U^6 - Q = cL^6U.$$

Comparing coefficients of x^{66} in both members of (6.6) we get $c = 1$, so that

(6.7) $$U^6 - L^6U = Q.$$

Using (6.4) this becomes

(6.8) $$T^6 + L^6T^5 = Q^5.$$

In terms of t as defined by (6.5), (6.8) yields

(6.9) $$t^6 + t^5 = \frac{Q^5}{L^{36}} = J.$$

We remark that it is not difficult to verify (6.7) by direct computation. Also (6.7) implies

(6.10) $$u(u - 1)^5 = J,$$

which is equivalent to (6.9). We may state

THEOREM 7. *For* $q = 9$, (1.4) *admits the resolvents* (6.9) *and* (6.10) *of degree* 6.

We shall next construct an equation of degree 6 with group $\mathfrak{A}_5$. This can be done by using one of the quadratic factors of U, for example $x^2 - 1 + \sigma$. We have

(6.11) $$\begin{aligned}&(x^2 - 1 - \sigma)(x^{10} - 1 + \sigma) - \sigma(x^2 - 1 + \sigma)^6 \\ &= (1 - \sigma)(x^{12} - x^{10} + x^6 - x^2 - 1) = (1 - \sigma)U,\end{aligned}$$

(6.12) $$\begin{aligned}&(x^{10} - 1 + \sigma)^2 - (x^2 - 1 + \sigma)(x^{18} - 1 + \sigma) \\ &= (1 - \sigma)(x^{18} + x^{10} + x^2) = (1 - \sigma)L^2.\end{aligned}$$

Put

(6.13) $$w = \frac{x^{10} - 1 + \sigma}{\sigma(x^2 - 1 + \sigma)^5}.$$

Then by (6.11)

(6.14) $$w - 1 = \frac{(1 - \sigma)U}{\sigma(x^2 - 1 + \sigma)^6}.$$

On the other hand it follows from (6.12) that

$$w^2 + 1 = -\frac{(1-\sigma)L^2}{(x^2 - 1 + \sigma)^{10}},$$

so that

$$w^6 + 1 = -\frac{(1+\sigma)L^6}{(x^2 - 1 + \sigma)^{30}}. \tag{6.15}$$

Comparison of (6.15) with (6.14) yields

$$w^6 + 1 = -\frac{L^6}{U^5}(w-1)^5 = -\frac{(w-1)^5}{u}. \tag{6.16}$$

If we make the substitution

$$w = \frac{1-u-z}{1-u+z} \tag{6.17}$$

(6.16) becomes

$$z^6 + z^5 = u(1-u)^5. \tag{6.18}$$

If we put $z = v - 1$, (6.18) takes on the more symmetrical form

$$u(1-u)^5 + v(1-v)^5 = 0; \tag{6.19}$$

Alternatively, since $u - t = 1$, we have

$$z^6 + z^5 + t^6 + t^5 = 0, \tag{6.20}$$

where t is defined by (6.5).

We omit the verification that z belongs to a dihedral subgroup $\mathfrak{D}_5$ of $\mathfrak{A}_5$ and state

THEOREM 8. *For $q = 9$, the equation (6.20) has group $\mathfrak{A}_5$ relative to $F_9(t)$.*

It is of interest to compare (6.20) with (6.9). Thus for J an indeterminate, (6.9) has group $\mathfrak{A}_6$, while for $-J = t^6 + t^5$ the group reduces to $\mathfrak{A}_5$. Since t belongs to $\mathfrak{A}_5$, this is in agreement with a familiar theorem on the effect on the Galois group of an adjunction to the coefficient field. In this connection we remark that a quintic with group $\mathfrak{A}_5$ relative to $F_9(t)$ is evidently

$$\frac{z^6 - t^6}{z - t} + \frac{z^5 - t^5}{z - t} = 0. \tag{6.21}$$

7. The ternary group. Define

$$[ijk] = \begin{vmatrix} x^{q^i} & y^{q^i} & z^{q^i} \\ x^{q^j} & y^{q^j} & z^{q^j} \\ x^{q^k} & y^{q^k} & z^{q^k} \end{vmatrix}; \tag{7.1}$$

in particular put

$$L = [012],\ Q_1 = \frac{[023]}{[012]},\ Q_2 = \frac{[013]}{[012]}. \tag{7.2}$$

Then L, Q_1, Q_2 are homogeneous polynomials in x, y, z and (see, for example (**8**, p. 17)) form a full system of invariants for the ternary linear group over F_q. Moreover x, y, z satisfy the equation

$$\xi^{q^3} = Q_2\xi^{q^2} - Q_1\xi^q + L^{q-1}\xi. \tag{7.3}$$

Indeed the general solution of (7.3) is furnished by

$$ax + by + cz \qquad (a, b, c \in F_q). \tag{7.4}$$

Now in particular when $q = 2$, the ternary group Γ is of order 168,

$$\deg L = 7,\ \deg Q_1 = 6,\ \deg Q_2 = 4. \tag{7.5}$$

Also (7.3) becomes

$$\xi^7 = Q_2\xi^3 + Q_1\xi + L, \tag{7.6}$$

an equation with group Γ.

Let

$$X = yz^2 + y^2z,\ Y = xz^2 + x^2z,\ Z = xy^2 + x^2y. \tag{7.7}$$

Then by (7.6)

$$\begin{aligned} Z^4 &= x^4(Q_2y^4 + Q_1y^2 + Ly) + y^4(Q_2x^4 + Q_1x^2 + Lx) \\ &= Q_1Z^2 + L(x^4y + xy^4), \\ Z^8 &= Q_1^2Z^4 + L^2x^2(Q_2y^4 + Q_1y^2 + Ly) + L^2y^2(Q_2x^4 + Q_1x^2 + Lx), \end{aligned}$$

so that

$$Z^8 + Q_1^2Z^4 + L^2Q_2Z^2 + L^3Z = 0. \tag{7.8}$$

Similarly X and Y also satisfy (7.8); indeed the general solution of (7.8) is

$$aX + bY + cZ \qquad (a, b, c \in F_2). \tag{7.9}$$

It follows that

$$L(XYZ) = L^3,\ Q_1(XYZ) = L^2Q_2,\ Q_2(XYZ) = Q_1^2. \tag{7.10}$$

We shall now construct a resolvent of degree 8 for the equation (7.6). To do this we make use of irreducible factorable polynomials over F_2, that is polynomials of the type

$$\prod_{i=0}^{2} (x + \alpha^{2^i}y + \beta^{2^j}z) \qquad (\alpha, \beta \in F_8). \tag{7.11}$$

The condition that (7.11) be irreducible (relative to F_2) is that α or β be a primitive number of F_8. We shall restrict our attention to those polynomials (7.11) that are of rank 3, that is those for which $1, \alpha, \beta$ are linearly independent relative to F_2; it is easily verified that the number of such polynomials is 8. If we define the field F_8 by means of

$$\phi^3 = \phi^2 + 1, \tag{7.12}$$

then the 8 polynomials in question are given by

$$\begin{aligned}(\alpha, \beta) = {} & (\phi, \phi^2),\ (\phi, \phi^3),\ (\phi, \phi^4),\ (\phi, \phi^6), \\ & (\phi^3, \phi^4),\ (\phi^3, \phi^5),\ (\phi^3, \phi),\ (\phi^5, \phi^3). \end{aligned} \tag{7.13}$$

The polynomials (7.13) are permuted by Γ; each is left invariant by a certain subgroup of order 21. By direct computation we find that the polynomials are

$$\begin{aligned}
P_1 &= x^3 + y^3 + z^3 + xyz + x^2y + x^2z + y^2z \\
P_2 &= x^3 + y^3 + z^3 + xyz + x^2y + xz^2 + y^2z \\
P_3 &= x^3 + y^3 + z^3 + xyz + x^2y + x^2z + yz^2 \\
P_4 &= x^3 + y^3 + z^3 + xyz + x^2y + xz^2 + yz^2 \\
P_5 &= x^3 + y^3 + z^3 + xyz + xy^2 + x^2z + y^2z \\
P_6 &= x^3 + y^3 + z^3 + xyz + xy^2 + xz^2 + y^2z \\
P_7 &= x^3 + y^3 + z^3 + xyz + xy^2 + x^2z + yz^2 \\
P_8 &= x^3 + y^3 + z^3 + xyz + xy^2 + xz^2 + yz^2.
\end{aligned}$$

Using (7.7) we find that the polynomials P_j can be exhibited as

$$P_1 + aX + bY + cZ \qquad (a, b, c \in F_2).$$

Consequently if the equation of degree 8 satisfied by P_j is $f(\xi) = 0$, then writing $\xi = \eta + P_1$, we have $f(\eta + P_1) = 0$ when η takes on the values (7.9). It follows that $f(\eta + P_1)$ is identical with the left member of (7.8). Hence we get

$$\xi^8 + Q_1^2Z^4 + L^2Q_2Z^2 + L^3Z = A \tag{7.14}$$

as the equation satisfied by P_j, where

$$A = \prod_{j=1}^{8} P_j. \tag{7.15}$$

It remains to compute the coefficient A. Since $\deg A = 24$ and A is an invariant we have

$$A = aQ_1^4 + bQ_1^2\,Q_2^3 + cQ_2^6 + dL^2Q_1\,Q_2,$$

and it is only necessary to determine the constants a, b, c, d. We readily compute the following special values:

$$Q_1(11z) = z^4 + z^2,\ Q_2(11z) = z^4 + z^2 + 1,\ L(11z) = 0.$$

In particular

$$Q_1(111) = 0,\ Q_2(111) = 1,\ L(111) = 0.$$

Since for $xyz = 111$ each $P_j = 1$ it follows that $c = 1$. We also find from the explicit polynomial expressions for P_j, that for $xy = 11$ each reduces to $z^3 + z + 1$ or $z^3 + z^2 + 1$. This yields the identity

$$(z^6 + z^5 + z^4 + z^3 + z^2 + z + 1)^4 = a(z^4 + z^2)^4 \\ + b(z^4 + z^2)^2(z^4 + z^2 + 1)^3 + (z^4 + z^2 + 1)^6.$$

Put $z = \epsilon$, $\epsilon^2 + \epsilon + 1 = 0$, and we get $a = 1$. For $z = \phi$ we get

$$0 = (\phi + 1)^4 + b(\phi + 1)^2\phi^3 + \phi^6,$$

so that $b = 0$. To get the coefficient d we take $xyz = \phi\phi^2\phi^4$. We find that $L(\phi\phi^2\phi^4) = 1$, $Q_1(\phi\phi^2\phi^4) = Q_2(\phi\phi^2\phi^4) = 0$. Also it is easily verified that each $P_j = 1$. It follows that $d = 1$. Hence (7.14) becomes

$$\xi^8 + Q_1^2\,\xi^4 + L^2 Q_2\,\xi^2 + L_3\,\xi = Q_1^4 + Q_2^6 + L^2 Q_1\,Q_2. \tag{7.16}$$

We may now state

THEOREM 9. *For $q = 2$, the equation* (7.16) *of degree* 8 *has the Galois group* $LF(3, 2)$ *of order* 168. *The solutions of* (7.16) *are the irreducible factorable cubics P_j; if P_1 is a particular solution then the general solution is*

$$P_1 + aX + bY + cZ,$$

where X, Y, Z are defined by (7.7) *and $a, b, c \in F_2$.*

REFERENCES

1. L. E. Dickson, *An invariantive investigation of irreducible binary modular forms*, Trans. Amer. Math. Soc. *12* (1911), 1–8.
2. L. E. Dickson, *Linear Groups* (Leipzig, 1901).
3. ———, *Modern Algebraic Theories* (New York, 1923).
4. R. Fricke, *Die elliptische Funktionen und ihre Anwendungen*, II (Leipzig and Berlin, 1922).
5. ———, *Lehrbuch der Algebra*, II (Braunschweig, 1926).
6. J. R. Garrett, *Normal equations and resolvents in fields of characteristic p*, Duke Math. J. *18* (1951), 373–384.
7. F. Klein, *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade* (Leipzig, 1884).
8. D. E. Rutherford, *Modular Invariants*, Cambridge Tracts in Mathematics and Mathematical Physics, No. 27 (Cambridge, 1932).

Duke University,
Durham, North Carolina

https://doi.org/10.4153/CJM-1956-062-6 Published online by Cambridge University Press