A COUNTEREXAMPLE IN DIFFERENTIAL ALGEBRA[1]

GEORGE M. BERGMAN

Kolchin [1, p. 791] calls a differential field extension "weakly normal" if the fixed field of its Galois group is the base field, and "normal" if it is weakly normal over every subextension. He gives an example to show that if the extension is allowed to have a larger field of constants than the base field, these conditions are not equivalent, but he does not know whether they are equivalent for extensions preserving constants. The example in §1 of the present paper shows that they are not. In §2, we describe precisely the Galois group of this example.

I would like to express my indebtedness to Professor A. Seidenberg, whose fascinating course in differential algebra here at Harvard has been my introduction to the field.

1. **The example.** Let A be a nontrivial additive subgroup of the complexes, $\mathbf{C}$, with a finite additive basis, $c_1, \cdots, c_n$; and let G be the multiplicative group of those complex numbers u such that A is closed under multiplication by both u and u^{-1}. Suppose that G does not consist entirely of roots of unity.[2]

Let F be the field of meromorphic functions generated over $\mathbf{C}$ by e^z and $e^{c_1 e^z}, \cdots, e^{c_n e^z}$. These generators are easily shown to be algebraically independent.

The field is closed under differentiation. The differential equations satisfied by our generators are:

$$\frac{d}{dz} e^z = e^z, \qquad \frac{d}{dz} e^{c_i e^z} = c_i e^z e^{c_i e^z}. \tag{1}$$

Received by the editors April 13, 1964.

[1] This work was done while the author held a National Science Foundation first year graduate fellowship.

[2] For example, let R be any finite integral algebraic extension ring of the integers, and A any finitely generated R-submodule of $\mathbf{C}$ (such as R itself). G will contain all the units of R. From the Dirichlet Unit Theorem, we know of a very large class of such rings R having units other than roots of unity.

Conversely, given any A, if we take R to be the ring of all complex numbers u such that $uA \subseteq A$, then G will consist exactly of the units of R. This R must be of finite rank as an additive group (for A is, and given any $a \neq 0$ in A, $R \subseteq (1/a)A$), hence must be a finite integral extension of the integers.

As a concrete example, $G = \{\pm(1 + \sqrt{2})^n\}_{n=\cdots,-1,0,1,2,\cdots}$, if A is generated by 1 and $\sqrt{2}$.

Now for any nonzero complex number u, consider the algebraic isomorphism σ_u of F defined by

$$e^z \longrightarrow ue^z,$$
$$e^{c_i e^z} \longrightarrow e^{uc_i e^z}.$$

That it is a differential isomorphism can be checked either by verifying that the images of the generators satisfy (1), or by noting that it is the restriction to F of the "translation"-automorphism $f(z) \to f(z+\lambda)$ of the field of all meromorphic functions, where λ is any logarithm of u.

If u is not a root of unity, the only elements of F invariant under this map are the constants. For suppose $f(z)$ is invariant. By the nature of the field F, $f(z)$ is a meromorphic function of e^z: $f(z) = m(e^z)$. Then we must have the identity $m(u\zeta) = m(\zeta)$. Expanding m about zero in powers of ζ, we find that it must consist of a constant term only.

If u is a member of G, σ_u will be an automorphism of F over $\mathbf{C}$. Taking u to be a member of G that is not a root of unity, we get an automorphism of F over $\mathbf{C}$ whose fixed field is $\mathbf{C}$. So F is weakly normal over $\mathbf{C}$.

To show that it is not normal, we shall show that for some prime p, any automorphism σ of F over $\mathbf{C}$ leaving e^{pz} fixed leaves e^z fixed as well, whence F is not weakly normal over $\mathbf{C}(e^{pz})$.

Let σ be an arbitrary automorphism of F over $\mathbf{C}$. Since $\sigma(e^z)$ must satisfy the same differential equation as e^z, it must be of the form ue^z for some $u \in \mathbf{C}^*$ (the nonzero complexes). From this, we calculate in turn that for each $a \in A$, $\sigma(e^{ae^z})$ must be of the form ke^{aue^z} ($k \in \mathbf{C}^*$, not necessarily the same for all a). The only elements of such a form in F are the $ke^{a'e^z}$ for $a' \in A$, hence $au = a'$, hence multiplication by u sends A into itself. Looking at σ^{-1}, we similarly conclude that multiplication by u^{-1} sends A into itself. Hence $u \in G$. (This is not to say that σ need equal σ_u—cf. §2.)

Now G can contain at most finitely many roots of unity. (For it is the group of units of a finite algebraic extension of the integers—see footnote 2.) Hence for some prime p it will *not* contain the primitive pth roots of unity. Now suppose the σ discussed above leaves e^{pz} fixed. Then $e^{pz} = \sigma(e^{pz}) = \sigma(e^z)^p = u^p e^{pz}$, hence $u = 1$, hence σ leaves e^z fixed. Q.E.D.

2. **Further observations.** From the argument begun above, we can see that any automorphism of F must be of the form:

$$e^z \longrightarrow ue^z \qquad (u \in G),$$
$$e^{c_i e^z} \longrightarrow k_i e^{uc_i e^z} \qquad (k_i \in \mathbf{C}^*;\ i = 1, \cdots, n).$$

We find that for *all* $u \in G$ and *all* values of $k_1, \cdots, k_n$ this gives an automorphism of F (for the images of e^z, $e^{c_i z}$ are algebraically independent and satisfy the differential equations (1)). Let us designate this automorphism $(k_1, \cdots, k_n, u)$.

Let X be any commutative group. The ring of $n \times n$ matrices with integral coefficients has an obvious action as a ring of endomorphisms on X^n—if X is written multiplicatively, for instance, for any n-tuplet $x = (x_1, \cdots, x_n)$ of members of X and any matrix $\bar{m} = (m_{ij})$, we can write $x^{\bar{m}} = (\prod^j x_j^{m_{1j}}, \cdots, \prod^j x_j^{m_{nj}})$. In particular, the *group of invertible matrices* acts as a group of automorphisms of X^n.

Given $u \in G$, let $\bar{u}$ be the matrix showing the action on A of multiplication by u, in terms of the basis $c_1, \cdots, c_n$. Then we can check easily that our automorphisms compose by the rule $(k, u) \cdot (k', u') = (k \cdot k'^{\bar{u}}, uu')$. Thus we have a semidirect product of $(C^*)^n$ and G.

Reference

1. E. R. Kolchin, *Galois theory of differential fields*, Amer. J. Math. 75 (1953), 753–824.

Harvard University