The author holds a NSF Coop fellowship. The preparation of this manuscript was partly supported by the NSF (G 24335).

References

1. E. A. Coddington and Norman Levinson, Theory of ordinary differential equations, McGraw-Hill, New York, 1955.

2. Witold Hurewicz, Lectures on ordinary differential equations, Wiley and MIT Press, New York, 1958.

ANOTHER PROOF OF WEDDERBURN'S THEOREM

T. J. Kaczynski, Evergreen Park, Illinois

In 1905 Wedderburn proved that every finite skew field is commutative. At least seven proofs of this theorem (not counting the present one) are known. See [1], [2], [5] (Part Two, p. 206 and Exercise 4 on p. 219), [6] (two proofs), and [7]. Unlike these proofs, the proof to be given here is group-theoretic, in the sense that the only non-group-theoretic concepts employed are of an elementary nature.

LEMMA. *Let q be a prime. Then the congruence $t^2+r^2\equiv -1$ (mod q) has a solution t, r with $t\not\equiv 0$ (mod q).*

Proof. If -1 is a quadratic residue, take $r=0$ and choose t appropriately. Assume -1 is a nonresidue. Then any nonresidue can be written in the form $-s^2$ (mod q) with $s\not\equiv 0$. If t^2+r^2 is ever a nonresidue for some t, r, set $t^2+r^2\equiv -s^2$, and we have $(ts^{-1})^2+(rs^{-1})^2\equiv -1$. (Throughout this note, x^{-1} denotes that integer for which $xx^{-1}\equiv 1$ (mod q).) On the other hand, if t^2+r^2 is always a residue, then the sum of any two residues is a residue, so $-1\equiv q-1=1+1+\cdots+1$ is a residue, contradicting our assumption.

Proof of the theorem. Let F be our finite skew field, F^* its multiplicative group. Let S be any Sylow subgroup of F^*, of order, say, p^α. Choose an element g of order p in the center of S. If some $h\in S$ generates a subgroup of order p different from that generated by g, then g and h generate a commutative field containing more than p roots of the equation $x^p=1$, an impossibility. Thus S contains only one subgroup of order p and hence is either a cyclic or a generalized quaternion group ([3] p. 189).

If S is a generalized quaternion group, then S contains a quaternion subgroup generated by two elements a and b, both of order 4, where $ba=a^{-1}b$. Now a^2 generates a commutative field in which the only roots of the equation $x^2=1$ or $(x+1)(x-1)=0$ are ± 1, so since $(a^2)^2=1$, we have

$$a^2 = -1. \tag{1}$$

Hence $a^{-1}=a^3=-a$, so

$$ba = -ab. \tag{2}$$

Similarly,

$$b^2 = -1. \tag{3}$$

Taking q = characteristic of F $(q \cdot 1 = 0)$, choose t and r as specified in the lemma. Using relations (1), (2), (3), we have

$$(t + ra + b)(r^2 + 1 + rta + tb) = r(t^2 + r^2 + 1)a + (t^2 + r^2 + 1)b = 0.$$

One of the factors on the left must be 0, so for some numbers $u, v, w, u \not\equiv 0 \pmod{q}$, we have $w + va + ub = 0$, or $b = -u^{-1}va - u^{-1}w$. So b commutes with a, a contradiction. We conclude that S is not a generalized quaternion group, so S is cyclic.

Thus every Sylow subgroup of F^* is cyclic, and F^* is solvable ([4], pp. 181–182). Let Z be the center of F^* and assume $Z \neq F^*$. Then F^*/Z is solvable, and its Sylow subgroups are cyclic. Let A/Z (with $Z \subset A$) be a minimal normal subgroup of F^*/Z. A/Z is an elementary abelian group of order p^k (p prime), so since the Sylow subgroups of F^*/Z are cyclic, A/Z is cyclic. Any group which is cyclic modulo its center is abelian, so A is abelian. Let x be any element of F^*, y any element of A. Since A is normal, $xyx^{-1} \in A$, and $(1+x)y = z(1+x)$ for some $z \in A$. An easy manipulation shows that $y - z = zx - xy = (z - xyx^{-1})x$.

If $y - z = z - xyx^{-1} = 0$, then $y = z = xyx^{-1}$, so x and y commute. Otherwise, $x = (z - xyx^{-1})^{-1}(y - z)$. But A is abelian, and z, y, $xyx^{-1} \in A$, so x commutes with y. Thus we have proven that A is contained in the center of F^*, a contradiction.

References

1. E. Artin, Über einen Satz von Herrn J. H. M. Wedderburn, Abh. Math. Sem. Hamburg, 5 (1927) 245.
2. L. E. Dickson, On finite algebras, Göttingen Nachr., 1905, p. 379.
3. M. Hall, The theory of groups, Macmillan, New York, 1961.
4. Miller, Blichfeldt and Dickson, Theory and applications of finite groups, Wiley, New York, 1916.
5. B. L. van der Waerden, Moderne Algebra, Ungar, New York, 1943.
6. J. H. M. Wedderburn, A theorem on finite algebras, Trans. Amer. Math. Soc., 6 (1905) 349.
7. E. Witt, Über die Kommutativität endlicher Schiefkörper, Abh. Math. Sem. Hamburg, 8 (1931) 413.

A NOTE ON PRODUCT SYSTEMS OF SETS OF NATURAL NUMBERS

T. G. McLaughlin, University of California at Los Angeles

In this note, we apply a slight twist to a trick exploited about twelve years ago by J. C. E. Dekker ([2]), our purpose being to expose a couple of elementary facts about nonempty, countable "product systems" of infinite sets of natural numbers which are, at the same time, "finite symmetric difference systems." We proceed in terms of the following definitions.

Definition. *By a product system of subsets of N (N the natural numbers), we mean a collection of subsets of N which contains, along with any two of its members, their intersection.*