ELSEVIER
Journal of Pure and Applied Algebra 119 (1997) 13–26
JOURNAL OF PURE AND APPLIED ALGEBRA

Compact rings having a finite simple group of units

Jo-Ann Cohen *, Kwangil Koh
Department of Mathematics, North Carolina State University, Raleigh, NC 27695-8205, USA

Communicated by J.D. Stasheff; received 14 November 1991; revised 28 September 1993

Abstract

For a compact Hausdorff ring, one observes that the group of units is a totally disconnected compact topological group and is a finite simple group if and only if it possesses no nontrivial closed normal subgroups. Three classification theorems for compact rings are now given. First, those compact rings with identity having a finite simple group of units are identified. Second, a classification of all compact rings A with identity for which 2 is a unit in A, G modulo the center of G is a finite simple group and the length of W is less than or equal to 4 (or equivalently, W is a torsion group) is given where G is the group of units in A and W is the subgroup of G generated by $\{g \in G\colon g^2 = 1\}$. Finally, those compact rings with identity having 2 as a unit and for which W is a nilpotent group are identified. © 1997 Elsevier Science B.V.

1991 Math. Subj. Class.: Primary 16A80, 13J99; Secondary 16A48, 16A25

1. Introduction

If A is a compact Hausdorff topological ring with identity and if G is the group of units in A, then G is a compact topological group by [1, Exercise 12h, p. 119; 7, Theorem]. Since A is a totally disconnected space, G is 0-dimensional [15, Theorem 8; 10, Theorem 3.5, p. 12]. Consequently, if π is an irreducible representation of G in a Hilbert space, then $\pi(G)$ is a finite group [11, Corollary 28.19, p. 69]. In particular, G contains no nontrivial closed normal subgroups if and only if G is a finite simple group.

In Section 2, we show that G is a finite simple group if and only if A is isomorphic and homeomorphic to the ring $\prod_{\alpha\in\Lambda}\mathbb{Z}/(2)$, endowed with the product topology, where Λ is a nonempty set and $\mathbb{Z}/(2)$ is the ring of integers modulo 2 or A is isomorphic and homeomorphic to $\left(\prod_{\alpha\in\Lambda}\mathbb{Z}/(2)\right)\times A_0$, endowed with the product topology, where Λ is an arbitrary set and A_0 is one of the following rings:

* Corresponding author. E-mail: Cohen@math. ncsu.edu.

PII S0022-4049(96)00128-4

(1) a finite field of cardinality 3 or cardinality 2^n where n is a positive integer such that $2^n - 1$ is prime,

(2) the set of $n \times n$ matrices over $\mathbb{Z}/(2)$ for some $n \geq 3$,

(3) $\mathbb{Z}/(4)$, the ring of integers modulo 4,

(4) $\mathbb{Z}/_{(2)}[x]_{/(x^2)}$ where $\mathbb{Z}/_{(2)}[x]$ is the ring of polynomials in x with coefficients in $\mathbb{Z}/(2)$ and (x^2) is the ideal of $\mathbb{Z}/_{(2)}[x]$ generated by x^2, or

(5) the set of all 2×2 upper triangular matrices over $\mathbb{Z}/(2)$.

If G is a group, let $Z(G)$ denote the center of G and let W be the subgroup of G generated by the set of involutions $\Delta = \{g \in G\colon g^2 = 1\}$. If $g \in W$, the *length* $l(g)$ of g is the smallest positive integer m such that there exist $w_1, w_2, \ldots, w_m$ in Δ with $g = w_1 w_2 \cdots w_m$. For each subgroup H of W, define the *length* $l(H)$ of H by $l(H) = \sup_{g \in H} l(g)$. There are compact rings with identity for which $l(W)$ is infinite, and $l(W)$ is finite if and only if W is compact. (See [5].) In [9], Gustafson et al. proved that if G is the group of nonsingular matrices over a field, then $l(W) \leq 4$. Consequently, if A is a semisimple compact ring with identity, then $l(W) \leq 4$ as A is isomorphic to the product $\prod_{\alpha \in \Lambda} M_\alpha$, where each M_α is a matrix ring over a finite field [15, Theorem 16; 12, Theorem, p. 431; 13, Theorem, p. 171]. In Section 3 we show that for a compact ring A, $G/Z(G)$ is a finite simple group if and only if it possesses no nontrivial closed normal subgroups and then give a characterization of those compact rings A with identity for which 2 is a unit in A, $G/Z(G)$ is a finite simple group and $l(W) \leq 4$. In particular, we show that A has the above properties if and only if $G/Z(G)$ is a finite simple group and W is a torsion group. Finally, in Section 4, we prove that if 2 is a unit in a compact ring A with identity, then the following are equivalent:

1. W is a nilpotent group.
2. W is abelian.
3. A is isomorphic and homeomorphic to the product $\prod_{\alpha \in \Lambda} N_\alpha$, where for each α in Λ, N_α is a compact local ring with identity such that the characteristic of N_α/J_α is an odd prime p_α where J_α is the Jacobson radical of N_α.

As a corollary, we obtain that if A is a compact ring with identity for which 2 is a unit, then G is abelian if and only if W and G/W are abelian.

Henceforth if A is a ring with identity, G, J, Δ and W will denote the group of units in A, the Jacobson radical of A, the subset $\{g \in G\colon g^2 = 1\}$ of involutions of G and the subgroup of G generated by Δ, respectively. In order to avoid confusion, we will sometimes denote G, J, Δ and W by $G(A)$, $J(A)$, $\Delta(A)$ and $W(A)$, respectively.

2. Compact rings having a simple group of units

Henceforth, all compact topologies are assumed to be Hausdorff.

Lemma 2.1. *Let G be a totally disconnected compact group. Then G possesses no nontrivial closed normal subgroups if and only if G is a finite simple group.*

Proof. Suppose that G contains no nontrivial closed normal subgroups. Since G is a compact group, G has a unitary irreducible representation in the group $\mathrm{GL}(V)$ of automorphisms of a finite dimensional complex vector space V by [16, Theorem 2, p. 27]. By hypothesis, this representation is faithful and hence G is isomorphic to a closed subgroup of $\mathrm{GL}(V)$. Therefore G is a Lie group [2, Corollary, p. 135]. Consequently, as each component of a Lie group is open [2, Proposition 1, p. 40], G is endowed with the discrete topology. Thus G is a finite group.

The converse is clear. □

Theorem 2.2. *Let G be the group of units of a compact ring A with identity.* (1) *G is a totally disconnected compact topological group.* (2) *G is a finite simple group if and only if G possesses no nontrivial closed normal subgroups.*

Proof. By [1, Exercise 12h, p. 119; 7, Theorem], G is a compact topological group. As A is totally disconnected [15, Theorem 8], G is totally disconnected as well. (2) follows from Lemma 2.1. □

Recall that an idempotent e in a ring A is *primitive* if e is not the sum of two nontrivial orthogonal idempotents in A.

Lemma 2.3. *Let A be a compact ring with identity and suppose $e+J$ is a primitive idempotent in A/J. If f is any idempotent in A such that $f+J=e+J$, then f is primitive.*

Proof. If f were not primitive, then there would exist nontrivial orthogonal idempotents f_1 and f_2 in A such that $f=f_1+f_2$. Consequently as $f+J$ is a primitive idempotent in A/J, either $f_1+J=J$ or $f_2+J=J$, that is, either $f_1 \in J$ or $f_2 \in J$. But J contains no nontrivial idempotent since $a^n \to 0$ for all a in J [15, Theorem 15]. Hence f is a primitive idempotent in A. □

Lemma 2.4. *Let A be a compact ring with identity such that $A/J = \prod_{\alpha\in\Lambda} \mathbb{Z}/(2)$ for some nonempty set Λ. For each β in Λ, let $E_\beta = \langle x_\alpha\rangle_{\alpha\in\Lambda}$ where $x_\beta = \bar{1}$, the multiplicative identity of $\mathbb{Z}/(2)$ and for $\alpha \neq \beta$, $x_\alpha = \bar{0}$, the additive identity of $\mathbb{Z}/(2)$. Then there exists a family $\{e_\alpha\colon \alpha\in\Lambda\}$ of primitive orthogonal idempotents in A such that $e_\alpha + J = E_\alpha$ for all α in Λ, $\sum_{\alpha\in\Lambda} e_\alpha = 1$ and $e_\alpha A e_\alpha / e_\alpha J e_\alpha \cong \mathbb{Z}/(2)$ for all α in Λ.*

Proof. Well-order Λ. If Λ has no largest element, let $\Lambda' = \Lambda$. Otherwise, adjoin ∞ to Λ and extend the ordering from Λ to $\Lambda \cup \{\infty\}$ by declaring that ∞ is the largest element in $\Lambda \cup \{\infty\}$. In this case, let $\Lambda' = \Lambda \cup \{\infty\}$. Let λ_0 be the smallest element of Λ. For each $\lambda \in \Lambda' \backslash \{\lambda_0\}$, define F_λ by $F_\lambda = \sum_{\rho<\lambda} E_\lambda$. So $F_\lambda = \langle y_\alpha\rangle_{\alpha\in\Lambda}$ where $y_\alpha = \bar{1}$ for all $\alpha < \lambda$ and $y_\alpha = \bar{0}$ for all $\alpha \geq \lambda$. Clearly, if $\lambda_1, \lambda_2 \in \Lambda'\backslash\{\lambda_0\}$ where $\lambda_1 \leq \lambda_2$, then $F_{\lambda_1}F_{\lambda_2} = F_{\lambda_2}F_{\lambda_1} = F_{\lambda_1}$. Moreover, if λ is a limit ordinal of $\Lambda'\backslash\{\lambda_0\}$, then $F_\lambda = \lim_{\rho<\lambda} F_\rho$. Hence by [15, Lemma 12], there exists a family $\{h_\lambda\colon \lambda \in \Lambda'\backslash\{\lambda_0\}\}$

of idempotents in A such that $h_{\lambda_1}h_{\lambda_2} = h_{\lambda_2}h_{\lambda_1} = h_{\lambda_1}$ for all $\lambda_0 < \lambda_1 \leq \lambda_2$ and $h_\lambda + J = F_\lambda$ for all $\lambda \in \Lambda' \backslash \{\lambda_0\}$. Let h_{λ_0} be the additive identity of A. For each $\lambda \in \Lambda$, let $\gamma(\lambda)$ denote the smallest element of $\{\rho \in \Lambda' \colon \lambda < \rho\}$ and let $e_\lambda = h_{\gamma(\lambda)} - h_\lambda$. Then $\{e_\lambda \colon \lambda \in \Lambda\}$ is a family of orthogonal idempotents in A such that for each α in Λ, $e_\alpha + J = E_\alpha$ and $e_\alpha A e_\alpha / e_\alpha J e_\alpha \cong \mathbb{Z}/(2)$. As each E_α is a primitive idempotent in A/J, Lemma 2.3 yields that each e_α is a primitive idempotent in A. So it suffices to prove that $\sum_{\alpha \in \Lambda} e_\alpha = 1$.

First notice that $\sum_{\alpha \in \Lambda} e_\alpha$ exists. Indeed, as A is compact, there exists a fundamental system of ideal neighborhoods of zero in A [10, Theorem 3.5, p. 12, Theorem 7.7, p. 62; 15, Theorem 8 and Lemma 9]. Since A is complete, it suffices to show that if U is an open ideal of A and if $M = \{\alpha \in \Lambda \colon e_\alpha \notin U\}$, then M is finite. Let U be an open ideal of A. Then A/U is a compact discrete ring and hence a finite ring. In particular, A/U has finitely many idempotents. Moreover, if α and β are distinct elements of M, then $e_\alpha + U \neq e_\beta + U$. Indeed, if $e_\alpha + U = e_\beta + U$, then $e_\alpha + U = e_\alpha^2 + U = e_\alpha e_\beta + U = 0 + U = U$, a contradiction. Hence M is finite and so $\sum_{\alpha \in \Lambda} e_\alpha$ exists. (The above proof is an adaptation of one given by Seth Warner in an unpublished manuscript.) Since $\{e_\alpha \colon \alpha \in \Lambda\}$ is a family of orthogonal idempotents in A, $\sum_{\alpha \in \Lambda} e_\alpha$ is an idempotent as well. Thus $1 - \sum_{\alpha \in \Lambda} e_\alpha$ is an idempotent in A. By construction, $1 - \sum_{\alpha \in \Lambda} e_\alpha \in J$ and therefore, as in the proof of Lemma 2.3, $1 - \sum_{\alpha \in \Lambda} e_\alpha = 0$. □

Lemma 2.5. *Let A be a ring with identity and let Γ denote a nonempty set of idempotents in A such that for all f in Γ, $f + J$ is a central idempotent in A/J. If Γ is contained in the centralizer of J in A, then Γ is contained in the center of A.*

Proof. Let $e \in \Gamma$ and let $x \in A$. Since $(e + J)(x + J) = (x + J)(e + J)$, $ex - xe \in J$. Denote $ex - xe$ by a. Then $ae = ea$ and so $ea = e^2 a = e(ea) = e(ae) = e(ex - xe)e = 0$. Thus $0 = ea = e(ex - xe) = ex - exe$ and hence $ex = exe$. Since $ae = ea = 0$, $0 = ae = (ex - xe)e$ and consequently, $exe = xe$ as well. Therefore e is in the center of A. □

Lemma 2.6. *Let Λ be a nonempty set and for each $\alpha \in \Lambda$, let F_α be a finite field endowed with the discrete topology. Let $A = \prod_{\alpha \in \Lambda} F_\alpha$, endowed with the product topology. If I is a nonzero closed left (right) ideal of $\prod_{\alpha \in \Lambda} F_\alpha$, then there exists a nonempty subset Λ_1 of Λ such that $I = \prod_{\alpha \in \Lambda} B_\alpha$ where $B_\alpha = F_\alpha$ for all α in Λ_1 and $B_\alpha = \{0_\alpha\}$ for all $\alpha \in \Lambda \backslash \Lambda_1$ (where 0_α is the additive identity of F_α).*

Proof. For each α in Λ, let 1_α denote the multiplicative identity of F_α. Define Λ_1 by, $\Lambda_1 = \{\alpha \in \Lambda \colon \text{there exists } \langle x_\beta \rangle_{\beta \in \Lambda} \text{ in } I \text{ with } x_\alpha \neq 0_\alpha\}$. For each α in Λ_1, let $B_\alpha = F_\alpha$ and for each α in $\Lambda \backslash \Lambda_1$, let $B_\alpha = \{0_\alpha\}$. Clearly $I \subseteq \prod_{\alpha \in \Lambda} B_\alpha$.

We first prove that given any α in Λ_1, the element s_α of A defined by, $s_\alpha = \langle v_\beta \rangle_{\beta \in \Lambda}$ where $v_\alpha = 1_\alpha$ and $v_\beta = 0_\beta$ for $\beta \neq \alpha$, is an element of I. Indeed, let $\langle x_\beta \rangle_{\beta \in \Lambda} \in I$ be such that $x_\alpha \neq 0_\alpha$ and let $y_\alpha \in F_\alpha$ be such that $x_\alpha y_\alpha = y_\alpha x_\alpha = 1_\alpha$. Define $\langle z_\beta \rangle_{\beta \in \Lambda} \in A$ by, $z_\alpha = y_\alpha$ and $z_\beta = 0_\beta$ for $\beta \neq \alpha$. Then $s_\alpha = \langle z_\beta \rangle_{\beta \in \Lambda} \langle x_\beta \rangle_{\beta \in \Lambda} \in I$.

Now let $\langle d_\alpha\rangle_{\alpha\in\Lambda} \in \prod_{\alpha\in\Lambda} B_\alpha$. As I is closed, it suffices to prove that $\langle d_\alpha\rangle_{\alpha\in\Lambda} \in \bar{I}$. So let U be a neighborhood of $\langle d_\alpha\rangle_{\alpha\in\Lambda}$ in A. Without loss of generality, we may assume that there exists a finite subset Λ_2 of Λ such that $U = \prod_{\alpha\in\Lambda} U_\alpha$ where $U_\alpha = \{d_\alpha\}$ for all α in Λ_2 and $U_2 = F_\alpha$ for all $\alpha \in \Lambda\backslash\Lambda_2$. Let $\Lambda_2' \subseteq \Lambda_2$ be such that for all α in Λ_2', $d_\alpha \neq 0_\alpha$ and for all α in $\Lambda_2\backslash\Lambda_2'$, $d_\alpha = 0_\alpha$. For each α in Λ_2', let $t_\alpha = \langle c_\beta\rangle_{\beta\in\Lambda}$ where $c_\alpha = d_\alpha$ and $c_\beta = 0_\beta$ for all $\beta \neq \alpha$. Recall that for each α in Λ_2', $s_\alpha \in I$. Thus $\sum_{\alpha\in\Lambda_2'} t_\alpha s_\alpha \in I \cap U$ and so $\langle d_\alpha\rangle_{\alpha\in\Lambda} \in \bar{I}$. □

Recall that a ring A with identity is called a *local* ring if the set of nonunits in A is an ideal of A.

Lemma 2.7. *Let A be a compact ring with identity having characteristic two such that $J = \{0, a\}$ for some nonzero a in A and $A/J \cong \prod_{\alpha\in\Lambda} \mathbb{Z}/(2)$ for some nonempty set Λ. Then for some indexing set Γ, A is isomorphic and homeomorphic to $\left(\prod_{\beta\in\Gamma} \mathbb{Z}/(2)\right) \times A_0$ where A_0 is one of the following rings:*

(1) *$\mathbb{Z}/_{(2)}[x]/_{(x^2)}$ where $\mathbb{Z}/_{(2)}[x]$ is the ring of polynomials in x with coefficients in $\mathbb{Z}/(2)$ and (x^2) is the ideal of $\mathbb{Z}/_{(2)}[x]$ generated by x^2; or*

(2) *the set of all 2×2 upper triangular matrices over $\mathbb{Z}/(2)$.*

Proof. First notice that as g is a unit in A if and only if $g + J$ is a unit in A/J, $G = 1 + J$. By Lemma 2.4, there exists a primitive idempotent e in A such that $ea \neq 0$ and $eAe/eJe \cong \mathbb{Z}/(2)$. In particular, as $ea \in J$, $ea = a$. Recall that the Pierce decomposition of A relative to e yields that $A = eAe \oplus (1-e)A(1-e) \oplus eA(1-e) \oplus (1-e)Ae$. (See for example [14, p. 48].)

Suppose that $eae = 0$. We first show that $A = eAe \oplus (1-e)A(1-e) \oplus eA(1-e)$ where $J = eA(1-e)$. Indeed, as $eae = 0$, $ae = 0$ and thus $(1-e)a(1-e) = (1-e)a = 0$. So $a = eae + (1-e)a(1-e) + ea(1-e) + (1-e)ae = ea(1-e)$ and consequently $J \subseteq eA(1-e)$. Notice that if $x \in eA(1-e)$, then $x^2 = 0$ and hence $(1+x)(1-x) = (1-x)(1+x) = 1$. Thus if $x \in eA(1-e)$, then $1 + x \in G = 1 + J$. Therefore, $eA(1-e) \subseteq J$. Similarly as $((1-e)Ae)^2 = \{0\}$, $(1-e)Ae \subseteq J = eA(1-e)$ and hence $(1-e)Ae = \{0\}$. So $A = eAe \oplus (1-e)A(1-e) \oplus eA(1-e)$ where $eA(1-e) = J$.

Observe next that as $eae = 0$, $eJe = \{0\}$ and hence eAe is a finite field having two elements. Moreover as $(1-e)a(1-e) = 0$ and as $(1-e)J(1-e)$ is the Jacobson radical of $(1-e)A(1-e)$ [14, Proposition 1, p. 48], $(1-e)A(1-e)$ is a compact semisimple ring with identity $1-e \neq 0$. Furthermore, $1-e$ is the only unit in $(1-e)A(1-e)$. Indeed, if x and y are elements in $(1-e)A(1-e)$ such that $x \neq 1-e$ but $xy = yx = (1-e)$, then as $xe = ex = ye = ey = 0$, $(x+e)(y+e) = (y+e)(x+e) = 1$. Therefore $x + e \in G = 1 + J = \{1, 1+a\}$. Since $x \neq 1-e$, $x + e = 1 + a$. Consequently, $ex + e^2 = e + ea = e + a$ and so $0 = ex = a$, a contradiction. Thus $(1-e)A(1-e)$ is isomorphic and homeomorphic to $\prod_{\alpha\in\Gamma_1} \mathbb{Z}/(2)$ for some nonempty set Γ_1 by [15, Theorem 16]. For simplicity of notation, assume that $(1-e)A(1-e) = \prod_{\alpha\in\Gamma_1} \mathbb{Z}/(2)$.

Let a^r denote the right annihilator of a in A and let $g : (1-e)A(1-e) \to J$ be given by $g(x) = ax$ for all x in $(1-e)A(1-e)$. Observe that g is a surjective additive group homomorphism with kernel $a^r \cap (1-e)A(1-e)$. So $a^r \cap (1-e)A(1-e)$ is a closed subset of $(1-e)A(1-e)$ and hence by Lemma 2.6, there exists a subset Γ_2 of Γ_1 such that $a^r \cap (1-e)A(1-e) = \prod_{\alpha \in \Gamma_1} B_\alpha$ where $B_\alpha = \mathbb{Z}/(2)$ for all α in Γ_2 and $B_\alpha = \{\bar{0}\}$ otherwise (where $\bar{0}$ is the additive identity of $\mathbb{Z}/(2)$). In particular, $a^r \cap (1-e)A(1-e)$ is a two-sided ideal of $(1-e)A(1-e)$. Moreover, as $(1-e)A(1-e)/a^r \cap (1-e)A(1-e) \cong J$, the cardinality, $|\Gamma_1 \backslash \Gamma_2|$, of $\Gamma_1 \backslash \Gamma_2$ is 1. Let $\alpha_0 \in \Gamma_1 \backslash \Gamma_2$ and let $I = \prod_{\alpha \in \Gamma_1} C_\alpha$ where $C_{\alpha_0} = \mathbb{Z}/(2)$ and for all $\alpha \in \Gamma_1 \backslash \{\alpha_0\}$, $C_\alpha = \{\bar{0}\}$. Then $(1-e)A(1-e) = I \oplus a^r \cap (1-e)A(1-e)$ and so $A = eAe \oplus [I \oplus a^r \cap (1-e)A(1-e)] \oplus eA(1-e)$. A routine proof shows that $eAe \oplus I \oplus eA(1-e)$ and $a^r \cap (1-e)A(1-e)$ are ideals of A, the first of which has 8 elements and the second of which is isomorphic and homeomorphic to $\prod_{\alpha \in \Gamma_2} \mathbb{Z}/(2)$ or to $\{\bar{0}\}$ if $\Gamma_2 = \emptyset$.

By construction, $I \cong \mathbb{Z}/(2)$. So if i is the multiplicative identity of I, then $e+i$ is the multiplicative identity of the ring $eAe \oplus I \oplus eA(1-e)$. Notice that $eAe \oplus I \oplus eA(1-e)$ is noncommutative as $ea \neq ae$. Thus $eAe \oplus I \oplus eA(1-e)$ is isomorphic to the ring of 2×2 upper triangular matrices over $\mathbb{Z}/(2)$ by [17, Theorem 14]. Consequently, if $eae = 0$, then A is isomorphic and homeomorphic to A_0 or to $\left(\prod_{\alpha \in \Gamma_2} \mathbb{Z}/(2)\right) \times A_0$ where A_0 is the ring of 2×2 upper triangular matrices over $\mathbb{Z}/(2)$.

Finally, suppose that $eae \neq 0$, that is, suppose that $eae = a$. We first show that e is in the center of A. Indeed, let $x \in A$. As A/J is commutative, $ex - xe \in J$. Therefore $ex - xe = 0$ or $ex - xe = a$. If $ex - xe = a$, then $e^2x - exe = ea = a = ex - xe$ and hence $exe = xe$. Similarly, $exe = ex$ and so in either case $ex = xe$. Thus e is in the center of A. In particular, $eA(1-e) = (1-e)Ae = \{0\}$ and so $A = eAe \oplus (1-e)A(1-e)$.

Recall that $eAe/eJe \cong \mathbb{Z}/(2)$, a finite field having two elements. So eAe is a local ring with identity having four elements and having characteristic 2. Consequently, by [3, Theorem 2.5], $eAe \cong \mathbb{Z}/(2)[x]/(x^2)$.

Since $ea = a$, $(1-e)a(1-e) = 0$. Therefore, as before, if $1 - e \neq 0$, then $(1-e)A(1-e)$ is isomorphic and homeomorphic to $\prod_{\alpha \in \Gamma} \mathbb{Z}/(2)$ for some nonempty set Γ. Otherwise, $(1-e)A(1-e) = \{0\}$. Thus A is isomorphic and homeomorphic to $\left(\prod_{\alpha \in \Gamma} \mathbb{Z}/(2)\right) \times \mathbb{Z}/(2)[x]/(x^2)$ or to $\mathbb{Z}/(2)[x]/(x^2)$. □

Theorem 2.8. *Let A be a compact ring with identity and let G be the group of units in A. G is simple if and only if A is isomorphic and homeomorphic to $\prod_{\alpha \in \Lambda} \mathbb{Z}/(2)$ for some nonempty set Λ or A is isomorphic and homeomorphic to $\left(\prod_{\alpha \in \Lambda} \mathbb{Z}/(2)\right) \times A_0$ where Λ is an arbitrary set and A_0 is one of the following rings:*

(1) *a finite field of cardinality 3 or 2^n for some positive integer n such that $2^n - 1$ is a prime,*

(2) *the set of $n \times n$ matrices over $\mathbb{Z}/(2)$ where n is a positive integer greater than or equal to 3,*

(3) $\mathbb{Z}/(4)$,

(4) $\mathbb{Z}/(2)[x]/(x^2)$, *or*

(5) *the ring of* 2×2 *upper triangular matrices over* $\mathbb{Z}/(2)$.

Proof. As $\mathrm{GL}(n, \mathbb{Z}/(2))$ is simple for all $n \geq 3$ [19, Theorem 9.9, p. 78], if A is one of the rings described above, then G is a finite simple group. Conversely, assume that G is a simple group. By Theorem 2.2, G is finite.

First assume that A is semisimple. By [15, Theorem 16], A is isomorphic and homeomorphic to $\prod_{\alpha \in \Lambda} M_\alpha$ where each M_α is the set of $n_\alpha \times n_\alpha$ matrices over a finite field F_α. For each α in Λ, let G_α denote the group of units in M_α. As G is a simple group, the set Λ_1 defined by $\Lambda_1 = \{\alpha \in \Lambda : |G_\alpha| > 1\}$ has at most one element. Moreover, if $\alpha \in \Lambda_1$, then G_α is a finite simple group. Thus for all β in $\Lambda \backslash \Lambda_1$, $M_\beta \cong \mathbb{Z}/(2)$ and if $\Lambda_1 = \{\alpha\} \neq \emptyset$, then M_α is a finite field such that the cardinality of G_α is a prime or M_α is isomorphic to the ring of $n \times n$ matrices over $\mathbb{Z}/(3)$ for some $n \geq 3$ [19, Theorem 9.9, p. 78].

Suppose then that $J \neq \{0\}$. Since $1+J$ is a closed normal subgroup of G, $G = 1+J$. Consequently, A/J is isomorphic and homeomorphic to $\prod_{\alpha \in \Lambda} \mathbb{Z}/(2)$ for some nonempty set Λ by [15, Theorem 16; 12, Theorem, p. 431; 13, Theorem, p. 171].

Since J is finite, $J^2 \neq J$ by Nakayama's Lemma [13, Theorem, p. 412]. Thus as $1 + J^2$ is a closed normal subgroup of $1 + J$, $J^2 = (0)$. In particular, as $G = 1 + J$, G is abelian and so the cardinality of G is a prime p. Note that $2 \in J$ since $A/J \cong \prod_{\alpha \in \Lambda} \mathbb{Z}/(2)$. Therefore as $J^2 = (0)$, the characteristic of A is either 2 or 4. Let $a \in J \backslash \{0\}$. If the characteristic of A is 2, then $(1+a)^2 = 1$ and hence the order of $1+a$ is 2. Thus $p = 2$. On the other hand, if the characteristic of A is 4, then $2 \in J \backslash \{0\}$ and $(1+2)^2 = 1$. Therefore in either case, $p = 2$, that is $1+J = G = \{1, 1+a\}$ for some nonzero a in J. By Lemma 2.7, it suffices to show that if A has characteristic 4, then A is isomorphic and homeomorphic to $\left(\prod_{\beta \in \Gamma} \mathbb{Z}/(2)\right) \times \mathbb{Z}/(4)$ for some indexing set Γ.

Assume then that the characteristic of A is 4. We first prove that A is a commutative ring. As $2 \in J \backslash \{0\}$, $J = \{0, 2\}$ and hence by Lemma 2.5, if e is any idempotent in A, then e is contained in the center of A. Consequently, A is commutative. Indeed, let $x \in A$. Then $x+J$ is an idempotent in A/J and hence there exists an idempotent e in A such that $x+J = e+J$ [15, Lemma 12]. Thus $x \in \{e, e+2\}$ and so x is in the center of A. Therefore by [15, Theorem 17], A is isomorphic and homeomorphic to $\prod_{\alpha \in \Lambda_1} N_\alpha$ where for each α in Λ_1, N_α is a commutative, local, compact ring with identity. For each α in Λ_1, let G_α denote the group of units in N_α and let J_α denote the Jacobson radical of N_α. As $A/J \cong \prod_{\alpha \in \Lambda} \mathbb{Z}/(2)$, for each α in Λ_1, $N_\alpha/J_\alpha \cong \mathbb{Z}/(2)$. Let Λ_2 be the subset of Λ_1 defined by, $\Lambda_2 = \{\alpha \in \Lambda_1 : |G_\alpha| > 1\}$. Then for all $\alpha \in \Lambda_1 \backslash \Lambda_2$, $|G_\alpha| = 1$ and hence $N_\alpha \cong \mathbb{Z}/(2)$. As before, since G is simple, Λ_2 has at most one element. But as A has characteristic 4, $\Lambda_2 \neq \emptyset$. Let $\Lambda_2 = \{\alpha_0\}$. Then A is isomorphic and homeomorphic to $\left(\prod_{\alpha \in \Lambda_1 \backslash \Lambda_2} \mathbb{Z}/(2)\right) \times N_{\alpha_0}$. It suffices to show that $N_{\alpha_0} \cong \mathbb{Z}/(4)$.

Observe that N_{α_0} has characteristic 4 as A has characteristic 4. Moreover, as $|G| = 2$, $|G_{\alpha_0}| = 2$ as well. Therefore $|N_{\alpha_0}| = 4$ since $N_{\alpha_0}/J_{\alpha_0} \cong \mathbb{Z}/(2)$. So N_{α_0} is a 4-element ring with identity having characteristic 4, that is, $N_{\alpha_0} \cong \mathbb{Z}/(4)$. □

Corollary 2.9. *Let A be a compact ring with identity and let G be the group of units in A. The following statements are equivalent*:

(a) *G possesses no nontrivial closed normal subgroups.*

(b) *G is a finite simple group.*

(c) *G is isomorphic to one of the following finite simple groups*:

  (1) *the trivial group*,

  (2) $\mathbb{Z}/(2)$,

  (3) $\mathbb{Z}/(2^n - 1)$ *where* $2^n - 1$ *is a prime or*

  (4) $GL(n, \mathbb{Z}/(2))$ *where* $n \geq 3$.

Proof. The corollary follows from Theorems 2.2 and 2.8. □

3. Simplicity of $G/Z(G)$

Throughout this section, unless otherwise stated, A is a compact ring with identity. For each subgroup U of G, we will denote the center of U by $Z(U)$.

Lemma 3.1. *$Z(G)$ is a closed normal subgroup of G and $G/Z(G)$ is a compact totally disconnected group.*

Proof. The fact that $Z(G)$ is a closed subset of G follows from the continuity of the map $(x, y) \to xyx^{-1}y^{-1}$. Since G is totally disconnected by Theorem 2.2, $G/Z(G)$ is also totally disconnected [10, Theorem 7.11, p. 63]. □

Lemma 3.2. *$G/Z(G)$ is a finite simple group if and only if $G/Z(G)$ has no nontrivial closed normal subgroups.*

Proof. The result follows from Lemmas 2.1 and 3.1. □

Lemma 3.3. *If $G/Z(G)$ is a finite simple group, then either $W = Z(W)$ or $W/Z(W) \cong G/Z(G)$.*

Proof. Assume that $W \neq Z(W)$. Since $WZ(G)$ is a normal subgroup of G containing $Z(G)$, $WZ(G) = Z(G)$ or $WZ(G) = G$. If $WZ(G) = Z(G)$, then $W \subseteq Z(G)$ and hence $W = Z(W)$, a contradiction. So $WZ(G) = G$. Therefore $G/Z(G) = WZ(G)/Z(G) \cong W/W \cap Z(G)$. In particular, $W/W \cap Z(G)$ is a simple group. Clearly, $W \cap Z(G) \subseteq Z(W)$. Therefore since $W/W \cap Z(G)$ is simple and since $W \neq Z(W)$ by assumption, $Z(W) = W \cap Z(G)$. So $G/Z(G) \cong W/Z(W)$. □

As in Section 1, for each $w \in W$, define the *length* $l(w)$ of w to be the smallest positive integer m such that there exist $w_1, w_2, \ldots, w_m$ in Δ with $w = w_1 w_2 \cdots w_m$. For each subset S of W, let $l(S) = \sup\{l(s)\colon s \in S\}$.

Lemma 3.4. *Let* $w \in W$ *be such that* $l(w) \leq 2$. *Then for each positive integer n,* $l(w^n) \leq 2$.

Proof. The result clearly holds if $l(w) = 1$, that is, if $w^2 = 1$. So assume that $l(w) = 2$. Let $d_1, d_2 \in \Delta$ be such that $w = d_1 d_2$ and let n be a positive integer. If $n = 2k+1$ for some positive integer k, then $w^n = [(d_1d_2)^k d_1][d_2(d_1d_2)^k]$ where $[(d_1d_2)^k d_1]^2 = [d_2(d_1d_2)^k]^2 = 1$ and so $l(w^n) \leq 2$. If n is an even integer, then $w^n = [(d_1d_2)^{n-2}d_1][d_2d_1d_2]$ where $[(d_1d_2)^{n-2}d_1]^2 = (d_2d_1d_2)^2 = 1$ and so once again, $l(w^n) \leq 2$. □

The following was proved in [6].

Lemma 3.5. *Suppose that* 2 *is a unit in A. The following are equivalent*:

(1) $\{g \in (1+J) \cap W\colon l(g) \leq 2\} = \{1\}$.

(2) $(1+J) \cap W = \{1\}$.

(3) *A is isomorphic and homeomorphic to* $\prod_{\alpha \in \Lambda} N_\alpha$ *where for each* α *in* Λ, N_α *is a matrix ring over a finite field of odd characteristic or* N_α *is a compact local ring with identity such that the characteristic of* N_α/J_α *is an odd prime where* J_α *is the Jacobson radical of* N_α.

Proof. See [6, Theorem 2.6]. □

Lemma 3.6. *Let F be a finite field having odd characteristic, let n be a positive integer and let* $A = M(n, F)$, *the ring of* $n \times n$ *matrices over F.*

(1) $W = \{x \in A\colon \det x = \pm 1\}$ *and* $l(W) \leq 4$.

(2) $Z(W) = Z(G) \cap W$.

(3) $W/Z(W)$ *is simple if and only if there is a k in F with* $k^n = -1$.

Proof. (1) holds by [9]. Clearly (2) and (3) hold when $n = 1$. So assume that $n \geq 2$. Notice that since F has odd characteristic, if $w \in G$, then $w\,\mathrm{diag}(1,1,\ldots,1,-1) = \mathrm{diag}(1,1,\ldots,1,-1)\,w$ if and only if

$$w = \begin{pmatrix} & & 0 \\ & B & \vdots \\ & & 0 \\ 0 & \ldots\ 0 & a_{nn} \end{pmatrix}$$

for some nonsingular matrix B in $M(n-1, F)$ and for some a_{nn} in $F \backslash \{0\}$. In particular, if $w \in Z(W)$, then w has the above form. So for all w in $Z(W)$ and for all k in $F\backslash\{0\}$, $w\,\mathrm{diag}(1,1,\ldots,1,k) = \mathrm{diag}(1,1,\ldots,1,k)w$. As $G = W\{\mathrm{diag}(1,1,\ldots,1,k)\colon k \in F\backslash\{0\}\}$ [18, Lemma 8.13, p. 163], $Z(W) \subseteq Z(G)$ and hence (2) holds.

Denote $\{x \in A\colon \det x = 1\}$ by $\mathrm{SL}(n,F)$. By (1) and (2), $Z(W) = \{\alpha I\colon \alpha^n = \pm 1\}$ where I is the $n \times n$ identity matrix in A. Hence as $Z(\mathrm{SL}(n,F)) = \{\alpha I\colon \alpha^n = 1\}$ [18, Theorem 8.15, p. 164], $Z(\mathrm{SL}(n,F)) = \mathrm{SL}(n,F) \cap Z(W)$.

Suppose there is a k in F with $k^n = -1$. Since $kI \in Z(W)$ and $\det(kI) = -1$, $\mathrm{SL}(n,F)Z(W) = W$. Therefore, $W/Z(W) = \mathrm{SL}(n,F)Z(W)/Z(W) \cong \mathrm{SL}(n,F)/(\mathrm{SL}(n,F) \cap Z(W)) = \mathrm{SL}(n,F)/Z(\mathrm{SL}(n,F)) = \mathrm{PSL}(n,F)$, the projective unimodular group. Therefore if $n \geq 3$, then $W/Z(W)$ is simple by the Jordan–Dickson Theorem [18, Theorem 8.27, p. 174]. Since there exists a k in F with $k^n = -1$, if $n = 2$, then the cardinality of F must be greater than 3. Consequently, $W/Z(W)$ is simple by the Jordan–Moore Theorem [18, Theorem 8.19, p. 167].

Conversely, assume that $W/Z(W)$ is simple. If for all k in F, $k^n \neq -1$, then $Z(W) = \{\alpha I\colon \alpha^n = 1\}$ and hence $\mathrm{SL}(n,F)/Z(W)$ is a proper normal subgroup of $W/Z(W)$, a contradiction. Therefore (3) holds. □

Lemma 3.7. *Suppose that 2 is a unit in A and that $G/Z(G)$ is a finite simple group. If $l(Z(W)) \leq 4$ or if $Z(W)$ is a torsion group, then $(1+J) \cap W \subseteq Z(G)$.*

Proof. Assume that $l(Z(W)) \leq 4$. By Lemma 3.2, since $G/Z(G)$ is a simple group, $G/Z(G)$ is finite. Therefore by the Feit–Thompson Theorem [8, Theorem, p. 775], the order, $|G/Z(G)|$, of $G/Z(G)$ is 1, a prime p or $2^n q$ where n is a positive integer and q is an odd integer. The result clearly holds if $|G/Z(G)| = 1$ and so we may assume that $|G/Z(G)|$ is a prime p or $|G/Z(G)|$ is even.

Suppose first that $|G/Z(G)| = 2$. We will prove that $(1+J) \cap W = \{1\}$. By Lemma 3.5 it suffices to show that if $w \in (1+J) \cap W$ and $l(w) \leq 2$, then $w = 1$. Let $d_1, d_2 \in \Delta$ where $d_1 d_2 \in 1+J$. If $d_1 d_2 \neq 1$, let $a \in J \backslash \{0\}$ be such that $d_1 d_2 = 1 + a$. Then $(d_1 d_2)^2 \neq 1$. Indeed, if $(d_1 d_2)^2 = 1$, then $1 + 2a + a^2 = (1+a)^2 = 1$ and so $a(2+a) = 0$. But $2 + a$ is a unit in A and consequently $a = 0$, a contradiction. So $(d_1 d_2)^2 \neq 1$. Therefore, $(d_1 d_2)^2 \in (1+J) \backslash \{1\}$ and so there exists a nonzero b in J with $(d_1 d_2)^2 = 1 + b$. By Lemma 3.4, $(d_1 d_2)^2 = \sigma_1 \sigma_2$ for some $\sigma_1, \sigma_2 \in \Delta$. Since $|G/Z(G)| = 2$, $\sigma_1 \sigma_2 = (d_1 d_2)^2 \in Z(G)$. Therefore $(1+b)^2 = (\sigma_1 \sigma_2)^2 = (\sigma_1 \sigma_2) \sigma_1 \sigma_2 = \sigma_1 (\sigma_1 \sigma_2) \sigma_2 = 1$. Hence $b(2+b) = 0$ and so $b = 0$, a contradiction. Consequently, if $|G/Z(G)| = 2$, then $(1+J) \cap W = \{1\} \subseteq Z(G)$.

Assume that $|G/Z(G)|$ is an odd prime p. Let $d \in \Delta$. Then $d = d^p \in Z(G)$ and therefore $W \subseteq Z(G)$.

Finally, assume that $|G/Z(G)| = 2^n q$ where n is a positive integer and q is odd. As $(1+J) \cap W$ is a normal subgroup of G, $((1+J) \cap W)Z(G) = G$ or $((1+J) \cap W)Z(G) = Z(G)$. In order to prove that $(1+J) \cap W \subseteq Z(G)$, it suffices to prove that $((1+J) \cap W)Z(G) \neq G$. Suppose that $((1+J) \cap W)Z(G) = G$. Since $|G/Z(G)|$ is even, there exists a g in G such that the order of $gZ(G)$ in $G/Z(G)$ is 2. As $((1+J) \cap W)Z(G) = G$, there exists a nonzero element a in J such that $1 + a \in W$ and $gZ(G) = (1+a)Z(G)$. Let $w = (1+a)^2$. Then $w \in W \cap Z(G) \subseteq Z(W)$. Observe that w has finite order. Indeed, since $l(Z(W)) \leq 4$, $w = d_1 d_2 d_3 d_4$ where each d_i is in Δ. As $w \in Z(G)$, an inductive argument establishes that for each positive integer k, $w^k = (d_1 d_2)^k (d_3 d_4)^k$. Let $k = |G/Z(G)|$. By Lemma 3.4, there exist $\sigma_1, \sigma_2, \sigma_3, \sigma_4 \in \Delta$ such that $(d_1 d_2)^k = \sigma_1 \sigma_2$ and $(d_3 d_4)^k = \sigma_3 \sigma_4$. Since $\sigma_1 \sigma_2 = (d_1 d_2)^k \in Z(G)$ and $\sigma_3 \sigma_4 = (d_3 d_4)^k \in Z(G)$, $(\sigma_1 \sigma_2)^2 = (\sigma_3 \sigma_4)^2 = 1$. Therefore $w^{2k} = 1$. Let k_1 be the order of w. Write $k_1 = 2^i k_0$ where i is a nonnegative integer and k_0 is odd. Recall that $w = (1+a)^2$. Notice that as the order of $(1+a)Z(G)$ in $G/Z(G)$ is 2, $(1+a)^{k_0} \neq 1$. So $(1+a)^{k_0} = 1+b$ for some nonzero b in J. Hence $(1+b)^{2^{i+1}} = (1+a)^{2\cdot 2^i k_0} = w^{k_1} = 1$. Therefore

$$b\left[2^{i+1} + \binom{2^{i+1}}{2} b + \cdots + b^{2^{i+1}-1}\right] = 2^{i+1}b + \binom{2^{i+1}}{2} b^2 + \cdots + b^{2^{i+1}} = 0.$$

But 2^{i+1} is a unit in A and $\binom{2^{i+1}}{2} b + \cdots + b^{2^{i+1}-1} \in J$. Consequently $b = 0$, a contradiction.

Observe that in the above argument, the assumption that $l(Z(W)) \leq 4$ was only used to prove that if $|G/Z(G)|$ is even and if $w \in W \cap Z(G)$, then w has finite order. Consequently a similar proof establishes that if $Z(W)$ is a torsion group, then $(1+J) \cap W \subseteq Z(G)$ as well. □

Theorem 3.8. *Let A be a compact ring with identity for which 2 is a unit in A. Let G denote the group of units in A and let W be the subgroup of G generated by the set $\{g \in G: g^2 = 1\}$ of involutions of G. Suppose that $(1+J) \cap W \subseteq Z(G)$. Then the following are equivalent:*

(1) $G/Z(G)$ is a finite simple group.

(2) A is isomorphic and homeomorphic to one of the following rings:

(i) $M(n,F) \times \prod_{\alpha \in \Lambda} N_\alpha$ where $M(n,F)$ is the ring of $n \times n$ matrices over a finite field F of odd characteristic for which there exists an element k in F satisfying $k^n = -1$ and for each α in Λ, N_α is a commutative compact local ring with identity such that the characteristic of N_α/J_α is an odd prime where J_α is the Jacobson radical of N_α,

(ii) $N \times \prod_{\alpha \in \Lambda} N_\alpha$ where N is a compact local ring with identity such that the characteristic of $N/J(N)$ is an odd prime and $G(N)/Z(G(N))$ is a simple group and where for each α in Λ, N_α has the properties described in (i), *or*

(iii) $\prod_{\alpha \in \Lambda} N_\alpha$ where Λ is a nonempty set and for each α in Λ, N_α has the properties described in (i).

Proof. By Lemma 3.6, if A is isomorphic to a ring of type (i), then $G/Z(G)$ is a simple group. Therefore 2° implies 1°.

Conversely, assume that $G/Z(G)$ is a simple group. Denote $\{g \in G : l(g) \leq 2\}$ by Δ^2. Then $(1+J) \cap \Delta^2 \subseteq (1+J) \cap W \subseteq Z(G)$. Therefore $(1+J) \cap \Delta^2 = \{1\}$. Indeed, if $d_1, d_2 \in \Delta$ and $d_1 d_2 \in 1+J$, then $(d_1 d_2)^2 = (d_1 d_2) d_1 d_2 = d_1 (d_1 d_2) d_2$ as $d_1 d_2 \in Z(G)$. So $(d_1 d_2)^2 = 1$. Hence if $d_1 d_2 = 1 + a$ where $a \in J$, then $(1+a)^2 = (d_1 d_2)^2 = 1$. So $a(2+a) = 0$. Consequently, as 2 is a unit in A and as $a \in J$, $a = 0$. Thus $d_1 d_2 = 1$. Therefore by Lemma 3.5, A is isomorphic and homeomorphic to $\prod_{\alpha \in \Lambda} N_\alpha$ where for each α in Λ, N_α is a matrix ring over a finite field having odd characteristic or N_α is a compact local ring with identity such that the characteristic of N_α/J_α is an odd prime where J_α is the Jacobson radical of N_α. For each α in Λ, let G_α denote the group of units in N_α. Since $G/Z(G)$ is simple, the subset Λ_1 of Λ defined by

$\Lambda_1 = \{\alpha \in \Lambda\colon G_\alpha$ is nonabelian$\}$, has at most one element. Note that for each α in $\Lambda \backslash \Lambda_1$, N_α is a commutative ring by [3, Theorem 3.10]. Suppose that $\Lambda_1 \neq \emptyset$. Let $\alpha \in \Lambda_1$. Since $G_\alpha/Z(G_\alpha)$ is a simple group, A is isomorphic and homeomorphic to a ring of type (i) or of type (ii) by Lemma 3.6. □

Corollary 3.9. *Let A be a compact ring with identity for which 2 is a unit. The following are equivalent:*

(1) *$G/Z(G)$ is a finite simple group and $l(W) \leq 4$.*

(2) *$G/Z(G)$ is a finite simple group and $l(Z(W)) \leq 4$.*

(3) *$G/Z(G)$ is a finite simple group and $(1+J) \cap W \subseteq Z(G)$.*

(4) *A is isomorphic and homeomorphic to a ring of type* (i), (ii) *or* (iii) *as described in Theorem* 3.8.

(5) *$G/Z(G)$ is a finite simple group and W is a torsion group.*

(6) *$G/Z(G)$ is a finite simple group and $Z(W)$ is a torsion group.*

Proof. By Lemma 3.7, (2) implies (3). Theorem 3.8 yields that (3) implies (4). Note that if N is a compact local ring with identity for which 2 is a unit, then $W(N) = \{\pm 1\}$ by [4, Theorem 2.9] (and in particular, $l(W(N)) = 1$). Consequently (4) implies (5). By Lemma 3.7, (6) implies (3) and hence (3)–(6) are equivalent. Lemma 3.6 and the above observation yield that if A is isomorphic to a ring of type (i), (ii) or (iii) as described in Theorem 3.8, then $l(W) \leq 4$. Thus (1)–(6) are equivalent. □

4. Nilpotency and commutativity of W

Lemma 4.1. *Let A be a compact ring with identity for which W is a nilpotent group. Then there exists a positive integer m such that for all $\sigma_1, \sigma_2 \in \Delta$, $(\sigma_1\sigma_2)^{2^m} = 1$.*

Proof. Let $\{1\} = Z_0 \subseteq Z_1 \subseteq \cdots \subseteq Z_{m-1} \subseteq Z_m = W$ be the ascending central series for W. So for all i, $0 \leq i \leq m-1$, $Z_{m-i}/Z_{m-(i+1)}$ is the center of $W/Z_{m-(i+1)}$. Let $\sigma_1, \sigma_2 \in \Delta$. Since Z_m/Z_{m-1} is abelian, $(\sigma_1\sigma_2)^2 \in Z_{m-1}$. By Lemma 3.4, there exist $\sigma_1^{(2)}$ and $\sigma_2^{(2)}$ in Δ such that $(\sigma_1\sigma_2)^2 = \sigma_1^{(2)}\sigma_2^{(2)}$. Since Z_{m-1}/Z_{m-2} is the center of W/Z_{m-2} and since $\sigma_1^{(2)}\sigma_2^{(2)} \in Z_{m-1}$, $(\sigma_1^{(2)}\sigma_2^{(2)})\sigma_1^{(2)}Z_{m-2} = \sigma_1^{(2)}(\sigma_1^{(2)}\sigma_2^{(2)})Z_{m-2}$, that is, $(\sigma_1^{(2)}\sigma_2^{(2)})^2 \in Z_{m-2}$. So $(\sigma_1\sigma_2)^{2^2} \in Z_{m-2}$. An inductive proof then establishes that $(\sigma_1\sigma_2)^{2^m} \in Z_0 = \{1\}$. □

Theorem 4.2. *Let A be a compact ring with identity for which 2 is a unit in A. The following are equivalent:*

(1) *W is a nilpotent group.*

(2) *A is isomorphic and homeomorphic to a product, $\prod_{\alpha \in \Lambda} N_\alpha$, where Λ is a nonempty set and for each α in Λ, N_α is a compact local ring with identity such that the characteristic of N_α/J_α is an odd prime p_α where J_α is the Jacobson radical of N_α.*

(3) *W is abelian.*

(4) *$W = \Delta$.*

Proof. (3) and (4) are equivalent by [6, Corollary 2.9]. Assume that W is nilpotent. Let $\sigma_1, \sigma_2 \in \Delta$ be such that $\sigma_1\sigma_2 \in 1 + J$. Then $\sigma_1\sigma_2 = 1 + a$ for some a in J. By Lemma 4.1, there exists a positive integer m such that $(\sigma_1\sigma_2)^{2^m} = 1$. Then $1 = (\sigma_1\sigma_2)^{2^m} = (1 + a)^{2^m}$ and so $0 = 2^m a + \binom{2^m}{2}a^2 + \cdots + a^{2^m} = a(2^m + \binom{2^m}{2}a + \cdots + a^{2^m-1})$. Since 2^m is a unit in A and since $a \in J$, $2^m + \binom{2^m}{2}a + \cdots + a^{2^m-1}$ is a unit in A. Hence $a = 0$, that is, $(1 + J) \cap \Delta^2 = \{1\}$. Therefore by Lemma 3.5, A is isomorphic and homeomorphic to a product, $\prod_{\alpha\in\Lambda} N_\alpha$, where for each α in Λ, N_α is the ring of $m_\alpha \times m_\alpha$ matrices over a finite field F_α having odd characteristic or N_α is a compact local ring with identity for which the characteristic of N_α/J_α is an odd prime p_α. Suppose that there exists an α in Λ such that N_α is the ring of $m_\alpha \times m_\alpha$ matrices over a finite field F_α where $m_\alpha > 1$. Denote $W(N_\alpha)$ by W_α. Since W_α is a homomorphic image of W, W_α is a nilpotent group [18, Theorem 5.25, p. 90] and consequently W_α is solvable. By [9], $W_\alpha = \{x \in N_\alpha\colon \det x = \pm 1\}$ and so $\mathrm{SL}(m_\alpha, F_\alpha) \subseteq W_\alpha$ (where $\mathrm{SL}(m_\alpha, F_\alpha) = \{x \in N_\alpha\colon \det x = 1\}$). Therefore, $\mathrm{SL}(m_\alpha, F_\alpha)$ is solvable [18, Theorem 5.12, p. 81]. So if Z is the center of $\mathrm{SL}(m_\alpha, F_\alpha)$, then $\mathrm{SL}(M_\alpha, F_\alpha)/Z$ is solvable as well [18, Theorem 5.13, p. 81]. By [19, Corollary, p. 80], $m_\alpha = 2$ and F_α has cardinality 3. Therefore we may assume that W_α is the group, $\mathrm{GL}(2, \mathbb{Z}/(3))$, of 2×2 nonsingular matrices over $\mathbb{Z}/(3)$ by [9]. A routine calculation shows that if Z_1 is the center of $\mathrm{GL}(2, \mathbb{Z}/(3))$, then $\mathrm{GL}(2, \mathbb{Z}/(3))/Z_1$ has a trivial center. Therefore if $m_\alpha > 1$, then W_α is not nilpotent. Hence (1) implies (2).

Clearly (3) implies (1) and so it suffices to prove that (2) implies (3). Assume that (2) holds. For each α in Λ, let W_α denote $W(N_\alpha)$. By Theorem 2.9 of [4], for each α in Λ, W_α has precisely two elements. Therefore W is abelian. □

Corollary 4.3. *Let A be a compact ring with identity such that 2 is a unit in A. The following are equivalent*:

(1) *W is abelian and G/W is abelian.*
(2) *A is a commutative ring.*
(3) *G is abelian.*

Proof. It suffices to prove that (1) implies (2). If W is abelian, then $A \cong \prod_{\alpha\in\Lambda} N_\alpha$ where for each α in Λ, N_α is a compact local ring with identity such that the characteristic of N_α/J_α is an odd prime where J_α is the Jacobson radical of N_α. For each α in Λ, let 1_α denote the multiplicative identity of N_α and let G_α and W_α denote $G(N_\alpha)$ and $W(N_\alpha)$, respectively. Note that by [4, Theorem 2.9], for each α in Λ, $W_\alpha = \{\pm 1_\alpha\}$ (and hence $W \cong \prod_{\alpha\in\Lambda}\{\pm 1_\alpha\}$). By [3, Theorem 3.10], it suffices to prove that if, in addition, G/W is abelian, then G is abelian, that is, if G/W is abelian, then G_α is abelian for all α in Λ.

Let $\alpha \in \Lambda$. As N_α/J_α is a compact local ring with identity, N_α/J_α is a finite field by [15, Theorem 16]. Thus since $g \in G_\alpha$ if and only if $g + J_\alpha$ is a unit in N_α/J_α, there exist an element g_α in G_α and a positive integer m such that $G_\alpha = \bigcup_{n=0}^{m}(g_\alpha^n + J_\alpha)$. Observe that $xy = yx$ for all x and y in J_α. Indeed, if $xy \neq yx$ for some x and y in J_α, then $(1_\alpha + x)(1_\alpha + y) = -(1_\alpha + y)(1_\alpha + x)$ since G_α/W_α is abelian and since $W_\alpha = \{\pm 1_\alpha\}$.

So $2 \cdot 1_\alpha = -[yx + xy + 2(x + y)] \in J_\alpha \cap G_\alpha$, a contradiction. Similarly, $g_\alpha x = xg_\alpha$ for all x in J_α. Therefore as $G_\alpha = \bigcup_{n=0}^{m}(g_\alpha^n + J_\alpha)$, G_α is abelian and consequently (1) implies (2). □

References

[1] N. Bourbaki, Topologie Générale (Hermann, Paris, 1960) Chapters 3 and 4.
[2] C. Chevalley, Theory of Lie Groups (Princeton University Press, Princeton, NJ, 1946).
[3] J. Cohen and K. Koh, The group of units in a compact ring, J. Pure and Appl. Algebra 54 (1988) 167–179.
[4] J. Cohen and K. Koh, Involutions in a compact ring, J. Pure Appl. Algebra 59 (1989) 151–168.
[5] J. Cohen and K. Koh, The subgroup generated by the involutions in a compact ring, Comm. Algebra 19 (1991) 2923–2954.
[6] J. Cohen and K. Koh, The structure of compact rings, J. Pure Appl. Algebra 77 (1992) 117–129.
[7] R. Ellis, A note on the continuity of the inverse, Proc. Amer. Math. Soc. 8 (1957) 372-373.
[8] W. Feit and J. Thompson, Solvability of groups of odd order, Pacific J. Math. 13 (1963) 775–1029.
[9] W. Gustafson, P. Halmos and H. Radjavi, Product of involutions, Linear Algebra Appl. 13 (1976) 157–162.
[10] E. Hewitt and K. Ross, Abstract Harmonic Analysis I (Springer, Berlin, 1963).
[11] E. Hewitt and K. Ross, Abstract Harmonic Analysis II (Springer, Berlin, 1970).
[12] N. Jacobson, Basic Algebra I (Freeman, San Francisco, 1974).
[13] N. Jacobson, Basic Algebra II (Freeman, San Francisco, 1980).
[14] N. Jacobson, Structure of Rings, Vol. 37 (A.M.S. Coll. Pub., Providence, RI, 1968).
[15] I. Kaplanksy, Topological rings, Amer. J. Math. 69 (1947) 153–183.
[16] S. Lang, $SL_2(\mathbf{R})$ (Springer, New York, 1985).
[17] R. Raghavendrun, Finite associative rings, Composition Math. 21 (1969) 195–229.
[18] J. Rotman, An Introduction to the Theory of Groups (Allyn and Bacon, Boston, 3rd ed., 1984).
[19] M. Suzuki, Group Theory I (Springer, New York, 1982).