JOURNAL OF ALGEBRA 31, 218–244 (1974)

Six Impossible Rings

WILFRID HODGES

Bedford College, Mathematics Department, Regent's Park, London NW1

Communicated by P. M. Cohn

Received January 16, 1973

We construct six rings whose properties are known to contradict Zorn's Lemma. We hasten to add that these rings do not really have the properties in question. In each case the ring R has the properties *from the point of view of* a certain universe M of sets which contains R. M will satisfy all of the axioms of Zermelo–Fraenkel set theory except Zorn's Lemma (= Axiom of Choice). Hence each ring with its accompanying universe of sets will constitute a proof that some well known theorem about rings cannot be proved without using Zorn's Lemma.

The basic tool for any such construction must be set-theoretic forcing as invented in 1963 by P. J. Cohen [2]. Fortunately, we shall not need to use any high power set theory in this note; we can rely on a more or less algebraic lemma (Lemma 3 below) which tells us what we need for the purpose in hand. A proof of this lemma will be given elsewhere [5], together with other applications.

In Section 1 we describe the necessary background from logic; Section 2 lists the six bad rings; Section 3 is a brief analysis, concentrating on chain conditions. This note is meant to be intelligible to algebraists; logicians will have to forgive a few shoddy definitions.

1. Tools From Logic

By *Zermelo-Fraenkel set theory*, abbreviated to ZF, we shall mean the following axioms for set theory:

(a) (Extensionality) No two distinct sets have just the same members.

(b) (Pair–set) For any sets x, y there is a set whose members are just x and y.

(c) (Sum–set) For any set x there is a set whose members are the members of members of x.

(d) (Power–set) For any set x there is a set whose members are the subsets of x.

(e) (Replacement) If x is a function definable by a first order formula, and the domain of x is a set, then the image of x is a set. (This is an axiom schema, yielding an axiom for each first order formula.)

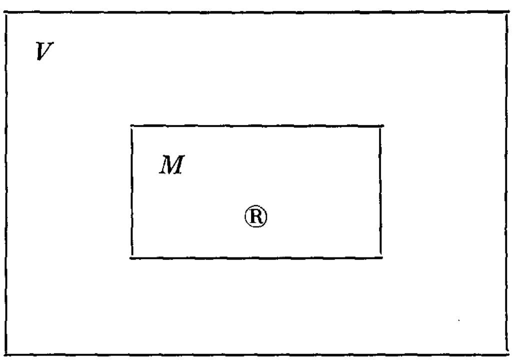
(f) (Infinity) The set of all natural numbers exists.

(g) (Regularity) Every non-empty set x has a member y such that x and y are disjoint.

ZF does not include Zorn's Lemma or any form of the Axiom of Choice; we write ZFC for ZF with Zorn's Lemma added. (See Cohen [2] for a fuller account.)

Leaving on one side some subtleties about categories (see Feferman [3]), every theorem of ring theory can be proved from ZFC. We shall show that certain well known results are not provable from ZF alone. Zorn's Lemma is peculiar among the axioms of ZFC, in that it says that certain sets exist without specifying exactly what is in them. Hence a proof using Zorn must be in a sense less explicit than one using only ZF. This is no reason for doubting the truth of Zorn, but it is a reason for investigating what can be done with ZF alone.

The setting will be as follows:



Here V is the "real world" of sets. To say that something is true "in V" is merely to say that it's true. We shall take for granted throughout that every axiom of ZFC is true in V, including Zorn's Lemma. M is a transitive model of ZF; which means the following.

(a) M is a nonempty set, and every member of a member of M is again a member of M.

(b) Let φ be any axiom of ZF, and interpret "set" in φ as meaning "set in M", i.e., as "member of M"; then φ is true under this interpretation.

The ring R is a member of the set M; so by (a), every element of R is also a member of M.

A set theoretic statement φ about members $x_1, \ldots, x_n$ of M can be interpreted in two ways.

In the *V-interpretation* of φ we take "set" to mean "set in V"; this is the straightforward and usual interpretation of φ.

In the *M-interpretation* of φ we take "set" to mean "set in M".

If φ is true in the M-interpretation, and ψ is a logical consequence of φ, then ψ must also be true in the M-interpretation. Since every axiom of ZF is true in the M-interpretation, this guarantees the following basic lemma.

LEMMA 1. *In the above setting, let φ be a statement of set theory which is not true in the M-interpretation. Then φ is not deducible from* ZF.

Set theorists single out a class of statements which they call *absolute*; an absolute statement must necessarily be true in the V-interpretation if and only if it's true in the M-interpretation, whenever V and M are as above. To avoid writing a textbook of set theory, we simply list here some important and typical statements which are absolute.

LEMMA 2. *The following statements are absolute*:

(a) *R is a commutative ring.*

(b) *R is an integral domain.*

(c) *R is a boolean ring.*

(d) *x is an element of the ring R.*

(e) $x + y = z$ *in R.*

(f) $x \cdot y = z$ *in R.*

(g) *I is an ideal of R.*

(h) *I is a maximal (prime, nil, nilpotent, idempotent) ideal of R.*

(i) *$x_1, \ldots, x_n$ are generators of the ideal I in R.*

(j) *The set X is finite.*

(k) *$(I_i)_{i \in \omega}$ is a strictly ascending (descending) chain of ideals of R.*

(These are all easy exercises given Cohen [2] p. 92ff. or Shoenfield [8] p. 265ff. For example, I is a *maximal* ideal of R iff $(\forall x \in R)[x \notin I \rightarrow (\exists y \in I)(\exists z \in R)[y + zx = 1]]$ & $1 \notin I$.) Broadly, a statement about R is absolute if it expresses elementary structural properties of R and does not talk of "all ideals" of R; though note that an absolute statement may talk of "all elements" of R.

M need not contain every subset of R which is in V; in fact M may miss some of the ideals of R. In Ring 1 below we shall see an example where R is an integral domain and no maximal ideal of R is in M; in this case the statement "R has a maximal ideal" is true in the V-interpretation but false in the M-interpretation. The statement "There is an integral domain with no maximal ideal" is then true in the M-interpretation. By Lemma 1, this constitutes a proof that ZF alone does not require every integral domain to have a maximal ideal.

Everything depends on our being able to ensure that such and such subsets of R are or are not in M. One fact we can rely on is the following. Suppose X is a subset of R, and suppose there is an absolute statement $S(x)$ which expresses "x is in X". ZF then implies the existence of the set $\{x : S(x)\}$; so ZF in the M-interpretation implies the existence in M of $\{x : S(x)$ in the M-interpretation$\}$. Since $S(x)$ is absolute, this means the set $X = \{x : S(x)\}$ is in M. A typical example occurs in Ring 3: the ideal generated by the atoms of a boolean algebra R is defined by the absolute formula "the set of elements $<x$ in R is finite".

When this method fails, we can ensure that a subset X of R gets into M by adding X as a *distinguished subset* to R. This means that X becomes part of the structure of R in the same way as $+$ and $\cdot$. The price we pay is that any automorphism of the resulting structure must respect X; this may exclude some ring automorphisms of the original structure R. We may in the same way add not just one distinguished subset to R, but a countable sequence $(X_i)_{i\in\omega}$ of distinguished subsets.

The main device for ensuring that subsets of R do *not* reach M is Lemma 3 below; it needs some preliminary definitions.

Let R be a ring (possibly with distinguished subsets), and let X be a subset of R. Then by a *support* of X, we mean a finite subset supp_X of R, such that if s is any automorphism of R which pointwise fixes supp_X, then $X = \{sx : x \in X\}$. Likewise if $X = (X_i)_{i\in\omega}$ is a countable sequence of subsets of R, then by a *support* of X we mean a finite subset supp_X of R which is a support of each X_i $(i \in \omega)$. (NB: an automorphism of R must respect the distinguished subsets.)

For example, any finitely generated ideal of R has a support, viz., a finite set of generators.

Let R be a ring (possibly with distinguished subsets), which is a member of the transitive model M of ZF. Then we shall call R *M-symmetric* if every subset of R which is in M has a support, and every sequence of subsets of R which is in M has a support.

LEMMA 3 (Removal of subsets). *Let R be a countable ring, possibly with up to countably many distinguished subsets. Then there is a transitive model $N(R)$ of* ZF *which contains an $N(R)$-symmetric isomorphic copy of R.*

There is no real danger of confusion in the arguments below if we identify this isomorphic copy of R with R itself.

Lemma 3 is proved (Hodges [5]) by extending the method invented by P. J. Cohen [2] to show the independence from ZF of the countable axiom of choice. The Lemma rests on fairly strong Cantorian assumptions about the world of sets. Set theorists have a uniform way of rewriting proofs of this type, so that they become strict formal proofs from ZF alone that this or that statement is unprovable from ZF alone unless ZF is inconsistent (cf. Cohen [2] p. 148). We could have presented our results in this strict style; suffice it to say that they would then be completely unintelligible.

Finally two conventions. Every ring is assumed to have a multiplicative identity 1, not necessarily nonzero. Also we freely write $(x_i)_i$ for the indexed set $(x_i)_{i \in I}$ when it is clear from the context what the index set I is.

2. THE RINGS

In this section we claim to construct six rings R, each of which has some specified properties P. These claims should be understood as follows. In each case we do construct a ring R. R will be countable with at most countably many distinguished subsets; hence by Lemma 3 there is a transitive model $N(R)$ of ZF which contains an $N(R)$-symmetric isomorphic copy of R. For ease of presentation we identify this copy with R itself. The claim is that the statement "R has property P" is true in the $N(R)$-interpretation.

The arguments proving these claims are to be taken completely at face value. For example, if we construct an automorphism of R, we do not require the automorphism to be a member of $N(R)$.

RING 1. *An integral domain R such that*

(a) *every ideal of R is finitely generated;*

(b) *R has no maximal ideal.*

R shall be the polynomial ring $Q[X_i]_{i \in \omega}$ over Q (the field of rationals) in the countably many distinct indeterminates X_i $(i \in \omega)$. We can define a preordering relation $\prec$ on the nonzero elements of R as follows. If x is a nonzero element of R, write $\deg_i x$ for the degree of x as a polynomial in X_i, and ord x for the largest i such that $\deg_i x \neq 0$. We put

$$x \prec y \quad \text{iff} \quad \text{either } \operatorname{ord} x < \operatorname{ord} y, \quad \text{or} \quad \operatorname{ord} x = \operatorname{ord} y \text{ and } \deg_{\operatorname{ord} x} x < \deg_{\operatorname{ord} x} y.$$

Clearly every nonempty set of nonzero elements of R contains a $\prec$-minimal element.

Let I be an ideal of R in $N(R)$. Then I has a support supp_I. Taking i to be the least nonnegative integer such that $\text{supp}_I \subseteq Q[X_k]_{k<i}$, put $J = I \cap Q[X_k]_{k<i}$. By Hilbert's Basis Theorem (Zariski and Samuel [10] p. 201), J is a finitely generated ideal of $Q[X_k]_{k<i}$. (Remark: we are here assuming that the Basis Theorem is true—which it is; we are not claiming that the $N(R)$-interpretation of it is true, which would need further argument.)

We claim that $I = JR$. Clearly $JR \subseteq I$. Suppose then that $I \not\subseteq JR$; let z be a $\prec$-minimal element of $I - JR$, and put $j = \text{ord}\, z$. There is a unique automorphism s of R such that

$$s(X_k) = \begin{cases} X_j + 1 & \text{if } k = j \\ X_k & \text{if } k \neq j. \end{cases}$$

Certainly s pointwise fixes supp_I, since $j \geqslant i$. Hence we have $sz \in I$, so $sz - z \in I$. Let c be the leading coefficient of z when written as a polynomial in X_j. Then $c \notin JR$; for otherwise $z - cX_j^{\deg_j z} \in I$ and $z - cX_j^{\deg_j z} \prec z$, which by choice of z implies that $z - cX_j^{\deg_j z} \in JR$ and so $z \in JR$, contradicting the choice of z. A simple computation shows that the leading coefficient of $sz - z$ as a polynomial in X_j is $(\deg_j z)c$. But $JR = J[X_k]_{i \leqslant k \in \omega}$, whence it follows that $sz - z \notin JR$. Hence $sz - z \in I - JR$. But $\deg_j(sz - z) < \deg_j z$, so $sz - z \prec z$. This contradicts the choice of z once again, so the claim is proved.

Since JR is finitely generated, the claim implies the same for I. But the statement "I is a finitely generated ideal of R" is absolute, by Lemma 2, as is the statement "R is an integral domain". Also the statement "I is a maximal ideal in R" is absolute, and I is hardly maximal if it is finitely generated. This completes the argument for Ring 1.

RING 2. *An atomless boolean ring R in which all ideals are principal and there are no infinite strictly descending chains of ideals.*

It will be convenient to regard R as a boolean algebra. Sikorski [9] p. 53 describes how to convert from ring notation to algebra notation and *vice versa*; an ideal in the ring sense is just the same as an ideal in the algebra sense. We write $\wedge$, $\vee$, $*$, $<$ for meet, join, complement and lattice ordering in the algebra. By an *atom* of R, we mean a nonzero element x of R such that there is no y in R for which $0 < y < x$. We call R *atomless* if it has no atoms. In an atomless boolean algebra, no principal filter is maximal; hence by duality no principal ideal is maximal.

We shall need the following lemma, which is well known but seems to have escaped the standard references.

LEMMA. *Let R, S be countable atomless boolean algebras, and let $f'\colon R' \to S'$ be an isomorphism from a finite subalgebra R' of R onto a finite subalgebra S' of S. Then f' extends to an isomorphism f between R and S.*

To prove this, let $(r_i)_{i\in\omega}$, $(s_i)_{i\in\omega}$ be enumerations of the elements of R, S respectively. We shall show that there is an increasing sequence $f' = f_0 \subseteq f_1 \subseteq \cdots$ of isomorphisms between finite subalgebras of R and S, such that for each i, $r_i \in \operatorname{dom} f_{i+1}$ and $s_i \in \operatorname{im} f_{i+1}$. Suppose the sequence has been constructed as far as f_i; then $\operatorname{dom} f_i$ is a finite subalgebra of R, say with atoms $a_1, \ldots, a_n$. For each j $(1 \leqslant j \leqslant n)$, we put $r_{ij} = r_i \wedge a_j$. For each j we have either $r_{ij} = a_j$, or $0 < r_{ij} < a_j$, or $r_{ij} = 0$. Since S is atomless, we can find elements s_{ij} which are related in the same way to $f_i(a_j)$, 0. Extend f_i to an isomorphism f_i' whose domain is generated by $\operatorname{dom} f \cup \{r_i\}$, so that $f_i'(r_{ij}) = s_{ij}$ for each j. Construct f_{i+1} from f_i', s_i in the same way. This yields the sequence $(f_i)_{i\in\omega}$ as promised. Put $f = \bigcup_{i\in\omega} f_i$; then $f\colon R \cong S$, proving the lemma.

We shall need three consequences of this lemma.

(1) There is, up to isomorphism, just one countable atomless boolean algebra.

(2) If R is a countable atomless boolean algebra, then every isomorphism between finite subalgebras of R can be extended to an automorphism of R.

(3) (for use in Ring 5 below) Let R be a countable atomless boolean algebra, let $a \in R$, and let f' be an isomorphism between finite subalgebras of R, such that if $b \geqslant a$ and $b \in \operatorname{dom} f'$, then $f'(b) = b$. Then f' extends to an automorphism f of R, such that if $b \geqslant a$ then $f(b) = b$. This is easily proved by choosing the s_{ij} sensibly in the proof of the lemma.

We now construct Ring 2. R shall be a countable atomless boolean algebra; by (1) this describes R uniquely. Let I be an ideal of R in $N(R)$. Then I has a support supp_I, which generates a finite subalgebra of R. Say the atoms of this subalgebra are $a_1, \ldots, a_n$, $b_1, \ldots, b_m$, where $a_1, \ldots, a_n \in I$ and $b_1, \ldots, b_m \notin I$. Put $a = a_1 \vee \cdots \vee a_n$; then $a \in I$ since I is an ideal.

We claim that I is the principal ideal generated by a. For suppose $c \in I$ and $c \nleqslant a$. Then $(b_1 \wedge c) \vee \cdots \vee (b_m \wedge c) > 0$, so some $b_i \wedge c > 0$; then by choice of the b_j's, $0 < b_i \wedge c < b_i$. This implies $0 < b_i \wedge c^* < b_i$. Hence, by (2) above, there is an automorphism s of R which pointwise fixes $a_1, \ldots, a_n$, $b_1, \ldots, b_m$ but transposes $b_i \wedge c$ and $b_i \wedge c^*$. Now $b_i \wedge c \in I$, and s pointwise fixes supp_I, so $b_i \wedge c^* = s(b_i \wedge c) \in I$. Since I is an ideal, I must contain $(b_i \wedge c) \vee (b_i \wedge c^*) = b_i$, which contradicts the definition of $b_1, \ldots, b_m$. This proves the claim. The claim together with Lemma 2 shows that "R is a principal ideal ring" is true in the $N(R)$-interpretation.

To show that "R has no infinite strictly descending chains of ideals" is true in the $N(R)$-interpretation, assume there is in $N(R)$ an infinite strictly descending chain $I = (I_i)_{i \in \omega}$ of ideals of R, and deduce a contradiction as follows. I has a support, which generates a finite subalgebra S of R. By just the same argument as before, each ideal I_i is a principal ideal generated in R by an element of S. Since S is finite, there are only finitely many distinct ideals among the I_i, which is clearly impossible.

This completes the argument for Ring 2. Observe that R has no maximal ideals in $N(R)$. Also the argument (Sikorski [9] p. 17) which shows that in a boolean ring maximal, prime and primary ideals are the same thing needs no more than ZF to prove it. Absoluteness then shows that the statement "R has no prime or primary ideals" is true in the $N(R)$-interpretation.

Ring 3. *An infinite atomic boolean ring R in which*

(a) *every proper ideal is an intersection of maximal ideals,*

(b) *there are no infinite strictly ascending or descending chains of ideals.*

As with Ring 2, we work in boolean algebra notation. We call the boolean algebra R ***atomic*** if for every nonzero element x of R there is an atom y with $y \leqslant x$. We call an element x of the atomic boolean algebra R *finite* if $x \leqslant a_1 \vee \cdots \vee a_n$ for some finite set $a_1, \ldots, a_n$ of atoms of R; we call x *cofinite* if x^* is finite. If R is an atomic boolean algebra and A is the set of atoms of R, then the set of finite or cofinite elements of R forms a subalgebra R' of R, which is determined up to isomorphism by the set A; we call R' the *finite–cofinite algebra* on A. A is the set of atoms of R', and every permutation of A extends to a unique automorphism of R'.

If R is any boolean algebra and b a nonzero element of R, then we form the boolean algebra $R \mid b$ as follows. (Sikorski [9] p. 30.) The elements of $R \mid b$ are the $x \in R$ such that $x \leqslant b$. If x, y are in $R \mid b$, then x, y have the same meet and join in $R \mid b$ as they had in R; the complement of x in $R \mid b$ is $x^* \wedge b$, where x^* is the complement of x in R. If I is an ideal of R, then $I \mid b = I \cap R \mid b$ is an ideal of $R \mid b$.

R shall now be the finite–cofinite algebra on a countable set A. R is itself countable, and the statement that R is an infinite atomic boolean algebra is absolute.

Let I be an ideal of R in $N(R)$. Then I has a support supp_I. There is some non empty finite set $B \subseteq A$ such that supp_I is a subset of the subalgebra generated by B in R. If $B = \{b_1, \ldots, b_n\}$, put $b = b_1 \vee \cdots \vee b_n$.

We claim that $I \mid b^*$ is either $R \mid b^*$, or the zero ideal $\{0\}$, or the ideal of all finite elements of $R \mid b^*$. For suppose $I \mid b^*$ is not the zero ideal; then it contains some $x \in A - B$. Note that $x \in I$. If y is any element of $A - B$, then there is an automorphism of R which transposes x and y, but pointwise fixes B. Since s thereby pointwise fixes supp_I, we deduce that y is also in I, so $y \in I \mid b^*$. Hence if $I \mid b^*$ is a nonzero ideal, then $I \mid b^*$ must contain all finite elements of $R \mid b^*$. If it contains anything else besides, then it must contain a cofinite element of R, so that $b^* \in I \mid b^*$ and $I \mid b^* = R \mid b^*$. The claim is proved.

We can now show that I is an intersection of maximal ideals in $N(R)$, assuming that I is a proper ideal. By the claim, there are three cases to consider. Suppose first that $I \mid b^*$ is $R \mid b^*$. Then $b^* \in I$, so I is principal, generated say by an element c; I is therefore the intersection of the principal ideals generated by elements x^* where x is an atom and $x \not\leqslant c$. But a principal ideal of R must be in $N(R)$, because it is definable absolutely from an element of R. The same argument works in the second case, viz., where $I \mid b^*$ is the zero ideal. There remains the third case, where $I \mid b^*$ is the ideal of finite sets in $R \mid b^*$. Let J be the ideal of all finite elements of R; the explicit definition of J from the structure of R puts J in $N(R)$. Also J is maximal in R. Let $a_1, \ldots, a_m$ be the atoms of R which are not in I; there are finitely many, because they form a subset of B. For each i, let J_i be the principal ideal generated by a_i^*. Then certainly $I \subseteq J \cap J_1 \cap \cdots \cap J_m$. If $x \in (J \cap J_1 \cap \cdots \cap J_m) - I$, then x must be the join of a finite (since $x \in J$) number of atoms which are in I (since $x \in J_1 \cap \cdots \cap J_m$); this is impossible since I is an ideal. We deduce that $I = J \cap J_1 \cap \cdots \cap J_m$, which concludes the proof of (a).

Suppose next that there is in $N(R)$ an infinite strictly ascending chain $(I_i)_{i \in \omega}$ of ideals of R. There is then a finite set $B \subseteq A$ which generates a subalgebra of R containing a support of the sequence $(I_i)_i$. Define $b \in R$ from the set B as before. The same argument as before shows that each $I_i \mid b^*$ must be either $R \mid b^*$ or the zero ideal or the ideal of finite elements in $R \mid b^*$. Hence the chain $(I_i \mid b^*)_i$ becomes stationary rather soon, say at $i_0 \leqslant 2$. The ideals I_j with $j \geqslant i_0$ can differ only by containing different elements of B, which is finite. This is absurd, since $(I_i)_i$ was assumed to be strictly ascending. We have shown that $N(R)$ contains no infinite strictly ascending chain of ideals. If we repeat this last argument standing on our heads, we shall have shown the same for descending chains. This concludes the argument for Ring 3.

Observe that the ideal of finite elements of R is not finitely generated, and that this is an absolute statement about R.

RING 4. *A quasilocal commutative ring R such that*

(a) *every nonempty set of ideals of R has a minimal element*;

(b) *there is an infinite strictly ascending chain of ideals of R.* (NB: *All our rings have a* 1.)

We take F to be the prime field of characteristic 2, and $(X_i)_{i\in\omega}$ to be a sequence of distinct indeterminates. In the polynomial ring $F[X_i]_i$ we take H to be the ideal generated by all monomials of degree 2; we write Y_i for the element $X_i + H$. Thus $F[Y_i]_i = F[X_i]_i/H$. For each k we take J_k to be the ideal of $F[Y_i]_i$ generated by $Y_0, ..., Y_{k-1}$.

R shall be the ring $F[Y_i]_i$ with the J_k as distinguished subsets.

Each nonzero element x of R is of the form $\sum_j a_j$, where the a_j are pairwise distinct and each a_j is either 1 or some Y_i; this representation of x is unique up to permutation of the terms. x is representable as $\sum_j a_j$, where the a_j are distinct Y_i's, if and only if x is in the ideal $\bigcup_k J_k$. Direct calculation reveals the following:

(i) If $x, y \in \bigcup_k J_k$, then $xy = 0$.

(ii) If $x \in \bigcup_k J_k$ and $y \notin \bigcup_k J_k$, then $xy = x$.

(iii) If $x, y \notin \bigcup_k J_k$, then $xy \notin \bigcup_k J_k$ and $x^2 = 1$.

(iii) shows that $\bigcup_k J_k$ must be the sole maximal ideal of R, so that R is quasilocal. The statements expressed by these calculations are absolute, so it holds also in the $N(R)$-interpretation that R is quasilocal with maximal ideal $\bigcup_k J_k$.

The sequence $(J_k)_{k\in\omega}$ is in $N(R)$, so that $N(R)$ contains an infinite strictly ascending chain of ideals of R.

Now let I be any ideal of R which is in $N(R)$. I has a support supp_I; let i be the least nonnegative integer such that $\text{supp}_I \subseteq F[Y_j]_{j<i}$.

We claim that if for some $k \geqslant i$, I contains an element of

$$F[Y_j]_{j\leqslant k} - F[Y_j]_{j<k},$$

then $J_k \subseteq I$. The proof is as follows. Suppose $x \in F[Y_j]_{j\leqslant k} - F[Y_j]_{j<k}$, and suppose $y \in J_k$. Then there is a unique automorphism s of R such that

$$s(Y_j) = \begin{cases} Y_k + y & \text{if } j = k \\ Y_j & \text{if } j \neq k. \end{cases}$$

Since $i \leqslant k$, s pointwise fixes supp_I, and so we infer that $sx \in I$. But I is an ideal, so I contains $sx - x = y$. This proves the claim.

By the claim, I must take up one of the following stances. (1) For all k, $I \not\subseteq F[Y_j]_{j<k}$. Then the claim shows I is either the maximal ideal $\bigcup_k J_k$ or the whole ring. (2) There is some least k such that $I \subseteq F[Y_j]_{j\leqslant k}$, and $k \geqslant i$. Then I contains no invertible elements, and by the claim $J_k \subseteq I$. I must therefore be J_{k+1}. (3) $I \subseteq F[Y_j]_{j<i}$. This allows finitely many possibilities.

Now let A be a nonempty set in $N(R)$, whose members are ideals of R. Since $N(R)$ is a transitive model of ZF, each of these ideals is also in $N(R)$.

We shall show that A has a minimal element which is an absolute statement about A. Suppose A has no minimal element. Then by the usual argument (which needs Choice; see Theorem 1 below) there is an infinite strictly descending chain $(I_j)_{j\in\omega}$ of ideals in A. (Since this argument needs Choice, we are asserting only that the sequence $(I_j)_j$ exists, and *not* that it is in $N(R)$.) Each I_j is in $N(R)$, so it must come under one of conditions (1)–(3) for some i. No I_j comes under condition (2) or (3) for any i, because an ideal $\subseteq F[Y_j]_{j<i}$ has only finitely many subideals. Hence each I_j must be either $\bigcup_k J_k$ or the whole ring; which is absurd.

This completes the argument for Ring 4.

RING 5. *A quasilocal commutative ring R with a maximal ideal J such that*

(a) *R has no infinite strictly ascending or descending chains of ideals*;

(b) *J is nil and idempotent*;

(c) *J is not finitely generated*;

(d) *J is the only prime ideal of R.*

For this we shall need sequences. We write $2^{<\omega}$ for the set of all finite sequences of 0's and 1's; this includes the empty sequence $\langle\ \rangle$. If σ, ρ are sequences, we write $\sigma\rho$ for the sequence consisting of σ followed by ρ.

Let F be the prime field of characteristic 2. Take a sequence $(t_\rho)_\rho$ of indeterminates, where ρ ranges over $2^{<\omega} \cup \{\omega\}$, and let K be the pure transcendental extension $F(t_\rho)_\rho$ of F. For each $\sigma \in 2^{<\omega}$ we define an element T_σ of K, by induction on the length of σ:

$$T_{\langle\rangle} = t_\omega ;$$

$$T_{\sigma 0} = t_\sigma ;$$

$$T_{\sigma 1} = T_\sigma \cdot t_\sigma^{-1}.$$

For each nonnegative integer i we define $R_i' = F[T_\sigma]_{\sigma \text{ of length } i}$. Since $T_\sigma = T_{\sigma 0} \cdot T_{\sigma 1}$, we see that $i \leqslant j$ implies $R_i' \subseteq R_j'$. Forming the union of this chain, we define $R' = \bigcup_{i\in\omega} R_i'$. We write H for the ideal of R' generated by the elements T_σ^2 with $\sigma \in 2^{<\omega}$, and we write S_σ for $T_\sigma + H$ in R'/H. By the Second Isomorphism Theorem we can identify $R_i'/(H \cap R_i')$ with $(R_i' + H)/H = F[S_\sigma]_{\sigma \text{ of length } i}$; R'/H is identical with $F[S_\sigma]_\sigma$.

R shall be the ring $R'/H = F[S_\sigma]_\sigma$. We write J for the ideal generated by the S_σ; there is no need to add J to R as a distinguished subset, because it will soon appear that J is explicitly and absolutely definable from the ring structure of R. We also write R_i for $R_i'/(H \cap R_i')$.

We begin our analysis by studying the rings R_i. The elements T_σ with σ of length i are algebraically independent in K, so that R_i' is in effect a polynomial ring over F with the T_σ (σ of length i) as indeterminates. The ideal $H \cap R_i'$ is generated by the elements T_σ^2 with σ of length i. Hence every nonzero element of R_i is representable uniquely (up to permutations) as a sum of terms each of which is a product of distinct elements S_σ with σ of length i; we count 1 as the empty product.

Let us call a nonzero element x of R *homogeneous* if x can be written as a product $S_{\sigma_1} \cdots S_{\sigma_n}$. Write B for the set of homogeneous elements of R, and B_i for the set of homogeneous elements in R_i. If $x \in B_i$, then x can be written uniquely (up to permutation of factors) as $S_{\sigma_1} \cdots S_{\sigma_n}$ with the σ_j all of length i. The last sentence of the previous paragraph therefore says that every nonzero element of R_i can be uniquely represented as a sum of elements of B_i.

Let x, y be elements of B; we write $x \leqslant y$ to mean that x divides y in R. If x, y are elements of B_i, then x, y can be written as products

$$x = \prod_{\sigma \in X} S_\sigma, \qquad y = \prod_{\sigma \in Y} S_\sigma, \tag{1}$$

where X, Y are sets of sequences σ with σ of length i. x divides y in R_i if and only if $X \subseteq Y$. Tracing this up through the R_j with $j \geqslant i$, we see that $x \leqslant y$ if and only if $X \subseteq Y$. Therefore $\leqslant$ defines on each B_i the structure of a boolean algebra, viz., the power set algebra of the set of sequences of length i. The top element of each B_i is $S_{\langle\,\rangle}$, which is the product of all the S_σ with σ of length i. The bottom element of each B_i is 1, which divides everything. The union of a chain of boolean algebras is again a boolean algebra, with the same top and bottom elements as in the chain. Thus B forms a boolean algebra with $\leqslant$ as lattice ordering, and top and bottom elements $S_{\langle\,\rangle}$ and 1 respectively.

If x, y are in B_i, then we have, using the notation of formula (1) above,

$$x \vee y = \prod_{\sigma \in X \cup Y} S_\sigma,$$

$$x \wedge y = \prod_{\sigma \in X \cap Y} S_\sigma,$$

$$x^* = \prod_{\sigma \text{ of length } i, \sigma \notin X} S_\sigma .$$

Note that if $x \wedge y = 1$, then $xy = x \vee y$; if $x \wedge y > 1$, then $xy = 0$. If $1 \neq x \in B_i$, then some element of B_{i+1} is a proper divisor of x; for example $S_{\sigma 0}$ is a proper divisor of S_σ. This implies that B is atomless. Clearly B is countable; so B is a countable atomless boolean algebra. We recall (cf., Ring 2) that in any such algebra, an isomorphism of finite subalgebras can always be extended to an automorphism of the whole algebra.

We claim that every automorphism of B extends to a unique automorphism of the ring R. For let s be an automorphism of B. Since each nonzero element x of R is uniquely a sum $\sum_j a_j$ of elements of B, we can define a permutation s of R extending s on B by setting $s(x) = \sum_j s(a_j)$, $s(0) = 0$. This permutation s of R is the only possible candidate for an automorphism extending s on B. Moreover it is an automorphism. It clearly preserves $+$; to check that it preserves $\cdot$, we need only look at nonzero elements. Say $x = \sum_j a_j$ and $y = \sum_k b_k$, where the a_j and b_k are homogeneous. Then $xy = \sum_{j,k} a_j b_k$. Now if $a_j \wedge b_k > 1$, then $a_j b_k = 0$; if $a_j \wedge b_k = 1$, then also $sa_j \wedge sb_k = 1$, so that $s(a_j b_k) = s(a_j \vee b_k) = sa_j \vee sb_k = (sa_j)(sb_k)$. Hence we have

$$xy = \sum_{a_j \wedge b_k = 1} a_j b_k,$$

and

$$\begin{aligned} s(xy) &= s\Big(\sum_{a_j \wedge b_k = 1} a_j b_k\Big) = \sum_{sa_j \wedge sb_k = 1} (sa_j)(sb_k) \\ &= (sx)(sy). \end{aligned}$$

This proves the claim.

If $x = \sum_j a_j$, where the a_j are distinct homogeneous elements, then by the characteristic we have $x^2 = \sum_j a_j^2$. If one of the a_j is 1, then $x^2 = 1$; otherwise $x^2 = 0$. Now $x \notin J$ precisely if one of the a_j is 1; it follows that J consists precisely of the noninvertible elements of R. This guarantees firstly that R is quasilocal with maximal ideal J; second, it yields an absolute description of J as a subset of R, and this entails that J is in $N(R)$. Thus by Lemma 2 the statement "R is a quasilocal ring with maximal ideal J" is true in the $N(R)$-interpretation.

J is nil. For say $x \in J$; then we have just seen that $x^2 = 0$. Also J is idempotent; to show this it suffices to prove that each $S_\sigma \in J^2$. But $S_\sigma = S_{\sigma 0} \cdot S_{\sigma 1} \in J^2$.

J is the only prime ideal of R in V, hence the only prime ideal of R in $N(R)$. For any prime ideal contains $0 = S_\sigma^2$, hence also S_σ, for each sequence σ.

Finally we consider chains of ideals. Suppose $(I_j)_{j\in\omega}$ is an ascending or descending chain of proper ideals of R, and $(I_j)_j$ is in $N(R)$. Then $(I_j)_j$ has a support; we now fix i to be the least positive integer such that this support lies in R_i. Write W for the set of all proper ideals of R in $N(R)$ which have supports $\subseteq R_i$. Then each $I_j \in W$. We shall show that if I_0, I_1 are distinct ideals in W, then they have distinct contractions $I_0 \cap R_{i+1}, I_1 \cap R_{i+1}$ in the ring R_{i+1}. Since R_{i+1} is finite, this will show that W is finite, and hence the chain $(I_j)_j$ is eventually constant.

By a *partition* of B, we mean a finite set $E = \{e_1, ..., e_n\}$ of elements $\neq 1$ in B, such that $e_i \wedge e_j = 1$ for each $i \neq j$, and $e_1 \vee \cdots \vee e_n = S_{\langle\,\rangle}$. If $F = \{f_1, ..., f_m\}$ is another partition of B, we shall say that F *refines* E if for each f_j there is some e_k such that $f_j \leqslant e_k$. We define

$$E_i = \{S_\sigma : \sigma \text{ has length } i\}.$$

E_i forms a partition; if F refines E_i, then any automorphism of B which pointwise fixes F must also pointwise fix E_i and so R_i.

Suppose $b \in B$ and $x \in R$. We shall say that b *nails* x if x is a sum (possibly 0) of terms $a_j \in B$ such that each a_j is either $\geqslant b$ or $\leqslant b^*$. The point of this definition is that if b nails x, then every automorphism of B which pointwise fixes every $a \geqslant b$ will also fix x.

LEMMA. *Let $I \in W$. Let $F = \{f_0, ..., f_k\}$ be a partition of B refining E_i, with $f_0 \vee f_1 \leqslant e$ for some $e \in E_i$. Let $x = af_0 + bf_1 + c$, where $f_0 \vee f_1$ nails each of a, b, c, and suppose $x \in I$. Then $af_0 \in I$.*

We begin the proof of the lemma by refining the partition F to replace f_0 by the two elements f_{00}, f_{01}, and f_1 by the two elements f_{10}, f_{11}, where $f_{00} \vee f_{01} = f_0$ and $f_{10} \vee f_{11} = f_1$. We have by assumption

$$af_0 + bf_1 + c \in I. \tag{2}$$

By consequence (3) of the Lemma of Ring 2, there is an automorphism of B which takes f_0 to f_{00}, f_1 to $f_{01} \vee f_1 = f_{01} \cdot f_1$, and which pointwise fixes everything $\geqslant f_0 \vee f_1$. Applying this automorphism to (2), we derive

$$af_{00} + bf_{01}f_1 + c \in I. \tag{3}$$

Similarly

$$af_{01} + bf_{00}f_1 + c \in I. \tag{4}$$

Then by adding (3) to (4) and remembering the characteristic,

$$(a + bf_1)(f_{00} + f_{01}) \in I. \tag{5}$$

Multiplying (5) by f_{01},

$$(a + bf_1) f_{00}f_{01} = (a + bf_1) f_0 = af_0 + b(f_0 \vee f_1) \in I. \tag{6}$$

Much as above, we can find an automorphism of B which transposes f_0 and f_1, and pointwise fixes everything $\geqslant f_0 \vee f_1$. Applying this automorphism to (6),

$$af_1 + b(f_0 \vee f_1) \in I. \tag{7}$$

Adding (6) to (7) and again invoking the characteristic,

$$af_0 + af_1 \in I. \tag{8}$$

Repeating the move that took (2) to (3), we get from (8)

$$af_{00} + af_{01}f_1 \in I. \tag{9}$$

Multiplying (9) by f_{01}, we have at last

$$af_{00}f_{01} = af_0 \in I. \tag{10}$$

The lemma is proved.

Now let I_0, I_1 be two distinct ideals $\in W$. Since the ideals are distinct, there is (renumbering if necessary) an element $x \in I_0 - I_1$. We fix this element x; the rest of the argument must show that there is an element $y \in (I_0 - I_1) \cap R_{i+1}$. Each element of R is a sum of homogeneous elements; we suppose we have chosen x in $I_0 - I_1$ to be a sum of as few as possible distinct homogeneous elements. Let F be a partition of B such that each homogeneous term of x lies in the subalgebra generated by F, and such that F refines E_i; choose F as small as possible with these properties.

Suppose that F contains distinct elements f_0, f_1 such that $f_0 \vee f_1 \leqslant e$ for some $e \in E_i$. Gathering the terms of x into three groups, we can write $x = af_0 + bf_1 + c$, where $f_0 \vee f_1$ nails each of a, b, c. By the lemma, both af_0 and bf_1 are in I_0, hence so is c. If $af_0 \notin I_1$, then by choice of x, af_0 must have as many homogeneous terms as x, hence $x = af_0$. Likewise if $bf_1 \notin I_1$, then $x = bf_1$, and so with c. But at least one of the three terms af_0, bf_1, c is not in I_1 since $x \notin I_1$. Hence x is either af_0 or bf_1 or c; but c is here impossible, because it would imply we could have replaced F by the smaller partition with $f_0 \vee f_1$ in place of f_0, f_1.

Let e now be some element of E_i, and suppose F refines e to $f_0, \ldots, f_n$ (i.e., $e = f_0 \vee \cdots \vee f_n$ with $f_0, \ldots, f_n \in F$), with $n \geqslant 1$. The previous paragraph shows that x is of form af_0 or bf_1, where $f_0 \vee f_1$ nails a, b; the minimality of F therefore requires $n = 1$. In short, if $e \in E_i$, then either $e \in F$, or F refines e to the two elements f_0, f_1 with $f_0 \vee f_1 = e$.

Now we can make our final thrust. There is an automorphism s of B which pointwise fixes E_i, and such that if F refines $S_\sigma \in E_i$ to f_0, f_1, then $s(f_0) = S_{\sigma 0}$ and $s(f_1) = S_{\sigma 1}$. This automorphism extends uniquely to an automorphism s of R, and $s(x) \in R_{i+1}$. But s pointwise fixes E_i, so $s(x) \in I_0 - I_1$. Hence $(I_0 \cap R_{i+1}) - (I_1 \cap R_{i+1})$ is not empty. This concludes the argument.

RING 6. *An integral domain R in which there is a nonzero element x such that the principal ideal xR has a prime overideal but no minimal prime overideal.*

We begin by taking F, K just as in the construction of Ring 5, and defining T_σ for each $\sigma \in 2^{<\omega}$ as with Ring 5. We write L for the set of all T_σ with $\sigma \in 2^{<\omega}$.

R shall be the ring $F[T_\sigma]_\sigma$ with L as distinguished subset. R is an integral domain since it is a subring of the field K. Hence the statement "R is an integral domain" is true in the $N(R)$-interpretation, since this statement is absolute.

Let $\sigma, \rho \in 2^{<\omega}$; we shall write $\sigma \subseteq \rho$ to mean that for some $\tau \in 2^{<\omega}$, $\rho = \sigma\tau$. We write J_σ for the ideal of R generated by all T_τ with $\sigma \subseteq \tau$. Since T_τ divides T_σ if and only if $\sigma \subseteq \tau$, we can define J_σ absolutely in terms of L, σ and the ring structure of R; hence J_σ is in $N(R)$. For each nonnegative integer i, we define R_i to be the subring $F[T_\tau]_{\tau \text{ of length } i}$ of R. Assuming that σ has length $\leqslant i$, $J_\sigma \cap R_i$ is the ideal of R_i generated by the T_τ with τ of length i and $\sigma \subseteq \tau$. Now the T_τ with τ of length i are algebraically independent, which implies that $J_\sigma \cap R_i$ is a prime ideal of R_i. But $R = \bigcup_i R_i$, from which it follows that J_σ itself is a prime ideal of R. Note that $L = J_{\langle\,\rangle}$, so that L is a prime ideal of R.

Now consider the element $T_{\langle\,\rangle}$. This is a nonzero element contained in the prime ideal L, so the principal ideal $T_{\langle\,\rangle}R$ has L as prime overideal. We must show that there is in $N(R)$ no minimal prime ideal containing T.

Let I be a prime ideal of R in $N(R)$, such that $T_{\langle\,\rangle} \in I$. Since I is in $N(R)$, it has a support supp_I; we define i to be the least nonnegative integer such that $\text{supp}_I \subseteq R_i$. Now $T_{\langle\,\rangle}$ is the product of the T_σ with σ of length i, and I is prime. Hence there is some σ of length i such that $T_\sigma \in I$. Fix such a σ.

We claim that $J_\sigma \subseteq I$. For suppose $J_\sigma \not\subseteq I$, and let τ be of minimal length such that $\sigma \subseteq \tau$ and $T_\tau \notin I$. τ is then a proper extension of σ, so we may suppose $\tau = \mu 0$ with $\sigma \subseteq \mu$. (The argument for $\tau = \mu 1$ is just the same.) By minimality of τ, we have $T_\mu \in I$. Since I is prime and $T_\mu = T_{\mu 0} \cdot T_{\mu 1} = T_\tau \cdot T_{\mu 1}$, we infer that $T_{\mu 1} \in I$. Now take s to be the unique automorphism of R such that for each ρ,

$$s(T_\rho) = \begin{cases} T_\rho & \text{if } \mu \not\subseteq \rho \text{ or } \mu = \rho \\ T_{\mu 1 \pi} & \text{if } \rho = \mu 0 \pi \\ T_{\mu 0 \pi} & \text{if } \rho = \mu 1 \pi. \end{cases}$$

Since $\sigma \subseteq \mu$, s pointwise fixes R_i. Hence $T_{\mu 1} \in I$ implies $s(T_{\mu 1}) = T_{\mu 0} = T_\tau \in I$. This contradicts the choice of τ, and thus proves the claim.

Now $J_{\sigma 0} \subset J_\sigma \subseteq I$, and $J_{\sigma 0}$ is a prime ideal of R in $N(R)$ containing $T_{\langle\,\rangle}$. It follows that I is not a minimal prime ideal containing $T_{\langle\,\rangle}$ in $N(R)$; which concludes our argument.

Ring 6 will not be appearing again in this note. Therefore we grasp this opportunity to point out that Zorn would have guaranteed a maximal chain of prime ideals of R containing the nonzero element x, and the intersection of this chain would then have been a minimal prime overideal of xR. (cf., Kaplansky [7] p. 6.)

3. Analysis

3.1. *Finiteness Conditions*

Let R be a commutative ring; we repeat the blanket assumption that R has a multiplicative identity 1. There are six "classical" finiteness conditions we can impose on R, namely the following.

A_1 : R has a composition series of ideals.

A_2 : (Minimum condition) Every nonempty set of ideals of R has a minimal member.

A_3 : (Descending chain condition) Every strictly descending chain of ideals of R is finite.

N_1 : (Maximum condition) Every nonempty set of ideals of R has a maximal member.

N_2 : (Finite basis condition) Every ideal of R is finitely generated.

N_3 : (Ascending chain condition) Every strictly ascending chain of ideals of R is finite.

(A stands for Artin and N for Noether, naturally.) In the presence of Zorn's Lemma the following implications hold between these conditions:

$$\begin{array}{ccc} A_1 & \Rightarrow & N_1 \\ \Updownarrow & & \Updownarrow \\ A_2 & & N_2 \\ \Updownarrow & & \Updownarrow \\ A_3 & & N_3 \end{array}$$

(cf., Zariski and Samuel [10] pp. 156, 161, 199, 203.) If we remove the proofs in which honest folk mention Zorn, the following arrows remain:

$$\begin{array}{ccc} A_1 & \Rightarrow & N_1 \\ \Downarrow & & \Downarrow \\ A_2 & & N_2 \\ \Downarrow & & \Downarrow \\ A_3 & & N_3 \end{array}$$

Theorem 1. *The arrows above describe all the implications between pairs of the properties A_1–N_3 which can be proved from* ZF *alone.*

Proof. Before we descend to details, we need to explain why a certain argument (used e.g., by Zariski and Samuel [10] p. 156) is less than valid. To prove N_1 from N_3 by ZF alone, we might be tempted to argue:

Suppose R is a ring in which N_1 fails but N_3 holds. Since N_1 fails, there is a nonempty set C of ideals of R which has no maximal member. Let $I_0 \in C$; then since I_0 is not maximal in C, there is some $I_1 \in C$ with $I_0 \subset I_1$. Likewise since I_1 is not maximal in C, there is some $I_2 \in C$ with $I_1 \subset I_2$; etc. But since N_3 holds, "this process must stop, and thus a maximal element of C is reached."

The trouble is that N_3 says nothing at all about this process stopping; indeed N_3 by itself puts no restrictions at all on *finite* strictly ascending sequence of ideals. N_3 merely says there is no *infinite* strictly ascending sequence of ideals. To bring N_3 into play, we have to show that successive extensions $I_0 \subset I_1 \subset \cdots$ can be strung together to form a single infinite chain. In general this involves choosing I_{i+1} from among infinitely many proper extensions of I_i in C, for each nonnegative integer i; this must surely need some kind of Choice principle.

A convenient Choice principle to use would be the Axiom of Dependent Choice, DC for short. This says: if A is a nonempty set, and S is a binary relation defined on A such that for each $a \in A$ there is a $b \in A$ with aSb, then there is an infinite sequence $(a_i)_{i\in\omega}$ of elements of A such that for each i, $a_i S a_{i+1}$. This axiom is due to P. Bernays ([1], p. 86); Zorn's Lemma implies it, but it does not imply Zorn (cf., Felgner [4], p. 146ff.). Putting $\subset$ for S, DC derives N_1 from N_3; putting $\supset$ for S, it derives A_1 from A_3.

We turn to proving the positive part of the theorem. Suppose first that A_1 holds of the commutative ring R, so that R has a composition series X. If either A_2 or N_1 fails, then by the valid part of the argument we castigated above, we can find a strictly ascending chain Y of ideals of R which is finite but longer than X. (Since Y is finite, we avoid Zorn.) By ZF alone we can prove as usual that X and Y have a common refinement, which must have more terms than X. Hence X cannot be a composition series for R. Thus ZF derives A_2 and N_1 from A_1.

A_3 follows at once from A_2, since if $(I_i)_{i\in\omega}$ is an infinite strictly descending chain of ideals of R, then the set $\{I_i : i \in \omega\}$ is nonempty but has no minimal element.

To deduce N_2 from N_1, assume N_1 holds, and suppose that R has an ideal I which is not finitely generated. Let C be the set of all finitely generated ideals contained in I. By N_1, C has a maximal element J, which is evidently a proper subideal of I. If $x \in I - J$, then $J + xR$ is a proper extension of J in C, which is a contradiction. (Again we chose only one element x, so no Choice principle is involved.)

To deduce N_3 from N_2, assume N_2 holds, and let $(I_i)_{i\in\omega}$ be an infinite ascending chain of ideals of R. ZF alone implies that $J = \bigcup_{i\in\omega} I_i$ is also an ideal of R, and N_2 requires J to be finitely generated. The finitely many generators must already occur together in some I_i, so that the chain is stationary from I_i onwards.

This completes the positive part of the proof.

Examples to show $N_1 \not\Rightarrow A_3$ are well known. Ring 4 shows $A_2 \not\Rightarrow N_3$. Ring 2 shows $A_3 \not\Rightarrow A_2$, since in an atomless boolean algebra the set of nonzero ideals has no minimal elements. Ring 1 shows $N_2 \not\Rightarrow N_1$. Finally Ring 5 shows $N_3 \not\Rightarrow N_2$. This completes the proof of the theorem. □

If we ask what implications hold between three or more of the finiteness conditions by ZF alone, then there are some open questions. Ring 2 shows that A_3 and N_2 together do not imply A_1 by ZF alone. On the other hand we have

THEOREM 2. ZF *entails that conditions* A_2 *and* N_1 *together on a ring* R *imply* A_1 *on* R.

Proof. Assume conditions A_2 and N_1 on R. Call a finite chain of proper ideals of R

$$\cdots \subset I_i \subset I_{i+1} \subset I_{i+2} \subset \cdots$$

tight if no ideal can be fitted properly between any two successive ideals of the chain. Let T be the set of tight chains of R. T is certainly nonempty since a single ideal forms a tight chain. Let T_m be the set of maximal elements of chains in T. Since T_m is nonempty, it has by N_1 a maximal element J. We claim J is a maximal ideal of R; for otherwise the set of proper ideals properly extending J is nonempty and so has a minimal element J' by A_2. Taking a tight chain with maximal element J, we would get a longer tight chain by adding J' at the top; this would contradict the maximality of J in T_m. Now let S be the set of all tight chains which have J as maximal element, and S_m the set of all minimal elements of chains in S. The arguments above will stand on their heads to show that S_m contains a minimal element K which is a minimal ideal of R. Hence we have a tight chain running from a minimal ideal of R to a maximal ideal of R. Such a chain yields a composition series. □

We do not know whether A_3 and N_1 together give A_1 by ZF, or whether A_2 and N_2 together give A_1.

A seventh finiteness condition which sometimes appears alongside the other six is the condition

C_1: Every prime ideal of R is finitely generated.

(C is for Irving Cohen.) Granting Zorn, C_1 is equivalent to N_1–N_3 (cf., Kaplansky [7], p. 5); N_2 trivially implies C_1 by ZF alone. In Ring 2 there are no prime ideals at all, and the set of proper ideals has no maximal elements; this proves that C_1 does not entail N_1 by ZF alone. We can use an old set theoretic independence result to strengthen this:

THEOREM 3. ZF + DC *does not entail that* C_1 *on a commutative ring* R *implies* N_3 *on* R.

Proof. In 1965 Feferman gave a model of ZF in which the power set algebra of ω has the property that every prime ideal is principal; Solovay later showed that DC is true in this model. (cf., Felgner [4], p. 160ff.). The ideal of finite subsets of ω is not finitely generated, so that this boolean ring violates N_2. But in the presence of DC, N_3 implies N_1 and hence N_2; so N_3 must also fail for this ring. □

3.2. *Noetherian Conditions*

The theory of commutative rings satisfying N_1 is largely independent of Zorn's Lemma. There are two main reasons for this. The first is that the chief use of Zorn in ring theory is to find ideals maximal with certain properties, and N_1 does this job even better than Zorn. For example, the whole theory of primary decomposition of ideals in commutative rings with condition N_1 survives intact without Zorn.

The second reason why N_1 works well without Zorn is that N_1 is preserved by the usual operations which (given Zorn) preserve Noetherianity. For example, take polynomial rings.

THEOREM 4 (Hilbert's Basis Theorem for N_1). *Let* R *be a commutative ring for which* N_1 *holds, and let* $R[X]$ *be the ring of polynomials over* R *in an indeterminate* X. *Then* ZF *entails that* N_1 *holds for* $R[X]$.

Proof. Let A be a nonempty set of ideals of $R[X]$; we must show that A has a maximal element. For each ideal $I \in A$ and each nonnegative integer n, write $I_{(n)}$ for the set of elements of R which are either 0 or the leading coefficients of polynomials $\in I$ with degree n. Then $I_{(n)}$ is an ideal of R. The set $B = \{I_{(n)} : I \in A \text{ and } n \geqslant 0\}$ is a nonempty set of ideals of R; so by N_1 for R, B has a maximal element, say $J_{(m)}$. Let C_0 be the set of ideals $I \in A$ such that $I_{(m)} = J_{(m)}$. We define nonempty sets $C_0 \supseteq C_1 \supseteq \cdots \supseteq C_m$ by induction as follows. Assuming C_i is defined and $<m$, pick some ideal $K \in C_i$ so that $K_{(i)}$ is maximal; this is possible by N_1 for R. Then take C_{i+1} to be the set of ideals $I \in C_i$ such that $I_{(i)} = K_{(i)}$. (No Choice principle is needed, because m is finite.)

C_m is thus a nonempty set of ideals of $R[X]$. Pick an ideal $I \in C_m$; we claim that I is maximal in the set A. Certainly $I \in A$, since $C_m \subseteq C_0 \subseteq A$. Suppose

$K \in A$ and $I \subset K$; then there is some polynomial F of least degree, say n, in $K - I$. Since $I \subset K$, we certainly have $I_{(j)} \subseteq K_{(j)}$ for each $j \geqslant 0$; this implies that $K \in C_i$ for each $i \leqslant m$, so that $I_{(j)} = K_{(j)}$ for each $j \geqslant 0$. In particular $I_{(n)} = K_{(n)}$, so that I contains some polynomial G of degree n with the same leading coefficient as F. Since $I \subseteq K$, the ideal K contains G and so also $F - G$. But $F - G$ is not in I, and $F - G$ has lower degree than F. This contradicts the choice of F, and so completes the proof. □

One can also show, by more or less the usual proof, that if R is a commutative ring with an ideal I, then N_1 holds in R iff N_1 holds in R/I and every nonempty set of ideals of R contained in I has a maximal element.

The facts above provide everything one needs to eliminate Zorn's lemma from the proof of the Hilbert Nullstellensatz which goes by Hilbert rings. (See for example Kaplansky [7], p. 19.) This is one way to get a proof of Hilbert's theorem which is both elementary and pleasant.

We turn to N_2 and N_3. Both these conditions preserve well under the usual operations. For example, we have Hilbert's Basis Theorem for N_2 and N_3 by ZF alone. Zariski and Samuel generously prove the Basis Theorem twice ([10], p. 201); their first proof works for N_3 and their second works for N_2.

Some small parts of the structure theory for commutative Noetherian rings can be nudged through for N_2. One example is Krull's Intersection Theorem. The following proof comes from one by Herstein (Kaplansky [7] p. 50) by rearranging to eliminate one use of N_1.

THEOREM 5 (Krull's Intersection Theorem for N_2). *Let R be a commutative ring for which N_2 holds, let I be an ideal in R, let M be a finitely generated R-module, and $N = \bigcap_n MI^n$. Then* ZF *entails $NI = N$.*

Proof. We note first that ZF suffices for the usual proof that the ascending chain condition holds for submodules of the finitely generated R-module M. Now take $x \in I$; we claim that for some m, $Mx^m \cap N \subseteq NI$. For by the ascending chain condition in M, some m makes $(NI : x^m)$ maximal. Fixing this m, suppose $y \in M$ and $yx^m \in N$. Then $yx^{m+1} \in Nx \subseteq NI$, so $y \in (NI : x^{m+1}) = (NI : x^m)$. Hence $yx^m \in NI$, as we claimed. Now by N_2, I is finitely generated. Hence there is some m such that $MI^m \cap N \subseteq NI$. But then $NI \subseteq N = MI^m \cap N \subseteq NI$, proving the theorem. □

We do not know whether ZF entails the Intersection Theorem for rings with just N_3, but it seems plausible.

In other ways rings satisfying N_2 or N_3 may be very badly behaved. Here follows a catalogue of misfortunes.

THEOREM 6. *Consider the following statements about a commutative ring* R:

(a) *Every ideal of* R *is an intersection of primary ideals.*

(b) *Every nil ideal of* R *is nilpotent.*

(c) *Every minimal prime ideal of* R *is the annihilator of some nonzero element of* R.

Then none of (a)–(c) *follows by* ZF *from assumption* N_3 *on* R; (a) *does not follow by* ZF *from assumption* N_2 *on* R.

Proof. Ring 2 is a ring for which N_2 holds but (a) fails; for in a boolean ring, primary ideals are the same thing as maximal ideals, and so Ring 2 has none of either.

Ring 5 is a ring satisfying N_3. The ideal J of that ring is nil, nonzero and idempotent, hence not nilpotent; thus (b) fails.

Ring 3 also satisfies condition N_3. Every proper ideal of this ring extends to a maximal ideal, so there is a maximal ideal I extending the ideal generated by the atoms. I is then prime and nonprincipal. In a boolean ring every prime ideal is a minimal prime ideal, by ZF alone. Now suppose that I annihilates the ring element x; then for all y in the ring, $y \leqslant x^*$. Since I contains all the atoms, this implies $x^* = 1$, so $x = 0$. Thus (c) fails. □

Contrast Theorem 6 with Zariski and Samuel [10] p. 209 (for (a)), Jacobson [6] p. 199 (for (b), "Levitzki's theorem"), and Kaplansky [7] p. 57 (for (c)).

We do not know whether ZF may combine with N_2 to yield (b) or (c). In fact the only interesting difference we know between N_2 and N_3 is that the latter is strictly weaker than the former.

The open questions of highest priority in this area are perhaps those which concern Krull dimension. First and foremost, does ZF entail Krull's Principal Ideal Theorem for commutative rings with N_3?

3.3. *Semisimplicity*

When algebraists want to see the descending chain condition looking its best, they combine it with the further condition that the Jacobson radical be zero. When we try to do this without Zorn, we quickly find that we have to decide which Jacobson radical we mean. It appears we have two choices for the Jacobson radical of a commutative ring R:

$$J_1(R) = \{x \in R\colon 1 + xy \text{ is invertible for all } y \in R\};$$
$$J_2(R) = \bigcap \{I\colon I \text{ a maximal ideal of } R\}.$$

The classical proof that $J_1(R) = J_2(R)$ (cf., Jacobson [6, p. 9] in particular) goes through whenever we have enough maximal ideals to call on; for this it's enough to assume either Zorn's Lemma or condition N_1 on R.

THEOREM 7. *Let R be any commutative ring. Then* ZF *entails that* $J_1(R) \subseteq J_2(R)$; *but it is consistent with* ZF *that* $J_1(R) \neq J_2(R)$ *even when conditions* A_3 *and* N_3 *hold for* R.

Proof. Suppose $J_1(R) \not\subseteq J_2(R)$; then there is some $x \in J_1(R)$ and some maximal ideal I of R such that $x \notin I$. Since I is maximal, there is some $y \in R$ and some $z \in I$ such that $z - yx = 1$. By the definition of $J_1(R)$ this implies that z is invertible, so that I is improper. This proves $J_1(R) \subseteq J_2(R)$ using only ZF.

Ring 2 is a boolean ring R with no maximal ideals. In a boolean ring only 1 is invertible, and $1 + x = x^*$, so that J_1 of a boolean ring is always (0). Hence for our ring, $J_1(R) = (0) \neq R = J_2(R)$. This completes the proof. □

It seems to us that $J_2(R)$ is a rather silly notion to use when we have no guarantee that maximal ideals exist. Fortunately $J_1(R)$ has sensible properties even without Zorn. For example, let $f: R \to S$ be a surjective homomorphism of rings; then $fJ_1(R) \subseteq J_1(S)$. Another sensible property is that every nilpotent element of R lies in $J_1(R)$. For say $x^n = 0$. Then for every $y \in R$ we have $(-xy)^n = 0$. Put $b = 1 - xy + (xy)^2 - \cdots + (-xy)^{n-1}$; then $b(1 + xy) = 1 - (-xy)^n = 1$, so $x \in J_1(R)$. No shadow of Zorn lies across this argument.

Let R be a commutative ring. We list five ways of defining what it is for R to be semisimple:

SS_1 : $J_1(R) = (0)$ and A_2 holds for R.

SS_1': R is the sum of a collection of irreducible ideals.

SS_1'' : R is the direct sum of a finite collection of irreducible ideals.

SS_2 : For every ideal I of R there is an ideal J such that $R = I \oplus J$.

SS_3 : $J_1(R) = (0)$ and A_3 holds for R.

(An ideal I of the commutative ring R is *irreducible* if I is minimal among the nonzero ideals of R.) In the presence of Zorn, these definitions are all equivalent; in fact Dependent Choice is all we need to glue them together. Zorn is not needed at all for the equivalences

$$SS_1 \Leftrightarrow SS_1' \Leftrightarrow SS_1''.$$

This will be Theorem 9. The arguments for Theorems 8 and 9 are all familiar taken piecemeal, but it is a rare author who uses them without slipping in a maximal ideal or the Axiom of Dependent Choice at some point.

THEOREM 8. *Suppose the commutative ring R satisfies condition SS_1, and I is a nonzero ideal of R. Then* ZF *implies the following: there is an idempotent* *e of R such that $I = eR$, I is a ring satisfying SS_1 with e as multiplicative identity, and every ideal of the ring I is also an ideal of the ring R.*

Proof. Use SS_1 to find a minimal nonzero ideal $J \subseteq I$. If $J^2 = (0)$, then every element of J is nilpotent, so by a remark above, $J \subseteq J_1(R) = (0)$ by SS_1. We deduce that for some $x \in J$, $xJ \neq (0)$; the minimality of J then implies $xJ = J$. We infer that for some nonzero $b \in J$, $xb = x$. The set of all $y \in J$ such that $xy = 0$ is an ideal J' of R, and $J' \subset J$ since $b \notin J'$. Hence by the minimality of J, $J' = (0)$. Now $x(b^2 - b) = xb^2 - xb = x - x = 0$, so $b^2 - b \in J' = (0)$, whence $b^2 = b$. This so far proves only that I contains a nonzero idempotent of R.

Now use SS_1 again to find a non-zero idempotent $e \in I$ such that the ideal $(0 : e) \cap I$ is minimal among such ideals. We assert that $(0 : e) \cap I = (0)$. For otherwise the argument above shows that $(0 : e) \cap I$ contains a nonzero idempotent a. Then $ae = 0$, so that $(a + e)e = ae + e^2 = e$. Hence $(0 : a + e) \subseteq (0 : e)$. Moreover $(a + e)^2 = a^2 + 2ae + e^2 = a + e$, so that $a + e$ is a nonzero idempotent in I. Hence by choice of e, $(0 : a + e) \cap I = (0 : e) \cap I$. But this is impossible since $a \in I$ and $ae = 0 \neq a(a + e)$. The contradiction shows that $(0 : e) \cap I = (0)$. Now if $z \in I$, then $(z - ze)e = ze - ze = 0$, so that $z - ze \in (0 : e) \cap I = (0)$. Hence e is a multiplicative identity on I, so $I \subseteq eR$. But $e \in I$, so $eR \subseteq I$, whence $I = eR$.

If K is any ideal of the ring I, then $KR = (Ke)R = K(eR) = KI$, so that K is also an ideal of R. This also guarantees A_2 for the ring I. Suppose finally that $x \in J_1(I)$, and let $y \in R$. Then $xy = (xe)y = x(ey)$, so that the assumption on x implies there is $z \in I$ such that $z(e + xy) = e$. Then

$$\begin{aligned}(z + 1 - e)(1 + xy) &= z + zxy + 1 + xy - e - exy \\ &= ze + zxy + 1 + xy - e - xy \\ &= e + 1 + xy - e - xy = 1.\end{aligned}$$

This shows that $x \in J_1(R)$. Therefore $J_1(I) \subseteq J_1(R) = (0)$, which completes the argument using only ZF. □

THEOREM 9. *ZF entails that SS_1, SS_1' and SS_1'' are equivalent.*

Proof. We go in a circle. First, $SS_1 \Rightarrow SS_1'$. Assume SS_1 holds for the commutative ring R. Consider the set of all ideals I of R such that for some finite set $K_1, \ldots, K_n$ of irreducible ideals of R, $R = K_1 \oplus \cdots \oplus K_n \oplus I$. This set is nonempty, since it contains R. By SS_1, pick a minimal ideal I in the set, together with irreducible ideals $K_1, \ldots, K_n$ such that $R = K_1 \oplus \cdots \oplus K_n \oplus I$. We claim that $I = (0)$. For otherwise by Theorem 8 I is a ring satisfying SS_1. I therefore contains an irreducible ideal J, and by Theorem 8 there is an idempotent f of I such that $J = fI$. Put $I' = (1 - f)I$;

then I' is an ideal of I, and I is a direct sum $I = fI \oplus (1 - f)I$. Ideals of I are also ideals of R, so that R has the direct sum decomposition $R = K_1 \oplus \cdots \oplus K_n \oplus J \oplus I'$. Since J is an irreducible ideal of I, and hence of R, this contradicts the choice of I. Therefore $I = (0)$ as claimed. This proves SS_1'', and hence SS_1'.

Next, $SS_1' \Rightarrow SS_1''$. For assume SS_1' holds in R; then there is some shortest sum $I_1 + \cdots + I_n$ of irreducible ideals of R such that $1 = a_1 + \cdots + a_n$ with $a_i \in I_i$ for each i. Clearly this sum of ideals is the whole of R. If $0 \neq x \in I_i \cap I_j$ with $i \neq j$, then $xR \subseteq I_i \cap I_j$, so by the irreducibility of I_i and I_j we have $I_i = xR = I_j$, implying that the sum could have been shortened by omitting I_j. Hence the sum is direct, and R satisfies SS_1''.

The third part is to show $SS_1'' \Rightarrow SS_1$. Assume $R = I_1 \oplus \cdots \oplus I_n$, where the I_i are distinct irreducible ideals of R. If $a \in I_i$ and $b \in I_j$ with $i \neq j$, then $ab \in I_i \cap I_j = (0)$, so $ab = 0$. Let $1 = e_1 + \cdots + e_n$ where each $e_i \in I_i$. If $x \in I_i$, then $x = 1x = \sum_j e_j x = e_i x$ by the previous sentence; hence I_i is a ring with multiplicative identity e_i, and $I_i = e_i R$. If J is an ideal of I_i, then $JR = (Je_i)R = J(e_i R) = JI_i = J$; so J is also an ideal of R. Therefore the ideals of I_i are simply the ideals of R which are contained in I_i. In a nonzero ring 0 is not invertible; so $J_1(I_i) = (0)$ by the irreducibility of I_i in R.

We show $J_1(R) = (0)$. Say $x \in J_1(R)$, and consider any I_i. If $y \in I_i$, then by assumption on x there is $b \in R$ such that $1 = b(1 + xy)$; whence $e_i = e_i^2 = e_i^2 b(1 + xy) = e_i b(e_i + e_i xy)$. Hence $e_i x \in J_1(I_i) = (0)$. Therefore $x = \sum_i e_i x = 0$, proving $J_1(R) = (0)$.

Finally we show A_2 holds for R. If J is an ideal of R, then for each i, $J \cap I_i$ is either I_i or (0). Since $x \in J$ implies $e_i x \in J$ for each i, this entails that R has only finitely many distinct ideals. A_2 follows. The theorem is proved, using no more than ZF. □

The facts about SS_2 and SS_3 are a little more disappointing.

THEOREM 10. *The only implications between pairs of conditions from SS_1, SS_2, SS_3, N_1, N_2 which are provable from* ZF *alone are those shown below*:

$$\begin{array}{ccc} SS_1 & \Rightarrow & N_1 \\ \Downarrow & & \Downarrow \\ SS_2 & \Rightarrow & N_2 \\ \Downarrow & & \\ SS_3 & & \end{array}$$

Proof. We take the positive assertions first. Theorem 1 gave us $N_1 \Rightarrow N_2$. Both N_1 and SS_2 follow smoothly from SS_1'', which by Theorem 9 is equivalent to SS_1 given only ZF. There remain the two consequences of SS_2.

Suppose R is a commutative ring satisfying SS_2. Let I be an ideal of R; then for some ideal J of R, $R = I \oplus J$. The third part of the proof of Theorem 9 showed that I must then be a ring of form $e_I R$, where the multiplicative identity e_I of I is an idempotent of R, and the ideals of I are the ideals of R contained in I. Likewise $J = e_J R$, and we have $1 = e_I + e_J$. This already shows I is principal, which proves N_2. It also follows at once that the complement J of I is unique. For say also $R = I \oplus K$ where K is an ideal of R. Then $e_I + e_J = 1 = e_I + e_K$; so $e_J = e_K$ and hence $J = K$.

We claim that SS_2 holds also for the ring I. For say I_0 is an ideal of I; then I_0 is also an ideal of R, whence for some ideal K of R, $R = I_0 \oplus K$. Then $e_I = (e_{I_0} + e_K)\, e_I = e_{I_0} e_I + e_K e_I = e_{I_0} + e_K e_I$, so $I = I_0 + e_K e_I R = I_0 + e_K I$. Since $e_K I \subseteq K$, the sum is direct. This proves the claim.

Now we can prove that R satisfies condition SS_3. Suppose there is an infinite strictly descending chain $(I_i)_{i \in \omega}$ of ideals of R. Then we have shown that there is for each i a unique ideal J_i of the ring I_i such that $I_i = I_{i+1} \oplus J_i$; the J_i must all be nonzero ideals of the ring R. Since the J_i are uniquely defined, we can describe the set $\{J_i : i \in \omega\}$ explicitly from the chain $(I_i)_i$, so we can form the direct sum $\bigoplus_{i \in \omega} J_i$. (NB: if the J_i were not uniquely definable, we should have to invoke some Choice principle here.) This sum is an ideal of R, so by SS_2 there is an ideal K of R such that $R = \bigoplus_i J_i \oplus K$. Now there must be some j such that $1 \in \bigoplus_{i<j} J_i \oplus K$, whence $R = \bigoplus_{i<j} J_i \oplus K$. But this implies $J_j = (0)$, which is false. This contradiction proves A_3 for R. It remains to prove that $J_1(R) = (0)$. By SS_2, there is some ideal I such that $R = J_1(R) \oplus I$; so $1 = a + b$ for some $a \in J_1(R)$ and $b \in I$. Now $1 - a$ is invertible by definition of $J_1(R)$, whence it follows that $I = R$. Hence $J_1(R) = (0)$ as was to be proved.

The positive part of the theorem is proved; we turn to the negative. It is classical that $N_1 \not\Rightarrow SS_3$, and we showed in Theorem 1 that $N_2 \not\Rightarrow N_1$. To show $SS_2 \not\Rightarrow N_1$, consider Ring 2. Every ideal of this boolean ring R is principal. Let aR be an ideal, and a^* the complement of a; then $R = aR \oplus a^*R$. Hence SS_2 holds for R. But N_1 fails for this ring, since it has no maximal ideals. Finally we show $SS_3 \not\Rightarrow N_2$. The ring R for this is Ring 3. Here $J_1(R) = (0)$ as in any boolean ring, and A_3 holds for R; so we have SS_3. But the ideal I of finite elements is not finitely generated, which refutes N_2. This completes the proof of Theorem 10. □

References

1. P. Bernays, A system of axiomatic set theory III, *J. Symb. Logic* **7** (1942), 65–89.
2. Paul J. Cohen, "Set Theory and the Continuum Hypothesis," Benjamin, New York, 1966.

3. SOLOMON FEFERMAN, Set-theoretical foundations of category theory, *in* "Reports of the Midwest Category Seminar III," Springer Lecture Notes in Mathematics 106, Springer-Verlag, Berlin/New York, 1969.
4. ULRICH FELGNER, "Models of ZF-Set Theory," Springer Lecture Notes in Mathematics 223, Springer-Verlag, Berlin/New York, 1971.
5. WILFRID HODGES, On the effectivity of some field constructions, submitted.
6. NATHAN JACOBSON, "Structure of Rings," A.M.S. Colloquium Publications, revised ed., American Mathematics Society, Providence, R.I., 1964.
7. IRVING KAPLANSKY, "Commutative Rings," Allyn and Bacon, Boston, 1970.
8. JOSEPH R. SHOENFIELD, "Mathematical Logic," Addison-Wesley, Reading, MA, 1967.
9. ROMAN SIKORSKI, "Boolean Algebras," Springer-Verlag, Berlin/New York, 1964.
10. OSCAR ZARISKI AND PIERRE SAMUEL, "Commutative Algebra,"Vol. I, Van Nostrand, Princeton, 1958.