Journal of Universal Computer Science, vol. 14, no. 22 (2008), 3648-3657
submitted: 30/6/08, accepted: 11/12/08, appeared: 28/12/08 © J.UCS

Constructive Notions of Maximality for Ideals

Douglas S. Bridges
(Department of Mathematics and Statistics, University of Canterbury,
Christchurch, New Zealand
d.bridges@math.canterbury.ac.nz)

Robin S. Havea
(School of Computing, Information and Mathematical Sciences, University of
the South Pacific, Suva, Fiji
robin.havea@usp.ac.fj)

Abstract: Working constructively, we discuss two types of maximality for ideals in a commutative ring with identity, showing also that the results are the best possible.
Key Words: constructive, ideal, maximal
Category: F.2.m, G.0

1 Introduction

In this note we continue the constructive study of rings and ideals begun in [Bridges 2001], by examining two constructively distinct, but classically equivalent, notions of maximality for ideals. By (Bishop-style) "constructive" we mean "using intuitionistic logic and an appropriate set theory" such as that described in [Aczel and Rathjen 2001]. The use of intuitionistic logic enables us to perceive certain fine distinctions that are obscured under classical logic. Every proof that is constructive in our sense embodies an algorithm that can be extracted and implemented; moreover, the proof itself shows that the extracted algorithm meets its specifications.

Let R be a commutative ring with an identity element e and a **ring inequality:** that is, a binary relation $\neq$ that satisfies not only the usual constructive conditions for an inequality,

$$x \neq y \Rightarrow y \neq x,$$
$$x \neq y \Rightarrow \neg (x = y),$$

but also $e \neq 0$ and the following:

$$x \neq y \Leftrightarrow x - y \neq 0,$$
$$x + y \neq 0 \Rightarrow x \neq 0 \vee y \neq 0,$$
$$xy \neq 0 \Rightarrow x \neq 0 \wedge y \neq 0.$$

Note that as a consequence of the first of the last three conditions we have

$$x \neq y \Leftrightarrow \forall_{z \in R} (x + z \neq y + z).$$

The **complement** of a subset S of R is the set

$$\sim S = \{x \in R : \forall_{y \in S} (x \neq y)\}.$$

In general this is not the same, constructively, as the **logical complement**,

$$\neg S = \{x \in R : x \notin S\},$$

of S: for example, in the ring $\mathbf{R}$ of real numbers—or, more generally, in any Banach algebra—the inequality is defined by

$$x \neq y \Leftrightarrow \|x - y\| > 0$$

and, in the absence of Markov's principle, is stronger than the denial inequality $\neg (x = y)$.

We call the ring R

- **discrete** if for all $x \in R$, either $x \neq 0$ or $x = 0$, and
- **quasidiscrete** if for all $x \in R$, either $x \neq e$ or x is invertible.

If R is discrete, then for all x, y in R either $x = y$ or $x \neq y$. Clearly, a discrete ring is quasidiscrete. A Banach algebra $\mathfrak{A}$ is quasidiscrete, since for each $x \in \mathfrak{A}$, either $x \neq e$ or $\|e - x\| < 1$, and in the latter case x is invertible; but if even the Banach algebra $\mathbf{R}$ were discrete, then we would be able to prove the essentially nonconstructive principle

> **LPO:** *For each binary sequence* $(a_n)_{n \geqslant 1}$, *either* $a_n = 0$ *for all* n *or else there exists* n *such that* $a_n = 1$.

We denote by $\langle S \rangle$ the ideal generated by a subset S of R. In the special case where $S = T \cup \{x\}$ for some $T \subset R$ and $x \in R$, we write $\langle T, x \rangle$ for $\langle S \rangle$; if, further, $T = \varnothing$, we write $\langle x \rangle$ rather than $\langle \{x\} \rangle$.

We say that an ideal I of R is

- ▷ **proper** if $e \in \sim I$;
- ▷ **maximal** if it is proper and for each $x \in \sim I$ the ideal $\langle I, x \rangle$ equals R;
- ▷ **weakly maximal** if (i) it is proper and (ii) for each $x \in R$, if $\langle I, x \rangle$ is a proper ideal, then $x \in I$.
- ▷ **stable** if $\sim\sim I = I$.

Note that a proper ideal I is weakly maximal if and only if $M = I$ whenever M is a proper ideal that includes I.

Although the notions of "maximal" and "weakly maximal" are classically equivalent, they can be distinguished constructively, as the following Brouwerian example shows. In the (discrete) ring $\mathbf{Z}$ of integers consider the ideal I generated by the set

$$S \equiv \{n \in \mathbf{Z} : n = 4 \vee (n = 2 \wedge (P \vee \neg P))\},$$

where P is any syntactically correct mathematical statement. It is easy to see that, since $\neg(P \vee \neg P)$ is false, $\sim I$ is the set of odd integers and therefore I is maximal. Now, $\langle I, 2\rangle = \langle 2\rangle$ is a proper ideal; but if $\langle I, 2\rangle = I$, then $P \vee \neg P$ holds. Thus the statement

Every maximal ideal of $\mathbf{Z}$ *is weakly maximal*

implies the law of excluded middle (**LEM**). However, as we shall see later (Corollary 15), every weakly maximal ideal of $\mathbf{Z}$ is maximal.

2 Stability

We begin our exploration of the links between maximality, weakly maximality, and stability with a couple of simple lemmas.

Lemma 1. *If I is a proper ideal in R and if $x \in R$ is invertible, then $x \in \sim I$.*

Proof. For each $y \in I$ we have $x^{-1}y \in I$, so $x^{-1}y \neq e = x^{-1}x$ and therefore $x^{-1}(y - x) \neq 0$; whence $y \neq x$. Thus $x \in \sim I$.

Lemma 2. *Let I be an ideal in R. Let $p \in I, q \in R$, and $x \in R$ be such that $p + qx \in \sim I$. Then $x \in \sim I$.*

Proof. For each $y \in I$, since $p + qy \in I$, we have $p + qx \neq p + qy$; whence $q(x - y) \neq 0$ and therefore $x \neq y$.

Lemma 3. *If R is quasidiscrete and I is a proper ideal of R, then for each $x \in \sim\sim I$, the ideal $\langle I, x\rangle$ is proper.*

Proof. Given $x \in \sim\sim I$, consider any element $p + qx$ of $\langle I, x\rangle$, where $p \in I$ and $q \in R$. Suppose that $p+qx$ is invertible. Then by Lemmas 1 and 2, $x \in \sim I$, which is absurd. Hence $p + qx$ is not invertible, and therefore, by quasidiscreteness, $p + qx \neq e$. Since $p \in I$ and $q \in R$ are arbitrary, we conclude that $e \in \sim \langle I, x\rangle$.

The trick used in the foregoing proof to prove that $p + qx \neq e$ is used again, twice, in the proof of Proposition 5 below. First, though, we deal with the stability of weakly maximal ideals.

Proposition 4. *If R is quasidiscrete, then every weakly maximal ideal in R is stable.*

Proof. Let I be a weakly maximal ideal in R, and $x \in \sim\sim I$. Since I is proper, Lemma 3 shows that the ideal $\langle I, x\rangle$ is proper. The weak maximality of I now ensures that $\langle I, x\rangle = I$ and therefore $x \in I$. Hence $\sim\sim I \subset I$ and so $\sim\sim I = I$.

What about the stability of maximal ideals? In the Brouwerian example preceding Lemma 1 we cannot prove that the maximal ideal I is stable: for, $2 \in \sim\sim I$, but if $2 \in I$, then we have $P \vee \neg P$. For maximal ideals in a quasidiscrete ring we have this stability result:

Proposition 5. *If R is quasidiscrete, then for each maximal ideal I of R, $\sim\sim I$ is a stable maximal ideal.*

Proof. Let $x, y \in \sim\sim I$ and $a \in R$. To show that $x - ay \in \sim\sim I$, first consider the case where $x \in I$. Since I is maximal, for each $z \in \sim I$ there exist $p \in I$ and $q \in R$ such that $e = p + qz$. Suppose that $p + q(x - ay)$ is invertible. Then, by Lemmas 1 and 2, $x - ay \in \sim I$. For each $y' \in I$, since $x - ay' \in I$, we have $x - ay \neq x - ay'$; whence $a\,(y - y') \neq 0$ and therefore $y \neq y'$. Thus $y \in \sim I$, a contradiction from which we conclude that $p + q(x - ay)$ is not invertible. Since the inequality is quasidiscrete,

$$p + q(x - ay) \neq e = p + qz$$

and therefore $x - ay \neq z$. Since $z \in \sim I$ is arbitrary, it follows that $x - ay \in \sim\sim I$. This disposes of the case $x \in I$.

In the general case, let z, p, q be as before, and consider any $x' \in I$. By the foregoing, $x' - ay \in \sim\sim I$. If $p + q(x - ay)$ is invertible, then, by Lemmas 1 and 2, $x - ay \in \sim I$ and therefore $x - ay \neq x' - ay$; whence $x \neq x'$. Since $x' \in I$ is arbitrary, this yields $x \in \sim I$, again a contradiction from which we conclude that $p + q(x - ay)$ is not invertible. Arguing as at the end of the case $x \in I$, we now obtain $x - ay \in \sim\sim I$. Since $x, y \in \sim\sim I$ and $a \in R$ are arbitrary, it follows that $\sim\sim I$ is an ideal in R.

Now, since

$$e \in \sim I = \sim\sim\sim I$$

and

$$\sim\sim(\sim\sim I) = \sim(\sim\sim\sim I) = \sim\sim I,$$

the ideal $\sim\sim I$ is both proper and stable. If $x \in \sim(\sim\sim I)$, then $x \in \sim I$; so $\langle I, x\rangle = R$ and therefore $\langle \sim\sim I, x\rangle = R$. Hence $\sim\sim I$ is maximal.

If I is an ideal of R such that $\sim\sim I$ is maximal (resp., weakly maximal), is I itself maximal (resp., weakly maximal)? To see that this is not so constructively even for a discrete ring, let P be any syntactically correct statement such that $\neg\neg P$ holds, and let I be the ideal generated in the ring $\mathbf{Z}$ of integers by the set

$$G \equiv \{n \in \mathbf{Z} : n = 2 \wedge P\}.$$

Then $\sim\sim I$ is the prime, maximal, and weakly maximal ideal $\langle 2 \rangle$. But if I is maximal, then we can find $m \in I$ and $n \in \mathbf{Z}$ such that $m + 3n = 1$; since $m \in I$ and, clearly, $m \neq 0$, we must have P. On the other hand, being a subset of $\sim\sim I$, the ideal $\langle I, 2 \rangle$ is proper; so if I is weakly maximal, then $2 \in I$ and again we obtain P. Thus the statement

> *Every proper ideal I of $\mathbf{Z}$ such that $\sim\sim I$ is a maximal (resp., weakly maximal) ideal is itself maximal (resp. weakly maximal)*

implies **LEM**. (Note that even with intuitionistic logic, the law $(\neg\neg P \Rightarrow P)$ is equivalent to **LEM**.)

The next three results shed more light on the stability of maximal ideals.

Proposition 6. *Let I be a maximal ideal of R, and J a proper ideal of R that includes I. Then $\sim I = \sim J$.*

Proof. Let $x \in \sim I$. Then there exist $p \in I$ and $q \in R$ such that $e = p + qx$. For each $y \in J$ we have $p + qy \in J$ and so $p + qy \neq e$; whence $q(x - y) \neq 0$ and therefore $x \neq y$. Thus $x \in \sim J$. Since $x \in \sim I$ is arbitrary, we conclude that $\sim I \subset \sim J$. The reverse inclusion is trivial.

Corollary 7. *Let I be a maximal ideal of R, and J a proper ideal of R that includes I. Then $J \subset \sim\sim I$.*

Proof. By Proposition 6, $J \subset \sim\sim J = \sim\sim I$.

Corollary 8. *A stable maximal ideal of a ring R is weakly maximal.*

Proof. Use the previous corollary.

As an aside, we now consider the question: if an ideal I of a ring is proper, is $\langle \sim\sim I \rangle$ proper? If the ring is discrete, then the answer is "yes".

Proposition 9. *Let R be quasidiscrete, and I a proper ideal of R, that is* ***coadditive*** *in the sense that*

$$\forall_{x,y \in R}\,(x + y \in \sim I \Rightarrow x \in \sim I \vee y \in \sim I).$$

Then $\langle \sim\sim I \rangle$ is proper.

Proof. For $1 \leqslant k \leqslant n$, let $p_k \in R$ and $x_k \in {\sim}{\sim}I$. Either

$$e \neq p_1 x_1 + \cdots + p_n x_n \tag{1}$$

or else $p_1 x_1 + \cdots + p_n x_n$ is invertible. In the latter case, Lemma 1 shows that $p_1 x_1 + \cdots + p_n x_n \in {\sim}I$; whence, by coadditivity, there exists k such that $p_k x_k \in {\sim}I$. For each $x \in I$ we then have $p_k x_k \neq p_k x$, so $p_k (x_k - x) \neq 0$ and therefore $x_k \neq x$. Thus $x_k \in {\sim}I$, a contradiction. We conclude that (1) holds. Since $p_1 x_1 + \cdots + p_n x_n$ is an arbitrary element of $\langle {\sim}{\sim}I \rangle$, it follows that $\langle {\sim}{\sim}I \rangle$ is proper.

Constructively, not every proper ideal of **Z** can be proved coadditive. Consider the ideal I generated by

$$\{6\} \cup \{n \in \mathbf{Z} : n = 2 \wedge P\} \cup \{n \in \mathbf{Z} : n = 3 \wedge \neg P\},$$

where P is any syntactically correct mathematical statement: we have $2+3 \in {\sim}I$, but if $2 \in {\sim}I$, then $\neg P$, while if $3 \in {\sim}I$, then $\neg\neg P$.

3 Does weakly maximal imply maximal?

When is a weakly maximal ideal of R maximal? To answer this, we first prove

Proposition 10. *If I is a maximal ideal in R, then for all $x \in R$,*

$$x \in {\sim}I \Rightarrow x^2 \in {\sim}I. \tag{2}$$

Proof. Let $x \in {\sim}I$. There exist $a \in I$ and $b \in R$ such that $e = a + bx$; then $bx^2 = x - ax$. For each $y \in I$ we have $ax + by \in I$ and therefore

$$\begin{aligned} b\left(x^2 - y\right) &= bx^2 - by \\ &= x - (ax + by) \neq 0. \end{aligned}$$

Thus $x^2 - y \neq 0$ and therefore $x^2 \neq y$.

An ideal I of R is said to be **semiprime** if

$$(xy \in I \wedge x \in {\sim}I) \Rightarrow y \in I.$$

Proposition 11. *Let I be a weakly maximal ideal in R such that* (2) *holds. Then I is semiprime.*

Proof. Consider $x, y \in R$ such that $xy \in I$ and $x \in {\sim}I$. Let $M = \langle I, y \rangle$. For each $a \in I$ and $b \in R$, we have

$$x\,(x - a - by) = x^2 - (ax + bxy) \neq 0,$$

since $ax + bxy \in I$ and, by Proposition 10, $x^2 \in {\sim}I$. Hence $x - a - by \neq 0$ and therefore $x \neq a + by$. It follows that $x \in {\sim}M$, so M is a proper ideal that includes I. Since I is weakly maximal, we must have $M = I$ and therefore $y \in I$. Thus I is semiprime.

We now recall from [Bridges 2001] some properties of our ring. We call R

- a **cancellation domain** if for all x, y in R,

$$(xy = 0 \wedge x \neq 0) \Rightarrow y = 0;$$

- an **FGP ring** if every finitely generated ideal in R is principal;
- a **principal ideal ring** if it is an FGP ring and satisfies the **divisor chain condition:** for each ascending chain $I_1 \subset I_2 \subset \cdots$ of principal ideals in R there exists n such that $I_n = I_{n+1}$ (See page 110 of [Mines et al. 1988] for more on the divisor chain condition.)

The ring of integers is the primary example of a **principal ideal cancellation domain:** that is, a principal ideal ring that is also a cancellation domain.

Theorem 12. *If R is a principal ideal cancellation domain, then the following are equivalent conditions on a weakly maximal ideal I.*

(i) *I is maximal.*

(ii) $\forall_{x \in R} \left(x \in {\sim}I \Rightarrow x^2 \in {\sim}I \right)$.

(iii) *I is semiprime.*

Proof. Proposition 10 shows that (i) implies (ii), and Proposition 11 that (ii) implies (iii). That (iii) implies (i) is just Theorem 12 of [Bridges 2001].

Proposition 13. *If R is quasidiscrete, then every weakly maximal ideal of R is semiprime.*

Proof. Let I be a weakly maximal ideal of R, and let x, y be elements of R such that $xy \in I$ and $x \in {\sim}I$. For all $a \in I$ and $b \in R$, either $e \neq a + by$ or $a + by$ has an inverse z. In the latter case,

$$x = xe = (xz)\,a + (bz)\,xy \in I,$$

a contradiction. It now follows that $e \in {\sim}\langle I, y \rangle$. Since I is weakly maximal, we have $\langle I, y \rangle = I$ and hence $y \in I$.

Theorem 14. *Every weakly maximal ideal of a quasidiscrete principal ideal cancellation domain is maximal.*

Proof. This follows from Proposition 13 and Theorem 12.

Corollary 15. *A weakly maximal ideal in* $\mathbf{Z}$ *is maximal.*

Proof. Since $\mathbf{Z}$ is (quasi)discrete and a principal ideal cancellation domain, Theorem 14 applies.

Corollary 16. *The following are equivalent conditions on an ideal I in a quasidiscrete principal ideal cancellation domain.*

(i) *I is weakly maximal.*

(ii) *I is stable and maximal.*

Proof. This follows from Theorem 14, Proposition 4, and Corollary 8.

If we consider ideals in a Banach algebra A, then, although we trade in the discrete inequality of $\mathbf{Z}$, we gain as partial compensation the existence of inverses of nonzero elements. Does the Banach algebra structure enable us to prove that if $I \subset A$ is an ideal such that $\sim\sim I$ is a maximal ideal, then I is maximal? Our concluding example shows that this is not the case. For that example we assume Markov's principle:

> For each binary sequence, if it is impossible that all terms are 0, then there exists a term equal to 1,

which is equivalent to the statement

$$\forall_{x\in\mathbf{R}} \left(\neg\left(x=0\right) \Rightarrow x \neq 0\right).$$

In $\mathbf{R}$, as in any metric space, $x \neq y$ means that the elements x and y are a positive distance apart.

Let A be the Banach algebra $C[0,1]$ with the usual sup norm, let P be any syntactically correct mathematical statement, and let

$$S \equiv \{f \in A : f(0) = 0 \wedge (P \vee \neg P)\}.$$

Let I be the (clearly proper) closed ideal of A generated by the set $\left\{x^2\right\} \cup S$, where we abuse notation by writing $1, x, x^2, \ldots$ for the power functions. Then $f(0) = 0$ for each $f \in \sim\sim I$. On the other hand, for each $g \in \sim I$, if $g(0) = 0$, then $\neg\left(P \vee \neg P\right)$, since if $P \vee \neg P$, then $g \in I$. But $\neg\left(P \vee \neg P\right)$ is absurd; so

$\neg(g(0)=0)$ and therefore, by Markov's principle, $g(0) \neq 0$. It follows that if $f \in A$ and $f(0)=0$, then $f \in {\sim\sim}I$. Hence

$$\sim\sim I = \{f \in A : f(0) = 0\},$$

which, as is well known, is a maximal ideal of A. Now suppose that I itself is maximal. Then, since $1+x \in {\sim}I$,

$$A = \langle I, 1+x \rangle . \tag{3}$$

Let V be the finite-dimensional subspace of A with basis $\left\{1, x, x^2\right\}$. Since, as is easily proved, $x^3 \in {\sim}V$, we see from Bishop's lemma ([Bishop and Bridges 1985], page 92, Lemma (3.8)) that

$$0 < d \equiv \rho\left(x^3, V\right).$$

By (3), there exist complex numbers $\zeta_0, \ldots, \zeta_{m+1}$, and elements $f_1, \ldots, f_m$ of S such that

$$\sup_{0 \leqslant t \leqslant 1} \left| t^3 - \zeta_0 t^2 - \sum_{k=1}^{m} \zeta_k f_k(t) - \zeta_{m+1}(1+t) \right| < \frac{1}{2} d.$$

Then

$$\begin{aligned} \left\| \sum_{k=1}^{m} \zeta_k f_k \right\| &\geqslant \sup_{0 \leqslant t \leqslant 1} \left| t^3 - \left(\zeta_{m+1} + \zeta_{m+1} t + \zeta_0 t^2\right) \right| - \frac{1}{2} d \\ &\geqslant \rho\left(x^3, V\right) - d = \frac{1}{2} d > 0. \end{aligned}$$

It follows that there exists k such that $\zeta_k f_k \neq 0$. Hence S is inhabited, and therefore $P \vee \neg P$ holds. Thus, under the assumption of Markov's principle, the statement

> If I is a proper closed ideal of a Banach algebra such that ${\sim\sim}I$ is a maximal ideal, then I is maximal

implies **LEM**.

Acknowledgement.

The authors thank the University of the South Pacific Research Committee (URC) for generously supporting Havea's visits to New Zealand during which this paper was completed.

References

[Aczel and Rathjen 2001] Aczel, P., Rathjen, M,: *Notes on Constructive Set Theory*; Report No. 40, Institut Mittag–Leffler, Royal Swedish Academy of Sciences.

[Bishop and Bridges 1985] Bishop E. A., Bridges, D. S.: *Constructive Analysis*; Grundlehren der Math. Wiss. **279**, Springer-Verlag, Heidelberg.

[Bridges 2001] Bridges, D. S.: "Prime and maximal ideals in constructive ring theory"; Comm. Alg. **29**, 7, 2787-2803.

[Mines et al. 1988] Mines, R., Richman, F., Ruitenburg, W.: *A Course in Constructive Algebra*; Springer Universitext, Springer-Verlag, New York.