Reductions in Norman Megill's axiom system for complex numbers

Eric Schmidt

1 Introduction

Metamath[1] is a formal proof verifier designed and implemented by Norman Megill. He has also formalized many mathematical proofs in this system. As part of this project, he devised a collection of axioms for complex numbers. As with any set of axioms, we may ask whether or not any of the axioms are redundant, that is, derivable from the other axioms. Additionally, we may investigate whether replacing an axiom with an apparently weaker assertion results in a system of the same strength. In general, given some axiom system, we would like, by a process of removing and weakening axioms, to arrive at a system in which there are (provably) no redundancies and (apparently) no notable weakenings.

Some simplifications of Megill's original system were known before this paper. We describe further simplifications, and make significant progress towards proving that the resulting system contains no redundancies. We also present some related results of interest.

2 Axioms

2.1 Axiom system $\mathcal{C}_1$

We will describe Megill's original system as a collection of 26 first-order axioms and one second-order axiom. The system contains unary predicates for "is a complex number" and "is a real number", denoted, respectively, as $\_\_ \in \mathbb{C}$ and $\_\_ \in \mathbb{R}$. It also contains binary operations $+$ and $\cdot$, a binary relation $<$, and constants 0, 1, and i. We strive to use typical notation. For instance, we denote $\cdot$ as simply juxtaposition and consider $\cdot$ to have higher precedence than $+$. We also use set-theoretic notation, particularly to describe axiom (sup) below. The statement (sup) could, of course, be written purely in the language of second-order logic.

We define $\mathcal{C}_1$ to be the set of the following first-order statements:

(resscn) $\forall x \in \mathbb{R}\ x \in \mathbb{C}$
(0re) $0 \in \mathbb{R}$
(1re) $1 \in \mathbb{R}$
(icn) $i \in \mathbb{C}$
(addcl) $\forall z,\ w \in \mathbb{C}\ z + w \in \mathbb{C}$
(addrcl) $\forall x,\ y \in \mathbb{R}\ x + y \in \mathbb{R}$
(mulcl) $\forall z,\ w \in \mathbb{C}\ zw \in \mathbb{C}$
(mulrcl) $\forall x,\ y \in \mathbb{R}\ xy \in \mathbb{R}$
(addcom) $\forall z, w \in \mathbb{C}\ z + w = w + z$
(mulcom) $\forall z,\ w \in \mathbb{C}\ zw = wz$
(addass) $\forall z,\ w,\ u \in \mathbb{C}\ (z + w) + u = z + (w + u)$

[1] `http://metamath.org`

(mulass) $\forall z,\, w,\, u \in \mathbb{C}\ (zw)u = z(wu)$

(distr) $\forall z,\, w,\, u \in \mathbb{C}\ z(w+u) = zw + zu$

(1ne0) $1 \neq 0$

(0id) $\forall z \in \mathbb{C}\ z + 0 = z$

(1id) $\forall z \in \mathbb{C}\ z1 = z$

(negex) $\forall z \in \mathbb{C}\ \exists w \in \mathbb{C}\ z + w = 0$

(recex) $\forall z \in \mathbb{C}\ (z \neq 0 \to \exists w \in \mathbb{C}\ zw = 1)$

(rnegex) $\forall x \in \mathbb{R}\ \exists y \in \mathbb{R}\ x + y = 0$

(rrecex) $\forall x \in \mathbb{R}\ (x \neq 0 \to \exists y \in \mathbb{R}\ xy = 1)$

(i2m1) $ii + 1 = 0$

(cnre) $\forall z \in \mathbb{C}\ \exists x,\, y \in \mathbb{R}\ z = x + yi$

(lttri) $\forall x,\, y \in \mathbb{R}\ (x < y \leftrightarrow \neg(x = y \vee y < x))$

(lttrn) $\forall x,\, y,\, z \in \mathbb{R}\ ((x < y \wedge y < z) \to x < z)$

(ltadd) $\forall x,\, y,\, z \in \mathbb{R}\ (x < y \to z + x < z + y)$

(mulgt0) $\forall x,\, y \in \mathbb{R}\ ((0 < x \wedge 0 < y) \to 0 < xy)$,

and the following second-order statement:

(sup) $$\begin{aligned}&\forall S \subseteq \mathbb{R}\ ((S \neq \varnothing \wedge \exists x \in \mathbb{R}\ \forall y \in S\ y < x)\\ &\quad \to \exists x \in \mathbb{R}\ (\forall y \in S\ (\neg\, x < y) \wedge \forall y \in \mathbb{R}\ (y < x \to \exists z \in S\ y < z))).\end{aligned}$$

Notes:

1. Megill's system, as he describes it, contains an axiom equivalent to the assertion that $\mathbb{C}$ is a set, rather than a proper class. We have omitted it since this cannot be stated in our formulation as a second-order theory. There are other, minor differences between our presentation and Megill's; these need not detain us.

2. Megill observes that (i2m1) could be used to eliminate 0 as a primitive constant, at the expense of complicating the statements of the other axioms.

3. We could assume that the universe is the set of complex numbers, which would make superfluous a number of the axioms. We have not done this since we wish to investigate whether these axioms are redundant.

2.2 Candidates for weaker axioms

Part of our aim is to investigate whether various axioms can be replaced with weaker axioms. We must, however, ask the question: what makes an axiom "weaker"? Consider, say, the axiom (1re). If we were able to replace this axiom with the assertion $1 \in \mathbb{C}$ (which, we will soon show, we can), we would be inclined to regard this as a weakening of (1re). However, since, as a whole, the resulting system is just as strong, in what sense has anything been "weakened"? We cannot resolve this by considering (1re) in isolation, since $1 \in \mathbb{R} \to 1 \in \mathbb{C}$ is not a logical truth. It is only together with the axiom (resscn) that it becomes coherent to regard $1 \in \mathbb{R}$ as a stronger assertion than $1 \in \mathbb{C}$.

Additionally, some weakenings may actually be considered undesirable. For instance, we could weaken (addass) by restricting u to be nonzero, since the case where $u = 0$ can be easily recovered from the other axioms. However, this would complicate the statement of the axiom.

We will not attempt to provide a solution to these matters. Instead, we will simply consider a restricted class of weakenings. These are of two types: replacing universal quantification over $\mathbb{C}$ with universal quantification over $\mathbb{R}$, and replacing membership in $\mathbb{R}$ with membership in $\mathbb{C}$. In particular, we will discuss the following statements as potential weakenings of axioms of $\mathcal{C}_1$:

(1cn)	$1 \in \mathbb{C}$
(addrass)	$\forall x, y, z \in \mathbb{R}\ (x+y)+z = x+(y+z)$
(mulrass)	$\forall x, y, z \in \mathbb{R}\ (xy)z = x(yz)$
(rdistr)	$\forall x, y, z \in \mathbb{R}\ x(y+z) = zy + xz$
(r1id)	$\forall x \in \mathbb{R}\ x1 = x$.

3 Reductions

In this section, we discuss various *reductions* of $\mathcal{C}_1$, that is, ways of either removing axioms or weakening them.

3.1 The reduction to $\mathcal{C}_2$

We first discuss the reductions found and published on the Metamath website prior to this paper. Define $\mathcal{C}_2$ to be $\mathcal{C}_1 - \text{(0re)} - \text{(negex)} - \text{(recex)} - \text{(1re)} + \text{(1cn)}$. We will show the equivalence of this system with $\mathcal{C}_1$.

The first reduction was found by Megill in 2005.

Lemma 3.1 (Megill)**.** *The statement* (0re) *is derivable from* $\mathcal{C}_1 - \text{(0re)}$.

Proof. By (1re) and (rnegex), there exists $x \in \mathbb{R}$ such that $1+x = 0$. Then, by (addrcl), we conclude $0 \in \mathbb{R}$. □

In 2007, the author discovered the following.

Lemma 3.2. $\mathcal{C}_2 \vdash \mathcal{C}_1$.

Proof. Deduction of (0re): By either (icn) or (1cn), $\mathbb{C}$ is nonempty. Thus, by (cnre), $\mathbb{R}$ is also nonempty. Take $x \in \mathbb{R}$. By (rnegex), there exists $y \in \mathbb{R}$ such that $x + y = 0$. Then, using (addrcl), we deduce (0re). At this point, we know that $\mathbb{R}$ is an ordered field.

Deduction of (negex): By (cnre), any complex number may be expressed as $a + bi$ for some $a, b \in \mathbb{R}$. Again, from (cnre) we know that $0 = x + yi$ for some x, $y \in \mathbb{R}$. Then, $yi = -x \in \mathbb{R}$. Therefore, there exists $c \in \mathbb{R}$ such that $b + c = yi$. Then, $a + bi + ci = a + yi \in \mathbb{R}$, so it has an additive inverse $d \in \mathbb{R}$. Thus, $ci + d$ is the desired additive inverse of $a + bi$. At this point, we know that $\mathbb{C}$ is a commutative ring.

Deduction of (1re): Using (1cn) and (cnre), we know that $1 = x + yi$ for some x, $y \in \mathbb{R}$. Because $\mathbb{C}$ is a ring, $0i = 0$. Thus, if we had $x = y = 0$, we would have $1 = 0$, which contradicts (1ne0). Thus, there exists a nonzero real number. So, applying (rrecex) and (rmulcl), we deduce (1re).

Deduction of (recex): Take an arbitrary nonzero complex number $a + bi$, with a, $b \in \mathbb{R}$. Since $a + bi \neq 0$, either $a \neq 0$ or $b \neq 0$. Since $\mathbb{R}$ is an ordered field, $a^2 + b^2 > 0$. Then, $(a - bi)(a^2 + b^2)^{-1}$ is a multiplicative inverse to $a + bi$. □

3.2 Some useful lemmas

Here we prove some lemmas that we will have need of later. First we have a basic fact noted by Dummit and Foote.[2]

Lemma 3.3. *Suppose R is a set with a group operation $+$ and a monoid operation $\cdot$ (with identity element 1), such that $\cdot$ distributes over $+$. Then, $+$ is commutative. Thus, R is a ring.*

[2] Dummit, David Steven, and Richard M. Foote. *Abstract Algebra.* 3rd ed. John Wiley & Sons Inc, 2004., p. 223.

Proof. By distributing the left term, we have $(a+b)\cdot(1+1) = a+b+a+b$. By distributing the right term instead, we obtain $(a+b)\cdot(1+1) = a+a+b+b$. By cancelling, we find that $a+b = b+a$. □

The following result and its proof are based on formal derivations found on the Metamath website.[3]

Lemma 3.4. *Let G be a set with a binary operation denoted by juxtaposition. Suppose that the binary operation is associative and that there exists $e \in G$ such that $ge = g$ for all $g \in G$. Suppose also that for all $g \in G$, there exists $h \in G$ such that $gh = e$. Then G is a group.*

Proof. Suppose $g \in G$. Then, by assumption, there exists $h \in G$ with $gh = e$. We claim that also $hg = e$. To prove this, note that there exists $k \in G$ such that $hgk = e$. Then, $hg = hge = hghgk = hegk = hgk = e$. Moreover, e is a left identity element since $eg = ghg = ge = g$. Thus, G is a group. □

Last, we present two more lemmas that we need.

Lemma 3.5. *It follows from* (addrcl), (lttri), *and* (ltadd) *that for all x, y, $z \in \mathbb{R}$, if $z + x = z + y$, then $x = y$.*

Proof. If $x \neq y$, then by (lttri), either $x < y$ or $y < x$. If $x < y$, then (ltadd) gives $z + x < z + y$, so $z + x \neq z + y$. We obtain the same conclusion if $y < x$. □

Lemma 3.6. *It follows from $\mathcal{C}_1 -$* (sup) *that every member of $\mathbb{C}$ has a unique representation in the form $a + bi$ with a, $b \in \mathbb{R}$.*

Proof. By (cnre), such representations exist, so we need only show uniqueness. By (i2m1), we have $i^2 = -1 < 0$, so $i \notin \mathbb{R}$. Next, suppose that $a + bi = 0$ with a, $b \in \mathbb{R}$. Then $b = 0$, for otherwise we would have $i = -a/b$. It then follows that $a = 0$. Thus, $0 + 0i$ is the unique representation of 0. To prove the result, take complex numbers $a_1 + b_1 i$, $a_2 + b_2 i$, and apply the previous observation to $(a_1 - a_2) + (b_1 - b_2)i$. □

3.3 The reduction to $\mathcal{C}_3$

We now show how $\mathcal{C}_2$ may be reduced even further. Let $\mathcal{C}_3 = \mathcal{C}_2 - (\text{addcom}) - (\text{0id}) - (\text{1id}) + (\text{r1id})$.

Lemma 3.7. $\mathcal{C}_3 \vdash \mathcal{C}_1$.

Proof. Deduction of (0re): As in Lemma 3.2.

Deduction of (1re): Using (1ne0), we see that there exist at least two complex numbers, so by (cnre), there exist at least two real numbers. Thus there exists a nonzero real number, so by (rrecex) and (mulrcl), we deduce (1re).

Deduction of (1id): For any $a + bi \in \mathbb{C}$, we have $(a + bi)1 = a1 + (b1)i = a + bi$.

Deduction of (0id): First we claim that $0 = 0+0$. To prove this, note that by (rnegex), there exists $c \in \mathbb{R}$ with $0+c = 0$. If $0 \neq 0+0$, then $c \neq 0$. For any $x \in \mathbb{R}$, we have $0x+0 = (0+c)x+0 = 0x+cx+0$. By Lemma 3.5, $0 = cx + 0$. Then, take $x = c^{-1}0$ to obtain $0 = 0 + 0$, a contradiction.

Next, we claim that $0x = 0$ for all $x \in \mathbb{R}$. For suppose we had $x \in \mathbb{R}$ with $0x \neq 0$. Then, for any $z \in \mathbb{C}$, multiplying the equation $0 = 0 + 0$ by $(0x)^{-1}xz$ yields $z = z + z$. Suppose $y \in \mathbb{R}$ and $w \in \mathbb{C}$. Write $w = a + bi$, with a, $b \in \mathbb{R}$. Then, $y + a = y + y + a$, so by Lemma 3.5, $a = y + a$.

[3] See `http://us.metamath.org/mpegif/grpidinvlem1.html` and ff. (where "left" and "right" are reversed from our formulation).

Adding bi on the right, we obtain $w = y + w$, for all real y and complex w. In particular, by (cnre), every complex number has the form bi for some $b \in \mathbb{R}$. Since there are at least two reals, there are at least two choices of $b \in \mathbb{R}$ such that $bi \in \mathbb{R}$. Hence, we can choose such a b so that $b \neq 0$. Then, $i = b^{-1}bi \in \mathbb{R}$. So, from $i^2 + 1 = 0$, we obtain $1 = 0$, a contradiction.

Further, we claim that $0z = 0$ for all $z \in \mathbb{C}$. To prove this, by writing $z = a + bi$ with a, $b \in \mathbb{R}$, we see that $0z = 0 + 0i$, for all $z \in \mathbb{C}$. When z is real, we know also that $0z = 0$. Thus $0 + 0i = 0$ and $0z = 0$ for all $z \in \mathbb{C}$.

Now we complete the proof of (0id). There exists $c \in \mathbb{R}$ with $1 + c = 0$. Then, $1 + c + 0 = 0 + 0 = 0 = 1 + c$, and applying Lemma 3.5, we obtain $c + 0 = c$. If $c \neq 0$, then, for any $z \in \mathbb{C}$, we may multiply by $c^{-1}z$ to obtain $z + 0 = z$, and we are done. So, suppose that $c = 0$. Then, $1 + 0 = 0$. Multiplying by z, we find that $z + 0 = 0$ for all $z \in \mathbb{C}$. From (i2m1), we have $i^2 + 1 = 0$, so by adding i^4 on the left, we obtain $i^4 + i^2 + 1 = 0$. Then,

$$0 + 0 = 0 = i^4 + i^2 + 1 = i^2(i^2 + 1) + 1 = 0 + 1,$$

and applying Lemma 3.5, we obtain $0 = 1$, a contradiction.

Deduction of (addcom): By Lemma 3.4, we find that $\mathbb{R}$ is a group under addition. Then, we may prove (negex) as in Lemma 3.2. By applying Lemma 3.4 again, $\mathbb{C}$ is a group under addition. By Lemma 3.3, we deduce (addcom).

Now we know that $\mathcal{C}_3 \vdash \mathcal{C}_2$, so by Lemma 3.2, we are done. □

3.4 Other reductions from $\mathcal{C}_1$

Here we present various reductions from $\mathcal{C}_1$. These arguments do not allow us to simplify $\mathcal{C}_3$ even further, since they use axioms not contained in that system. Combined with some of the independence results of Section 4, this shows that there are multiple, mutually exclusive ways to simplify $\mathcal{C}_1$.

Lemma 3.8. (mulrcl) *is derivable from* $\mathcal{C}_1 -$ (mulrcl)*.*

Proof. If $0 < 1$, then by adding 1 to both sides, we obtain $1 < 2$. Similarly if $1 < 0$, then $2 < 1$. Thus, $2 \neq 0$. We claim that if $x \in \mathbb{R}$, then $x/2 \in \mathbb{R}$. This is immediate if $x = 0$, and for $x \neq 0$, this follows from the identity $x/2 = (x^{-1} + x^{-1})^{-1}$. We claim next that if $x \in \mathbb{R}$, then $x^2 \in \mathbb{R}$. This is obvious if $x = 0$ or $x = 1$, and in other cases this follows from the identity $x^{-1} + (1 - x)^{-1} = (x - x^2)^{-1}$. Finally, for any x, $y \in \mathbb{R}$, the identity $xy = ((x + y)^2 - x^2 - y^2)/2$ shows that $xy \in \mathbb{R}$. □

Lemma 3.9. *The system* $\mathcal{C}_1 -$ (negex) $-$ (rnegex) *is logically equivalent to* $\mathcal{C}_1$*.*

Proof. Deduction of (negex): First, for any $x \in \mathbb{R}$, we have $0x = (0 + 0)x = 0x + 0x$, and so by Lemma 3.5, we have $0x = 0$. Now, using (cnre), write $a + bi = 0$ for some $a, b \in \mathbb{R}$. Multiplying this equation by 0, we obtain $0i = 0$. From this we see that $0z = 0$ for all $z \in \mathbb{C}$. Thus, we have $z + zi^2 = z(1 + i^2) = z0 = 0$, so (negex) follows.

Deduction of (rnegex): As $-a = (-1)a$ for any a, it suffices to show that $-1 \in \mathbb{R}$. If $i \in \mathbb{R}$, this is immediate, so suppose that $i \notin \mathbb{R}$. Write $a + bi = -1$ for some $a, b \in \mathbb{R}$. Then, $bi = (1 + a)i^2$. So, by cancelling, $b = (1 + a)i$. This implies that $a = -1$, for otherwise we would have $i = b/(1 + a)$, contradicting the assumption that $i \notin \mathbb{R}$. Since $a \in \mathbb{R}$ by hypothesis, we are done. □

Lemma 3.10. *The system* $\mathcal{C}_1 -$ (0id) $-$ (rnegex) *is logically equivalent to* $\mathcal{C}_1$*.*

Proof. By the previous lemma, it suffices to derive (0id). By (negex), there exists $u \in \mathbb{C}$ such that $0 + u = 0$. Then, for any $z \in \mathbb{C}$, $0 + u + z = 0 + z$, and using Lemma 3.5 and (cnre), we may cancel to get $u + z = z$. So we need only show that $u = 0$. To do this, suppose that $u \neq 0$. Then, we may multiply the equation $u + u = u$ by $u^{-1}0$, to obtain $0 + 0 = 0 = 0 + u$. We then cancel to obtain $0 = u$, a contradiction. □

Lemma 3.11. (rrecex) *is derivable from* $\mathcal{C}_1 -$ (rrecex)*.*

Proof. Let A be a model of $\mathcal{C}_1 -$ (rrecex) $-$ (sup). We use the symbols $\mathbb{R}_A$ and $<_A$ to denote, respectively, the real numbers and the ordering relation in A. We use unadorned symbols $\mathbb{C}$, etc., to denote the other components of A. Now, we know that $\mathbb{R}_A$ is an ordered ring, and we want to know that is is an ordered field. Using (mulgt0), we see that $\mathbb{R}_A$ is an integral domain. Let $\mathbb{R}_B$ denote the fraction field of $\mathbb{R}_A$ in $\mathbb{C}$. Suppose we have fractions a/b, $c/d \in \mathbb{R}_B$, where a, b, c, $d \in \mathbb{R}_A$ and b, $d > 0$. Write $a/b <_B c/d$ iff $ad <_A cb$. This makes $\mathbb{R}_B$ into an ordered field. Form a structure B from A by replacing $\mathbb{R}_A$ with $\mathbb{R}_B$ and $<_A$ with $<_B$. Since (cnre) is true in A, it is immediate that is it also true in B. Thus, B is a model of $\mathcal{C}_1 -$ (sup).

Now, by applying Lemma 3.6 to B, we find that any $z \in \mathbb{C}$ has a unique representation in the form $a + bi$ with a, $b \in \mathbb{R}_B$. We will be done if we show that $\mathbb{R}_A = \mathbb{R}_B$. Plainly, $\mathbb{R}_A \subseteq \mathbb{R}_B$. For the other inclusion, suppose that $x \in \mathbb{R}_B$. Then $x + 0i$ is the unique representation of x. But, by applying (cnre) to A, we find that $x = a + bi$ for some a, $b \in \mathbb{R}_A$. It follows that $x = a$, so $x \in \mathbb{R}_A$. Hence $\mathbb{R}_B \subseteq \mathbb{R}_A$. This completes the proof.

□

4 Independence proofs

In this section we present proofs of the independence of various axioms. In each case, in order to prove that a sentence P cannot be derived from a collection $\mathcal{A}$ of axioms, we exhibit a structure $(U; \mathbb{C}_{\mathrm{M}}, \mathbb{R}_{\mathrm{M}}, 0_{\mathrm{M}}, 1_{\mathrm{M}}, i_{\mathrm{M}}, +_{\mathrm{M}}, \cdot_{\mathrm{M}}, <_{\mathrm{M}})$, where U is the universe, that satisfies $\mathcal{A}$ but not P. In what follows, if the universe is a ring, the symbols $+$, $\cdot$, etc., refer to the addition, multiplication, etc., of the universe.

4.1 Axioms independent in $\mathcal{C}_1$

We have shown that a number of the axioms of $\mathcal{C}_1$ are redundant in that system. We now show that most of the rest are not redundant.

Lemma 4.1. (resscn) *cannot be derived from* $\mathcal{C}_1 -$ (resscn)*.*

Proof. Use $(\mathbb{Q}(i); \mathbb{Q}(i), \mathbb{R}, 0, 1, i, +, \cdot, <)$. □

Lemma 4.2. (1cn) *cannot be derived from* $\mathcal{C}_1 -$ (1re)*.*

Proof. Let x and y be distinct objects. Let $+_{\mathrm{M}} = \cdot_{\mathrm{M}}$ be the binary operation on $\{x, y\}$ with constant value x. Use $(\{x, y\}; \{x\}, \{x\}, x, y, x, +_{\mathrm{M}}, \cdot_{\mathrm{M}}, \varnothing)$. □

Lemma 4.3. (icn) *cannot be derived from* $\mathcal{C}_1 -$ (icn)*.*

Proof. Use $(\mathbb{C}; \mathbb{R}, \mathbb{R}, 0, 1, i, +, \cdot, <)$. □

Lemma 4.4. (addcl) *cannot be derived from* $\mathcal{C}_1 -$ (addcl)*.*

Proof. Use $(\mathbb{C}; \mathbb{R} \cup \mathbb{R}i, \mathbb{R}, 0, 1, i, +, \cdot, <)$. □

Lemma 4.5. (addrcl) *cannot be derived from* $\mathcal{C}_1 -$ (addrcl).

Proof. Let $<_{\mathrm{M}}$ be the smallest transitive relation on $\mathbb{F}_5$ such that

$$-2 <_{\mathrm{M}} 1 <_{\mathrm{M}} 0 <_{\mathrm{M}} 1 <_{\mathrm{M}} 2.$$

Use $(\mathbb{F}_5; \mathbb{F}_5, \{-1, 0, 1\}, 0, 1, 2, +, \cdot, <_{\mathrm{M}})$. □

Lemma 4.6. (addass) *cannot be derived from* $\mathcal{C}_1 -$ (addass) $+$ (addrass).

Proof. For any z, $w \in \mathbb{C}$, define

$$z +_{\mathrm{M}} w = \begin{cases} 0 & \text{if } w \neq 0 \text{ and } z/w \in \{1+i, (1+i)^{-1}\}, \\ z + w & \text{otherwise.} \end{cases}$$

Use $(\mathbb{C}; \mathbb{C}, \mathbb{R}, 0, 1, i, +_{\mathrm{M}}, \cdot, <)$. □

Lemma 4.7. (mulass) *cannot be derived from* $\mathcal{C}_1 -$ (mulass) $+$ (mulrass).

Proof. Let $\mathcal{B}_{\mathrm{r}}$ be a basis for $\mathbb{R}$ as a $\mathbb{Q}$-vector space, chosen so that $1 \in \mathcal{B}_{\mathrm{r}}$. Extend $\mathcal{B}_{\mathrm{r}}$ to a basis $\mathcal{B}$ for $\mathbb{C}$ as a $\mathbb{Q}$-vector space, chosen so that $i \in \mathcal{B}$. For each integer $n \geq 0$, we will define a partial map ϕ_n on $\mathcal{B} \times \mathcal{B}$. After this, we will define multiplication of elements of $\mathcal{B}$ in such a way so that $\alpha \cdot_{\mathrm{M}} \beta = \phi_n(\alpha, \beta)$ whenever (a, b) is in the domain of ϕ_n. Finally, we will extend the definition of multiplication to all complex numbers by requiring that it be bilinear.

We define ϕ_0 as follows. For any $\alpha, \beta \in \mathcal{B}_{\mathrm{r}}$, let $\phi_0(\alpha, \beta) = \alpha\beta$. Additionally, for any $\alpha \in \mathcal{B}$, let $\phi_0(\alpha, 1) = \phi_0(1, \alpha) = \alpha$, and, for $\alpha \in \mathcal{B}_{\mathrm{r}} \cup \{i\}$, let $\phi_0(\alpha, i) = \phi_0(i, \alpha) = \alpha i$. The effect of these definitions will be to ensure that $x \cdot_{\mathrm{M}} y = xy$ for x, $y \in \mathbb{R}$, that $z \cdot_{\mathrm{M}} 1 = z$ for $z \in \mathbb{C}$, and that $z \cdot_{\mathrm{M}} i = zi$ for $z \in \mathbb{R} \cup \{i\}$.

Next, we will define ϕ_n for each $n \geq 1$ in such a way as to ensure that each nonzero complex number has a multiplicative inverse. Let $\{\mathcal{B}_n\}_{n \geq 1}$ be a partition of $\mathcal{B}$ such that all the $\mathcal{B}_n$, for $n \geq 1$, have the same (infinite) cardinality. (This will be the cardinality of the continuum, but we do not need that fact for this proof.) Also, choose this partition so that $\mathcal{B}_{\mathrm{r}} \cup \{i\} \subseteq \mathcal{B}_1$. For each $n \geq 1$, let $\mathcal{A}_n = \bigcup_{i=1}^n \mathcal{B}_i$, and choose bijections $f_n : \operatorname{span}_{\mathbb{Q}}(\mathcal{A}_n) \longrightarrow \mathcal{B}_{n+1}$.

Fix n, and consider some $z \in \operatorname{span}_{\mathbb{Q}}(\mathcal{A}_n)$ such that $z \notin \mathbb{R}$. Write $z = q + p_1\alpha_1 + \cdots + p_m\alpha_m$ with $p_1, \ldots, p_m \in \mathbb{Q} \setminus \{0\}$, $q \in \mathbb{Q}$, and $\alpha_1, \ldots, \alpha_m \in \mathcal{A}_n \setminus \{1\}$. Let

$$\phi_n(\alpha_1, f_n(z)) = \phi_n(f_n(z), \alpha_1) = \frac{1 - qf_n(z)}{p_1}.$$

For $2 \leq i \leq m$, let $\phi_n(\alpha_i, f_n(z)) = \phi_n(f_n(z), \alpha_i) = 0$. Thus, we will ensure that $z \cdot_{\mathrm{M}} f_n(z) = 1$ for all nonreal $z \in \operatorname{span}_{\mathbb{Q}}(\mathcal{A}_n)$. Since every z is in $\operatorname{span}_{\mathbb{Q}}(\mathcal{A}_n)$ for some n, we have guaranteed the existence of multiplicative inverses.

Now we define $\cdot_{\mathrm{M}} : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C}$ as follows. For α, $\beta \in \mathcal{B}$, if there is some (necessarily unique) n for which (α, β) is in the domain of ϕ_n, let $\alpha \cdot_{\mathrm{M}} \beta = \phi_n(\alpha, \beta)$. Otherwise, let $\alpha \cdot_{\mathrm{M}} \beta = 0$. Extend $\cdot_{\mathrm{M}}$ to $\mathbb{C} \times \mathbb{C}$ by requiring that it be $\mathbb{Q}$-bilinear. Now, $\cdot_{\mathrm{M}}$ is not associative, for if it were associative, $(\mathbb{C}, +, \cdot_{\mathrm{M}})$ would be a field. Since there exist basis elements whose product is 0 (for instance, any two elements of $\mathcal{B}_n$ for $n > 1$), this is impossible.

To prove the lemma, use $(\mathbb{C}; \mathbb{C}, \mathbb{R}, 0, 1, i, +, \cdot_{\mathrm{M}}, <)$. □

Lemma 4.8. (distr) *cannot be derived from* $\mathcal{C}_1 -$ (distr) $+$ (rdistr).

Proof. For any $z \in \mathbb{C}$, define

$$\phi(z) = \begin{cases} 2+i & \text{if } z = 1+i, \\ 1+i & \text{if } z = 2+i, \\ z & \text{otherwise,} \end{cases}$$

and for any z, $w \in \mathbb{C}$, define

$$z \cdot_{\mathrm{M}} w = \phi^{-1}(\phi(z)\phi(w)).$$

Use $(\mathbb{C}; \mathbb{C}, \mathbb{R}, 0, 1, i, +, \cdot_{\mathrm{M}}, <)$. □

Lemma 4.9. (1ne0) *cannot be derived from* $\mathcal{C}_1 - $ (1ne0).

Proof. Let U be the ring with one element. Use $(U; U, U, 0, 0, 0, +, \cdot, \varnothing)$. □

Lemma 4.10. (1id) *cannot be derived from* $\mathcal{C}_1 - $ (1id).

Proof. Use $(\mathbb{C}; \mathbb{C}, \mathbb{R}, 0, 2, i\sqrt{2}, +, \cdot, <)$. □

Lemma 4.11. (i2m1) *cannot be derived from* $\mathcal{C}_1 - $ (i2m1).

Proof. Use $(\mathbb{C}; \mathbb{C}, \mathbb{R}, 0, 1, 2i, +, \cdot, <)$. □

Lemma 4.12. (cnre) *cannot be derived from* $\mathcal{C}_1 - $ (cnre).

Proof. Use $(\mathbb{C}(x); \mathbb{C}(x), \mathbb{R}, 0, 1, i, +, \cdot, <)$. □

Lemma 4.13. (lttri) *cannot be derived from* $\mathcal{C}_1 - $ (lttri).

Proof. Use $(\mathbb{C}; \mathbb{C}, \mathbb{R}, 0, 1, i, +, \cdot, \varnothing)$. □

Lemma 4.14. (lttrn) *cannot be derived from* $\mathcal{C}_1 - $ (lttrn).

Proof. For any a, $b \in \mathbb{F}_3$, write $a <_{\mathrm{M}} b$ iff $b - a = 1$. Let i_{M} denote a square root of -1 in $\mathbb{F}_9$. Use $(\mathbb{F}_9; \mathbb{F}_9, \mathbb{F}_3, 0, 1, i_{\mathrm{M}}, +, \cdot, <_{\mathrm{M}})$. □

Lemma 4.15. (ltadd) *cannot be derived from* $\mathcal{C}_1 - $ (ltadd).

Proof. For any $x \in \mathbb{R}$, define

$$\phi(x) = \begin{cases} 1-x & \text{if } 0 < x < 1, \\ x & \text{otherwise.} \end{cases}$$

For x, $y \in \mathbb{R}$, write $x <_{\mathrm{M}} y$ iff $\phi(x) < \phi(y)$. Use $(\mathbb{C}; \mathbb{C}, \mathbb{R}, 0, 1, i, +, \cdot, <_{\mathrm{M}})$. □

Lemma 4.16. (mulgt0) *cannot be derived from* $\mathcal{C}_1 - $ (mulgt0).

Proof. Use $(\mathbb{C}; \mathbb{C}, \mathbb{R}, 0, 1, i, +, \cdot, >)$. □

Lemma 4.17. (sup) *cannot be derived from* $\mathcal{C}_1 - $ (sup).

Proof. Use $(\mathbb{Q}(i); \mathbb{Q}(i), \mathbb{Q}, 0, 1, i, +, \cdot, <)$. □

4.2 Other sets of independent axioms

We now provide examples of sets of axioms that cannot be simultaneously removed from $\mathcal{C}_1$ even though the individual axioms are redundant (or their status is unknown).

Lemma 4.18. *Neither* (mulcl) *nor* (recex) *can be derived from* $\mathcal{C}_1 -$ (mulcl) $-$ (recex)*.*

Proof. Use $(\mathbb{C}; \mathbb{R} + \mathbb{Z}i, \mathbb{R}, 0, 1, i, +, \cdot, <)$. □

Lemma 4.19. *Neither* (mulrcl) *nor* (1re) *can be derived from* $\mathcal{C}_1 -$ (mulrcl) $-$ (1re) $+$ (1cn)*.*

Proof. For z, $w \in \mathbb{C}$, write $z <_{\mathrm{M}} w$ iff $[(z, w \in \mathbb{R}i$ and $z/i < w/i)$ or $(z = 0,\ w \in \mathbb{R}$, and $w < 0)]$. Use $(\mathbb{C}; \mathbb{C}, \mathbb{R}i, 0, 1, i, +, \cdot, <_{\mathrm{M}})$. □

Lemma 4.20. *Neither* (recex) *nor* (rrecex) *can be derived from* $\mathcal{C}_1 -$ (recex) $-$ (rrecex)*.*

Proof. Use $(\mathbb{Z}[i]; \mathbb{Z}[i], \mathbb{Z}, 0, 1, i, +, \cdot, <)$. □

Lemma 4.21. *Neither* (0id)*,* (negex)*, nor* (rnegex) *can be derived from* $\mathcal{C}_1 -$ (0id) $-$ (negex) $-$ (rnegex)*.*

Proof. Let $\mathbb{C}_{\mathrm{M}} = \mathbb{R}_{\mathrm{M}}$ denote the set of positive real numbers. Use $(\mathbb{R}; \mathbb{C}_{\mathrm{M}}, \mathbb{R}_{\mathrm{M}}, 2, 1, 1, +, \cdot, <)$. □

5 Conclusion

The results of Sections 3 and 4 prove the following.

Theorem. *System $\mathcal{C}_3$ is logically equivalent to $\mathcal{C}_1$. Moreover, every axiom of $\mathcal{C}_3$, with the possible exception of* (mulcom)*, is independent of the others.*

There remain a number of open questions. Most interesting would be to determine whether (mulcom) is redundant in $\mathcal{C}_3$. Additionally, it is not known whether (mulcl) or (mulcom) are redundant in $\mathcal{C}_1$.