FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 143–150, 2023
DOI: 10.2478/forma-2023-0013
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Embedding Principle for Rings and Abelian Groups

Yasushige Watase
Suginami-ku Matsunoki 6, 3-21 Tokyo
Japan

Summary. The article concerns about formalizing a certain lemma on embedding of algebraic structures in the Mizar system, claiming that if a ring A is embedded in a ring B then there exists a ring C which is isomorphic to B and includes A as a subring. This construction applies to algebraic structures such as Abelian groups and rings.

MSC: 13B25 68V20

Keywords: Abelian group; ring; embedding

MML identifier: RING_EMB, version: 8.1.14 5.76.1452

Introduction

The article concerns about formalizing a certain lemma on embedding of algebraic structures in the Mizar system [2], [3], along with the lemma appeared in the book [12] at §13 of Chapter 1. The lemma claims that if a ring A is embedded in a ring B then there exists a ring C which is isomorphic to B and includes A as a subring [11]. A basic idea to prove the lemma is that for given monomorphism φ from A to B, one can obtain such ring C by introducing the addition and multiplication on the set $(B \setminus \varphi(A)) \cup A$, while B does not meet A. The same argument has already been discussed and formalized in [9] in line with field extensions [10] (recently reused to formalize algebraic closures, see e.g. [8]).

We treat here a general case, namely the case of B meets A, it is enough to create a set X which does not meet A and $X \cong B \setminus \varphi(A)$ and construct a new ring C from the set $(X \cong B \setminus \varphi(A)) \cup A$. The formalized lemma can be applied to another algebraic structures such as Abelian groups as shown in the article as well with the same formulation of rings [6].

We need the following 3 steps required for precise arguments and formalization to construct the target object C:

Step 1. Prepare a set X which does not meet A and isomorphic to $B \setminus \varphi(A)$ as set-theoretical. The step is coded in Theorem 1 and 2;

Step 2. Make a $X \setminus S$ a ring as C, corresponds to Theorem 7 and 12 for rings and for Abelian groups, respectively;

Step 3. Construct an isomorphism $G : A \xrightarrow{\sim} C$ such that $\iota = G \circ \varphi$ is an identity mapping. Corresponding formal counterparts are Theorem 9 and 14 for rings and for Abelian groups, respectively.

As a consequence of the principle, taking Polynom-Ring(A) as B, we have a polynomial ring over A with indeterminate X and includes A as a subring, say $A[X] = C$. Here Polynom-Ring(A) is existing formalized ring of polynomials [4], which is constructed by sequences. An indeterminate X is defined by the image of $(0, 1, 0, 0, \cdots) \in$ Polynom-Ring(A) by the map G of Step 3. Some of the Mizar functors had to be defined additionally as we used the groups not in their multiplicative version [1], [7], which is more common in the Mizar Mathematical Library, but in the additive setting [5].

1. Preliminaries from Set Theory

From now on a denotes a non empty set and b, x, o denote objects.

Now we state the propositions:

(1) There exists an object b such that for every set x, $\langle x, b \rangle \notin a$.

(2) Let us consider non empty sets a, b. Then there exists a non empty set c such that

(i) $a \cap c = \emptyset$, and

(ii) there exists a function f such that f is one-to-one and $\operatorname{dom} f = b$ and $\operatorname{rng} f = c$.

Proof: Consider d being an object such that for every set x, $\langle x, d \rangle \notin a$. Set $C = b \times \{d\}$. Consider f being a function such that f is one-to-one and $\operatorname{dom} f = b$ and $\operatorname{rng} f = C$. $a \cap C = \emptyset$. $\square$

2. Embedding Principle Applied to Rings

Now we state the proposition:

(3) Let us consider a ring A, a non empty set X, a function f from A into X, and elements a, b of X. Suppose f is bijective. Then $f(($the addition of $A)((f^{-1})(a), (f^{-1})(b)))$ is an element of X.

Let A be a ring, X be a non empty set, f be a function from A into X, and a, b be elements of X. Assume f is bijective. The functor addemb(f, a, b) yielding an element of X is defined by the term

(Def. 1) $f(($the addition of $A)((f^{-1})(a), (f^{-1})(b)))$.

Now we state the proposition:

(4) Let us consider a ring A, a non empty set X, a function f from A into X, and elements a, b, c of X. Suppose f is bijective. Then addemb$(f, a,$ addemb $(f, b, c))$ = addemb$(f,$ addemb$(f, a, b), c)$.

Let A be a ring, X be a non empty set, and f be a function from A into X. The functor addemb(f) yielding a binary operation on X is defined by

(Def. 2) for every elements a, b of X, $it(a, b)$ = addemb(f, a, b).

Now we state the proposition:

(5) Let us consider a ring A, a non empty set X, a function f from A into X, and elements a, b of X. Suppose f is bijective. Then $f(($the multiplication of $A)((f^{-1})(a), (f^{-1})(b)))$ is an element of X.

Let A be a ring, X be a non empty set, f be a function from A into X, and a, b be elements of X. Assume f is bijective. The functor multemb(f, a, b) yielding an element of X is defined by the term

(Def. 3) $f(($the multiplication of $A)((f^{-1})(a), (f^{-1})(b)))$.

The functor multemb(f) yielding a binary operation on X is defined by

(Def. 4) for every elements a, b of X, $it(a, b)$ = multemb(f, a, b).

The functor embRing(f) yielding a strict, non empty double loop structure is defined by the term

(Def. 5) $\langle X,$ addemb$(f),$ multemb$(f), f(1_A), f(0_A)\rangle$.

Now we state the propositions:

(6) Let us consider a ring A, a non empty set X, and a function f from A into X. If f is bijective, then embRing(f) is a ring.

PROOF: Reconsider $Z_1 = \langle X,$ addemb$(f),$ multemb$(f), f(1_A), f(0_A)\rangle$ as a non empty double loop structure. For every elements v, w of Z_1, $v+w = w+v$. For every elements u, v, w of Z_1, $u+(v+w) = (u+v)+w$. For every element v of Z_1, $v+0_{Z_1} = v$. Every element of Z_1 is right complementable. For every elements a, b, v of Z_1, $(a+b)\cdot v = a\cdot v+b\cdot v$. For every elements

a, b, v of Z_1, $v \cdot (a + b) = v \cdot a + v \cdot b$ and $(a + b) \cdot v = a \cdot v + b \cdot v$. For every elements a, b, v of Z_1, $(a \cdot b) \cdot v = a \cdot (b \cdot v)$. For every element v of Z_1, $v \cdot (1_{Z_1}) = v$ and $1_{Z_1} \cdot v = v$. □

(7) Let us consider a commutative ring A, a non empty set X, and a function f from A into X. If f is bijective, then $\mathrm{embRing}(f)$ is a commutative ring.
PROOF: $\mathrm{embRing}(f)$ is commutative. □

(8) Let us consider rings A, B, and a function i from A into B. Suppose i inherits ring homomorphism and $i = \mathrm{id}_A$. Then A is a subring of B.
PROOF: For every object o such that $o \in$ the carrier of A holds $o \in$ the carrier of B. The addition of $A =$ (the addition of B) $\restriction$ (the carrier of A). The multiplication of $A =$ (the multiplication of B) $\restriction$ (the carrier of A). □

(9) Let us consider rings A, B, and a function f from A into B. Suppose f is monomorphic and $\Omega_B \setminus (\mathrm{rng}\, f) \neq \emptyset$. Then there exists a ring C and there exists a set X and there exists a function h and there exists a function G from B into C such that $X \cap \Omega_A = \emptyset$ and h is one-to-one and $\mathrm{dom}\, h = \Omega_B \setminus (\mathrm{rng}\, f)$ and $\mathrm{rng}\, h = X$ and $\Omega_C = X \cup \Omega_A$ and A is a subring of C and G inherits ring isomorphism and $\mathrm{id}_A = G \cdot f$.
PROOF: Consider X being a non empty set such that $\Omega_A \cap X = \emptyset$ and there exists a function h such that h is one-to-one and $\mathrm{dom}\, h = \Omega_B \setminus (\mathrm{rng}\, f)$ and $\mathrm{rng}\, h = X$. Consider h being a function such that h is one-to-one and $\mathrm{dom}\, h = \Omega_B \setminus (\mathrm{rng}\, f)$ and $\mathrm{rng}\, h = X$ and $\Omega_A \cap X = \emptyset$.

Define $\mathcal{P}[\text{element of } B, \text{element of } \Omega_A \cup X] \equiv \$_1 \in \mathrm{rng}\, f$ and $(f^{-1})(\$_1) = \$_2$ or $\$_1 \notin \mathrm{rng}\, f$ and $\$_2 = h(\$_1)$. Set $C_1 = \Omega_A \cup X$. Consider g being a function from the carrier of B into C_1 such that for every element x of B, $\mathcal{P}[x, g(x)]$. g is bijective. Reconsider $C = \mathrm{embRing}(g)$ as a non empty ring. Reconsider $G = g$ as a function from B into C. G is linear. For every o such that $o \in \Omega_A$ holds $(G \cdot f)(o) = o$. A is a subring of C. □

3. Embedding Principle Applied to Abelian Groups

Let G be an Abelian group. A subgroup of G is an Abelian group defined by

(Def. 6) the carrier of *it* $\subseteq$ the carrier of G and the addition of *it* $=$ (the addition of G) $\restriction$ (the carrier of *it*) and $0_{it} = 0_G$.

Let G, H be Abelian groups and f be a homomorphism from G to H. The functor $\mathrm{Im}\, f$ yielding a strict additive loop structure is defined by

(Def. 7) the carrier of *it* $= \mathrm{rng}\, f$ and the addition of *it* $=$ (the addition of H) $\restriction$ $\mathrm{rng}\, f$ and the zero of *it* $= 0_H$.

Now we state the proposition:

(10) Let us consider an Abelian group A, a non empty set X, a function f from A into X, and elements a, b of X. Suppose f is bijective. Then $f((\text{the addition of } A)((f^{-1})(a), (f^{-1})(b)))$ is an element of X.

Let A be an Abelian group, X be a non empty set, f be a function from A into X, and a, b be elements of X. Assume f is bijective. The functor addemb(f, a, b) yielding an element of X is defined by the term

(Def. 8) $f((\text{the addition of } A)((f^{-1})(a), (f^{-1})(b)))$.

Now we state the proposition:

(11) Let us consider an Abelian group A, a non empty set X, a function f from A into X, and elements a, b, c of X. Suppose f is bijective. Then $\text{addemb}(f, a, \text{addemb}(f, b, c)) = \text{addemb}(f, \text{addemb}(f, a, b), c)$.

Let A be an Abelian group, X be a non empty set, and f be a function from A into X. The functor addemb(f) yielding a binary operation on X is defined by

(Def. 9) for every elements a, b of X, $it(a, b) = \text{addemb}(f, a, b)$.

The functor embAbGr(f) yielding a strict, non empty additive loop structure is defined by the term

(Def. 10) $\langle X, \text{addemb}(f), f(0_A)\rangle$.

Now we state the propositions:

(12) Let us consider an Abelian group A, a non empty set X, and a function f from A into X. If f is bijective, then embAbGr(f) is an Abelian group.
PROOF: Reconsider $Z_1 = \langle X, \text{addemb}(f), f(0_A)\rangle$ as a non empty additive loop structure. For every elements v, w of Z_1, $v + w = w + v$. For every elements u, v, w of Z_1, $u + (v + w) = (u + v) + w$. For every element v of Z_1, $v + 0_{Z_1} = v$. Every element of Z_1 is right complementable. □

(13) Let us consider Abelian groups A, B, and a homomorphism i from A to B. If $i = \text{id}_A$, then A is a subgroup of B.
PROOF: For every object o such that $o \in$ the carrier of A holds $o \in$ the carrier of B. The addition of A = (the addition of B) $\restriction$ (the carrier of A). □

(14) Let us consider Abelian groups A, B, and a homomorphism f from A to B. Suppose f is one-to-one and $\Omega_B \setminus (\text{rng} f) \neq \emptyset$. Then there exists an Abelian group C and there exists a set X and there exists a function h and there exists a function G from B into C such that $X \cap \Omega_A = \emptyset$ and h is one-to-one and $\text{dom} h = \Omega_B \setminus (\text{rng} f)$ and $\text{rng} h = X$ and $\Omega_C = X \cup \Omega_A$ and A is a subgroup of C and G is a homomorphism from B to C and $\text{id}_A = G \cdot f$.
PROOF: Consider X being a non empty set such that $\Omega_A \cap X = \emptyset$ and there

exists a function h such that h is one-to-one and $\operatorname{dom} h = \Omega_B \setminus (\operatorname{rng} f)$ and $\operatorname{rng} h = X$. Consider h being a function such that h is one-to-one and $\operatorname{dom} h = \Omega_B \setminus (\operatorname{rng} f)$ and $\operatorname{rng} h = X$ and $\Omega_A \cap X = \emptyset$. Define $\mathcal{P}[$element of $B,$ element of $\Omega_A \cup X] \equiv \$_1 \in \operatorname{rng} f$ and $(f^{-1})(\$_1) = \$_2$ or $\$_1 \notin \operatorname{rng} f$ and $\$_2 = h(\$_1)$. Set $C_1 = \Omega_A \cup X$.

Consider g being a function from the carrier of B into C_1 such that for every element x of B, $\mathcal{P}[x, g(x)]$. g is bijective. Reconsider $C = \operatorname{embAbGr}(g)$ as a non empty Abelian group. Reconsider $G = g$ as a function from B into C. G is additive. For every o such that $o \in \Omega_A$ holds $(G \cdot f)(o) = o$. A is a subgroup of C. □

4. Relation with Polynomial Rings

Now we state the proposition:

(15) Let us consider a bag b of 0. Then

(i) $\operatorname{dom} b = \emptyset$, and

(ii) $b = \operatorname{EmptyBag} \emptyset$, and

(iii) $\operatorname{rng} b = 0$, and

(iv) $\operatorname{EmptyBag} \emptyset = \emptyset \longmapsto 0$, and

(v) $\operatorname{Bags} \emptyset = \{\operatorname{EmptyBag} \emptyset\}$.

From now on R denotes a right zeroed, add-associative, right complementable, Abelian, well unital, distributive, associative, non trivial, non trivial double loop structure. Now we state the propositions:

(16) Let us consider a polynomial f of $0,R$. Then

(i) $\operatorname{dom} f = \operatorname{Bags} 0$, and

(ii) $\operatorname{Bags} 0 = \{\emptyset\}$, and

(iii) $\operatorname{rng} f = \{f(\operatorname{EmptyBag} 0)\}$.

The theorem is a consequence of (15).

(17) Every polynomial of $0,R$ is constant.

(18) Let us consider a polynomial f of $0,R$. Then there exists an element a of R such that $f = a \restriction (0, R)$. The theorem is a consequence of (17).

Let us consider R. The functor $1\_1(R)$ yielding a sequence of R is defined by the term

(Def. 11) $\mathbf{0}.R +\cdot (1, 1_R)$.

Now we state the proposition:

(19) Let us consider a non degenerated commutative ring R.
Then Support $1\_1(R) = \{1\}$.
Proof: For every o such that $o \in$ Support $1\_1(R)$ holds $o \in \{1\}$. For every o such that $o \in \{1\}$ holds $o \in$ Support $1\_1(R)$. □

Let us consider R. One can verify that $1\_1(R)$ is finite-Support. Now we state the propositions:

(20) Leading-Monomial $1\_1(R) = 1\_1(R)$.

(21) Let us consider an element m of R. Then $\mathrm{eval}(1\_1(R), m) = m$. The theorem is a consequence of (20).

In the sequel R denotes a non degenerated commutative ring. Now we state the propositions:

(22) Let us consider an element p_0 of Polynom-Ring$(0, R)$. Then p_0 is not a polynomial over Polynom-Ring$(0, R)$.

(23) Let us consider a non degenerated commutative ring R.
Then Polynom-Ring Polynom-Ring$(0, R)$ and Polynom-Ring$(1, R)$ are isomorphic.

Let us consider a non degenerated ring R. Now we state the propositions:

(24) $\Omega_{\text{Polynom-Ring}\,R} \setminus (\mathrm{rng}(R \overset{\text{canHom}}{\hookrightarrow} \text{Polynom-Ring}\,R)) \neq \emptyset$.

(25) There exists a non degenerated ring P_1 and there exists a set X and there exists a function h and there exists a function G from Polynom-Ring R into P_1 such that R is a subring of P_1.

And G inherits ring isomorphism and $\mathrm{id}_R = G\cdot(R \overset{\text{canHom}}{\hookrightarrow} \text{Polynom-Ring}\,R)$ and $X \cap \Omega_R = \emptyset$ and h is one-to-one and $\mathrm{dom}\,h = \Omega_{\text{Polynom-Ring}\,R} \setminus (\mathrm{rng}(R \overset{\text{canHom}}{\hookrightarrow} \text{Polynom-Ring}\,R))$ and $\mathrm{rng}\,h = X$ and $\Omega_{P_1} = X \cup \Omega_R$. The theorem is a consequence of (24) and (9).

(26) $\Omega_{\text{Polynom-Ring}(0,R)} \cap \Omega_{\text{Polynom-Ring Polynom-Ring}(0,R)} = \emptyset$. The theorem is a consequence of (22).

(27) Let us consider a non degenerated ring R. Then there exists a non degenerated ring P_1 and there exists a set X and there exists a function h and there exists a function G from Polynom-Ring Polynom-Ring$(0, R)$ into P_1 such that Polynom-Ring$(0, R)$ is a subring of P_1.

And G inherits ring isomorphism and $\mathrm{id}_{\text{Polynom-Ring}(0,R)} = G\cdot(\text{Polynom-Ring}(0, R) \overset{\text{canHom}}{\hookrightarrow} \text{Polynom-Ring Polynom-Ring}(0, R))$ and $X \cap \Omega_{\text{Polynom-Ring}(0,R)} = \emptyset$ and h is one-to-one and $\mathrm{dom}\,h = \Omega_{\text{Polynom-Ring Polynom-Ring}(0,R)} \setminus (\mathrm{rng}(\text{Polynom-Ring}(0, R) \overset{\text{canHom}}{\hookrightarrow} \text{Polynom-Ring Polynom-Ring}(0, R)))$ and $\mathrm{rng} h = X$ and $\Omega_{P_1} = X \cup \Omega_{\text{Polynom-Ring}(0,R)}$.

Let us consider R. Let A be an R-monomorphic commutative ring and x be an element of A. We say that x is indeterminate if and only if

(Def. 12) there exists a function g from Polynom-Ring R into A such that g is isomorphism and $x = g(1\_1(R))$.

Now we state the proposition:

(28) Let us consider a non degenerated commutative ring R. Then there exists an element X of Polynom-Ring R such that

(i) X is indeterminate, and

(ii) $X = 1\_1(R)$.

References

[1] Michael Francis Atiyah and Ian Grant Macdonald. *Introduction to Commutative Algebra*, volume 2. Addison-Wesley Reading, 1969.

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[3] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[4] Edward J. Barbeau. *Polynomials.* Springer, 2003.

[5] Adam Grabowski and Christoph Schwarzweller. On duplication in mathematical repositories. In Serge Autexier, Jacques Calmet, David Delahaye, Patrick D. F. Ion, Laurence Rideau, Renaud Rioboo, and Alan P. Sexton, editors, *Intelligent Computer Mathematics, 10th International Conference, AISC 2010, 17th Symposium, Calculemus 2010, and 9th International Conference, MKM 2010, Paris, France, July 5–10, 2010. Proceedings*, volume 6167 of *Lecture Notes in Computer Science*, pages 300–314. Springer, 2010. doi:10.1007/978-3-642-14128-7_26.

[6] Adam Grabowski, Artur Korniłowicz, and Christoph Schwarzweller. On algebraic hierarchies in mathematical repository of Mizar. In M. Ganzha, L. Maciaszek, and M. Paprzycki, editors, *Proceedings of the 2016 Federated Conference on Computer Science and Information Systems (FedCSIS)*, volume 8 of *Annals of Computer Science and Information Systems*, pages 363–371, 2016. doi:10.15439/2016F520.

[7] Piotr Rudnicki, Christoph Schwarzweller, and Andrzej Trybulec. Commutative algebra in the Mizar system. *Journal of Symbolic Computation*, 32(1/2):143–169, 2001. doi:10.1006/jsco.2001.0456.

[8] Christoph Schwarzweller. Existence and uniqueness of algebraic closures. *Formalized Mathematics*, 30(**4**):281–294, 2022. doi:10.2478/forma-2022-0022.

[9] Christoph Schwarzweller. On monomorphisms and subfields. *Formalized Mathematics*, 27(**2**):133–137, 2019. doi:10.2478/forma-2019-0014.

[10] Christoph Schwarzweller and Agnieszka Rowińska-Schwarzweller. Algebraic extensions. *Formalized Mathematics*, 29(**1**):39–48, 2021. doi:10.2478/forma-2021-0004.

[11] Yasushige Watase. Ring of endomorphisms and modules over a ring. *Formalized Mathematics*, 30(**3**):211–221, 2022. doi:10.2478/forma-2022-0016.

[12] Oscar Zariski and Pierre Samuel. *Commutative Algebra I.* Springer, 2nd edition, 1975.

Accepted November 21, 2023