A Free Magma, Semigroup, Monoid, and Group

Ko Bong-soo

자유마그마, 자유반군, 단위적 반군과 군에 관한 연구

高 鳳 秀

Ⅰ. Introduction

A magma is a set with a binary operation. Some informations of a magma are in Bourbaki. And informations of semigroups, monoids, and groups are well-known. Futhermore, we can easily construct a free abelian group on any set X.

In this paper, I am going to construct a free magma on X which is not a semigroup and to make a free semigroup on X by using an associative congruence relation on the free magma. The free semigroup is not necessarily monoid. By adding a new element in the free semigroup, I am also going to form a free monoid which is not necessarily a group. Finally, by using a congruence relation on the free magma, I intend to set a free group on X which is not necessarily abelian, and then to build a free abelian group.

Ⅱ. A free magma

Given set X, let $X_1=X$, $X_n=\bigsqcup_{p=1}^{n-1}(X_p\times X_{n-p})$ for all positive integer n, and $M(X)=\bigsqcup_{n=1}^{\infty} X_n$. For any $a\in M(X)$, we write $l(a)=n$ if $a\in x_n$. If a, $b\in M(X)$, $l(a)=p$, $l(b)=q$, and $p+q=n$, and we define $\mu(a, b)=(a,b)\in X_n$, then $\mu: M(X)\times M(X)\rightarrow M(X)$ is a well-defined map, and so $(M(X), \mu)$ is a magma. The following theorem tells us M(X) is a gree magma on X.

Theorem Ⅰ. Let X be a set, (S, m) be a magma, and $f: X\rightarrow(S, m)$ be a function. then there exists a unique magma homomorphism $\hat{f}:(M(x), \mu)\rightarrow(S, m)$ such that $\hat{f}(x)=f(x)$ if $x\in X$ (i.e. $\hat{f}$ is a magma homomorphism if $\hat{f}(\mu(a, b))=m(\hat{f}(a), \hat{f}(b))$.

Proof) First, I find a magma homomorphism $\hat{f}:(M(x), \mu)\rightarrow(S, m)$ such taht $\hat{f}(x)=f(x)$.

Let $f_1: X_1\rightarrow(S, m)$ be a map with $f_1(x)=f(x)$, and $f_n: X_n\rightarrow(S, m)$ be a map which if $a\in X_p$, $b\in X_{n-p}$, and $1\leq p\leq n-1$, then $f_n(a, b)=m(f_p(a), f_{n-p}(b))$. Then we can define the function $\hat{f}$ given by $\hat{f}(c)=f_n(c)$ if $l(c)=n$. The map $\hat{f}$ is a magma homomorphim : Because if a, $b\in M(x)$, $l(a)=p$, $l(b)=q$, and $p+q=n$, then $\hat{f}(\mu(a, b))=\hat{f}((a, b))=f_n(a, b)=m(f_p(a), \hat{f}_q(b))=m(\hat{f}(a), \hat{f}(b))$.

Second, I show uniqueness of $\hat{f}$. Assume $g: M(X)\rightarrow(S, m)$ is a magma homomorphism which $g(x)=f(x)$ for all $x\in X$ and $\hat{f}\neq g$. Then $\hat{f}(c)\neq g(c)$ for some $c\in M(X)$. Let $l(c)=n$. If $n=1$, then $g(c)=f(c)=\hat{f}(c)$. So $n\rangle 1$. Let $C=(a, b)$, $l(a)=p\langle n$, and $l(b)=q\langle n$. Then $g(c)=m(g(a), g(b))$, By induction on n, $g(c)=m(\hat{f}(a), \hat{f}(b))=\hat{f}(\mu(a, b))$. Hence $g(c)=\hat{f}(c)$. This leads to contradiction. Therefore $\hat{f}=g$.

Corollary. If (S, m) is a magma, then there exists a set X and a surjective magma homomorphism $h:(M(x), \mu)\rightarrow(S, m)$.

PROOF. Let X=S as a set and $f: X\rightarrow S$ be identity function. By Theorem I, $h=\hat{f}$.

Ⅲ. A free semigroup

A congruence relation on a magma S is an equivalence relation R such that (ax, ay) ∊ R and (xa, ya) ∊ R for all a ∊ S, (x, y) ∊ R. If S is a magma, then S x S is a congruence relation on S, and if {Ra | a ∊ A} is a collection of congruence relations on S, then $\bigcap_{a\in A}$ Ra is a congruence relation on S.

Theorem Ⅲ. 1. Let R be a congruence relation on a magma (S, m). Then (a) $\bar{m}$: S/R×S/R→S/R defined by $\bar{m}([x]_R, [y]_R)=[m(x, y)]_R$ is a well-defined map, where $[x]_R$ is an equivalence [congruence] class on S.

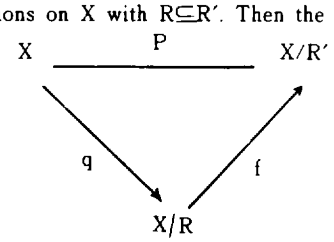
(b) P : (S, m)→(S/R, $\bar{m}$) defined by $p(x)=[x]_R$ is a magma homomorphism.

Proof) The part of (a). Sujppose $[x]_R=[x']_R$ and $[y]_R=[y']_R$. Then (x, x')∊ R and (y, y') ∊ R. Since R is congruent, (xy, x'y)∊ R and(x'y, x'y') ∊ R. Hence (x y, x'y') ∊ R. So$[m(x, y)]_R=[m(x', y')]_R$.

The part of (b). $P(m(x,y))=[\bar{m}([x]_R, [y]_R)=\bar{m}(p(x), p(y))$.

Let S be a magma. A congruence relation R on S is associative if ((ab)c, a(bc)) ∊ R for any a, b, c ∊ S. If R' is an assocoative congruence relation on S, then S/R' is a semigroup under the binary operartion $[x]_{R'}[y]_{R'}=[xy]_{R'}$: Because the operation is welldefined by Theorem Ⅲ. 1.and the associativity holds, for ((ab) c, a(bc)) ∊ R'. Futhermore, if we assume {Ra | a ∊ A} is a collection of associative congruence relations on a magma S, then$R=\bigcap_{a\in A}$ Ra is also an associative congruence relation on S, and so S/R is also a semigroup.

Lemma Let X be a set and R,R' be equivalence relations on X with R⊆R'. Then the diagram.

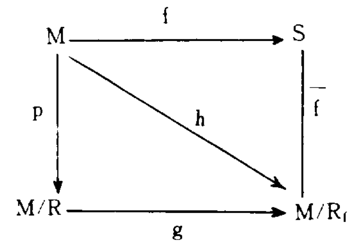


is commutative, where $p(x)=[x]_{R'}$, $q(x)=[x]_R$ and $f([x])_R)=[x]_{R'}$.

PROOF. I show f is well-defined. Suppose $[x]_R=[y]_R$. Then (x, y) ∊ R, So (x, y) ∊ R'. Hence $f([x]_R)=[x]_{R'}=[y]_{R'}=f([y]_R)$.

Theorem Ⅲ. 2. Let M be a magma, R=⋂{R' | R' is an associative congruence relation on M}. Then M / R is a semigroup, and if f : M→S is a magma homomorphism with S a semigroup, then there is a unique semigroup homomorphism f_1 : M/R→S such that $f_1([x]_R)=f(x)$

Proof) Let R_f= {(x, y) | f(x)=f(y), x, y ∊ M}. Then R_f is an associative congruence relation on M and R⊆R_f and then the diagram

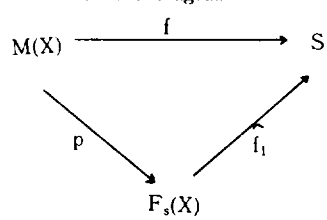


is commutative, where $p(x)=[x]_R$, $g([x]_R)=[x]_{R_f}$, $h(x)=[x]_{R_f}$, and $f([x]_{R_f})=f(x)$. Let $f_1=\hat{f}.g$. We are done.

Let X be a set. Then M(X) is a free magma on X. Let R=⋂{R' | R' is an associative congruence relation on M(X)}. We denote M(X)/R by $F_s(X)$. Then the following theorem inform us that $F_s(x)$ is a free semigroup on X.

Theorem Ⅲ. 3. Let X be a set, S be a semigroup, and f : X→S be a function. Then there exists a unique semigroup homomorphism $\acute{f}$: $F_s(x)$→s such that $\acute{f}$ · j=f, where j=X→ $F_s(X)$ defined by $j(x)=[x]_R$. Moreover, j is one-one.

Proof) By theorem I, there is a unique magma homomorphism $\hat{f}$: M(X)→S such that f(x)=f(x) for all x ∊ X. Then the diagram



is commutative by Theorem Ⅲ. 2. Let $\acute{f}=\hat{f}_1$. Then f is a semigroup homomorphism and $\acute{f}(j(x))=\hat{f}_1([x]_R)=\hat{f}(x)=f(x)$ for all $x \in X$. I show $\hat{f}_1$ is unique. Since $\hat{f}$ is uniquely determined from f and $\hat{f}_1$ uniquely determined by $\acute{f}$, so f is uniquely determined from f. I prove the part of moreover. Let $\hat{X}=X\sqcup\{0\}$. $0\notin X$ and define a map $* : \hat{X}x\hat{X}\rightarrow\hat{X}$ by $a*b=o$ for any $a.b \in \hat{X}$. Then $(\hat{X}.*)$ is a semigroup and $X\subset\hat{X}$. Let $f : X\rightarrow\hat{X}$ be an inclusion map. Then there is a semigroup homomorphism $\acute{f} \cdot F_s(X)\rightarrow\hat{X}$ such that $\acute{f}\cdot j=f$. If $x, x' \in X$, and $j(x)=j(x')$, then $f(j(x))=f(j(x'))$. Then $f(x)=f(x')$ or $x=x'$. So j is one-one.

Corollary. Let X be a set. $X_1=X$. $X_2=X \times X$, ⋯ ⋯, and $X^+=\bigcup_{i=1}^{\infty} X_i$. If $a=(x_1, \cdots\cdots, x_i) \in X_i$ $b=(y_1,\cdots\cdots, y_j) \in X_j$, we define $m : X^+ \times X^+ \rightarrow X^+$ by $m(a, b)=, (x_1\cdots\cdots, x_i, y_1, \cdots\cdots, y_j)$. Then (X^+, m) is a semigroup. The inclusion map $f : X\rightarrow X^+$ extends to a unique semigroup homomorphism $\acute{f} : F_s(X)\rightarrow X^+$ such that $\acute{f}\cdot j=f$. Moreover, $\acute{f}$ is a semigroup isomorphism.

Ⅳ. A free monoid

Let (S. m) be a semigroup and define $S_1=S\sqcup\{e\}$ (where e is a new element not in S), m' : $S_1 \times S_1\rightarrow S_1$ by $m'(e, e)=e$, $m'(e, s)=m(s, e)=s$, and $m'(s, s')=m(s, s')$ if $s, s' \in S$. Then m' is associative on S_1 and e is an identity. So (S_1, m') is a monoid. Let $f : S\rightarrow S'$ is a semigroup homomorphism. Let define $f_1 : S_1\rightarrow S_1'$ by $f_1(e)=e'$ and $f_1(a)=f(a) \in S$. Then f_1 is a monoid homomorphism. Let X be a set. Then $F_s(X)$ is a free semigroup on X. We denote $F_s(X)_1=F_m(X)$. The following theorem tells us $F_s(X)_1$ is a free monoid on X.

Theorem Ⅳ. 1. Let M be a monoid with identity e' and $f : X\rightarrow M$ be a function.Then there is a unique monoid homomorphism $\grave{f} : F_m(x)\rightarrow M$ such tat $\grave{f}\cdot=f$, where $j : X\rightarrow F_s(x)\subseteq F_m(x)$.

Proof) Since M is a semigroup, by Theorem Ⅲ. 3, there is a semigroup homomorphism $\acute{f}$: $F_s(x)\rightarrow M$ such that $f\cdot j=f$. Let $\grave{f} : F_m(x)\rightarrow M$ defined by $\grave{f}(a)=\acute{f}(a)$ if $a \in F_s(x)$ and $\grave{f}(a)=e'$. Then $\grave{f}$ is a monoid homomorphism and $\grave{f}\cdot j=\acute{f}\cdot j=f$. I prove uniqueness of $\grave{f}$. Suppose $g : F_m(x)\rightarrow M$ is a monoid homomorphism with $g\cdot j=f$. Since $F_s(x)\subseteq F_m(x)$ and $g(ab)=g(a)\,g(b)$ for any $a, b \in F_s(x)$, so the restriction of g on $F_s(x)$ is a semigroup homomorphism and $g\cdot j=f$. By uniqueness for $F_s(x)$, we have $g \mid F_s(x)=\acute{f}$. Thus $g(a)=\acute{f}(a)$ for any $a \in F_s(x)$ and $g(e)=e'$. Hence $g=\grave{f}$.

Let S be a monoid with identity e, and B be a subset of S. Let $\langle B\rangle=\{x_1\cdots x_k \mid x_i \in B\sqcup\{e\}, k=1, 2, \cdots\}$. Then $\langle B\rangle$ is a submonoid, we call the submonoid generated by B. We note that if $f : S\rightarrow S'$ is a onto monoid homomprphism, and B generates S, then f(B) generates S'. The following theorem tells us that $F_m(x)$ is a monoid generated by j(x).

Theorem Ⅳ. 2. Let X be a set. Then $F_m(x)$ is generated by j(x)

Proof) Consider $\langle j(x)\rangle=F$ is a submonoid of $F_m(x)$.

Let $K : X\rightarrow F$ defined by $K(x)=j(x)$ for all $x \in X$. From K we get a unique monoid homomorphism $\grave{K} : F_m(x)\rightarrow F$ with $\grave{K}\cdot j=K$. Then $F_m(x)\xrightarrow{\grave{k}} F \xrightarrow{ind} F_m(x)$. $h=incl\cdot\grave{K}$, and $h(j(x))=incl(\grave{K}(j(x)))=j(x)$. So h is a monoid homomorphism from $F_m(x)$ to $F_m(x)$ with $h\cdot j=j$. However, the identity map $id_{Fm}(x)$ is also a monoid homomorphism with $id_{Fm}(x)\cdot j=j$. Since $F_m(x)$ is a free monoid, $h=id_{Fm}(x)$. Hence $F=F_m(x)$.

Ⅴ. A free group

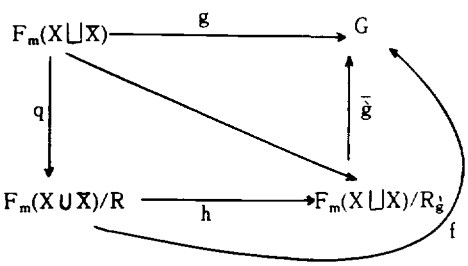
Let X be a set and $\bar{X}$ be a copy of X under $X\rightarrow\bar{X}$ by $x\rightarrow\bar{x}$. Consider $F_m(X\sqcup\bar{X})$. Let $R=\bigcap\{R' \mid R'$ is a congruence relation on $F_m(X\sqcup\bar{X})$ with $(j(x)j(\bar{x}), e) \in R'$ and $(j(\bar{x})\,j(x), e) \in R'\}$. Then R is a congruence relation on $F_m(X\sqcup\bar{X})$and $(j(x)\,j(x), e)\, k \in R$, $(j(x)j(\bar{x}), e) \in R$ for all $x \in X$. Define $F(X)=F_m(X\sqcup\bar{X})/R$, and let $K : X\rightarrow F(X)$ be defined by $K(x)=[j(x)]_R$. Then the following theorem tells us F(X) is a free group on X.

Theorem Ⅴ. Ⅰ. Let G be a group and $f : X\rightarrow G$ be a function. Then there is a unique group homomorphism $\hat{f} : F(x)\rightarrow G$ such that $f\cdot k=f$.

Proof. By Theorem Ⅳ. 2., $j(X\sqcup\bar{X})$ generates $F_m(X\sqcup\bar{X})$. Let the canonical map q : $F_m(X\sqcup\bar{X})\rightarrow F(X)$ be defined by $q(a)=[a]_R$. Since q is onto, so $q(j(X \sqcup \bar{X}))$ qenerates F(X). Let $B = q(j(X \sqcup \bar{X}))$. If $b \in B$, then $b = q(j(x))) = [j(x)]_R$ or $b = q(j(\bar{x})) = [j(\bar{x})]_R$. Let define

$$b' = \begin{cases} [j(\bar{x})]_R \text{ if } b = [j(x)]_R \\ [j(x)]_R \text{if } b = [j(\bar{x})]_R \end{cases}$$

Since $[j(x)\ j(\bar{x})]_R = [e]_R = [j(\bar{x})\ j(x)]_R$ we have $[j(x)]_R [j(\bar{x})]_R = e_{F(X)} = [j(\bar{x})]_R\ [j(x)]_R$ where $e_{F(X)} = [e]_R$ is the identity in F(X). So $bb' = b'b = e_{F(X)}$. Thus $\langle B \rangle = F(X)$ has inverses. So F(X) is a group. I find a group homomorphism $\hat{f}$. Define $g : X \sqcup \bar{X} \to G$ by $g(x) = f(x)$ if $x \in X$ and $g(\bar{x}) = f(x)^{-1}$if $\bar{x} \in \bar{X}$. Then g is determined by f. And then there is a unique monoid homomorphism $\hat{g} : F_m(X \sqcup \bar{X}) \to G$ such that $\hat{g} \cdot j = g$ (Theorem Ⅳ. 1) and $\hat{g}(j(x)j(\bar{x})) = (\hat{g}(j(x))) = (x)g(\bar{x}) = e$. So $(j(x)\ j(\bar{x}), e) \in R_{\hat{g}} = \{(x, y) \mid \hat{g}(x) = \hat{g}(y)\ x, y \in F_m(X \sqcup \bar{X})\}$ (congruence relation on $F_m(X \sqcup \bar{X})$). Also $(j(\bar{x})j(x), e) \in R_{g'}$. So $R_{g'} \supseteq R$. By the diagram



where $\hat{f} = \bar{g} \cdot h$, $\hat{f}$ is a group homomorphism uniquely determined by f.

Corollary. In Therem V. 1., $K : X \to F(X)$ is one-one. Proof). Let P(X) be a family of all subsets of X. Then P(X) is a group with the binary operation $A * B = (A-B) \sqcup (B-A)$ if $A, B \subset X$. Consider $f : X \to P(X)$ defined by $f(x) = \{x\}$. Then f is one-one, By Theorem V. I., there is a group homomrphism $f : F(X) \to P(X)$ such that $\hat{f} \cdot K = f$. If $K(x) = K(x')$ for $x, x' \in X$, then $(\hat{f} \cdot K)(x) = (f \cdot K)(x')$, i. e. $f(x) = f(x')$. So $x = x'$.

Remark. Suppose we want to construct a group that has elements a, b such tat $a^2 = e$, $b^3 = e$, and $aba = b^2$. Consider $X = \{A, B\}$, F(X), and $R = \bigcap \{R' \mid R'$ is a congruence relation on F(X) with $(A^2, e) \in R'$, $(B^3, e) \in R'$, $(ABA, B^2) \in R'\}$. Then F(X)/R is that group which $a = [A]_R$ and $b = [B]_R$.

Ⅵ. A free abelian group

Remark (1). Let G be a group, S be a subset of G, and assume that if $g \in G$ and $s \in S$, then $gsg^{-1} \in S$. Let $N = \bigcap \{H \mid H$ is a subgroup of G containing $S\}$. Then N is a normal subgroup of G. And any normal subgroup K of G with $S \subseteq K$ has $N \subseteq K$. Furthermore, if $f : G \to G'$ is a group homomorphism with $f(s) = e$ for all $s \in S$, ;then $N \subseteq \ker(f)$ and $f = h \cdot K$, where $K : G \to G/N$ is given by $K(g) = gN$ and $h : G/N \to G'$ is given by $h(gN) = f(g)$.

(2) Let G be a group and $(a, b) = a^{-1}b^{-1}ab$ for $a, b \in G$. Let A, B be normal subgroups of G and let $S = \{(a, b) \mid a \in A, b \in B\}$. Then $gsg^{-1} \in S$ if $g \in G$ and $s \in S$, Let $(A, B) = \bigcap \{H \mid H$ is a subgroup of G containing $S\}$. Let $K : G \to G/(A, B)$ be the homomorphism defined by $K(g) = g(A, B)$. Then $K(a)\ K(b) = K(b)K(a)$ for all $a \in A$ and $b \in B$. If $f : G \to G'$ is a group homomorphism with $f(a)f(b) = f(b)f(a)$ for all $a \in A$ and $b \in B$, then $(A, B) \subseteq \ker(f)$. Furthermore, if $A = B = G$ and $f : G \to G'$ is a group homomorphism with G' abelian, then (G, G) ker(f), and then G/(G, G) is abelian.

By the above Remark (1), (2), we can state and preve the following theorem.

Theorem Ⅵ. 1. Let $G = F(X)$ be the free group on X, and let $K : X \to G$ be the injective map associated to it. Let $F_{ab}(X) = G/(G, G)$ and let $\bar{K} : X \to F_{ab}(X)$ be defined by $\bar{k}(X) = k(X)(G, G)$. Then $F_{ab}(X)$ is abelian, and if $f : X \to G'$ is any function from X to an abelian group, then there is a unique group homomorphism $\bar{f} : F_{ab}(X) \to G'$ such that $\bar{f}(\bar{k}(x)) = f(x)$ for all $x \in X$.

Proof. By the above Remark (1), (2), $F_{ab}(x)$ is abelian. So we find the function $\hat{f} : F_{ab}(x) \to G'$. By Theorem V. 1. there is a unique group homomorphism $\hat{f} : G \to G'$ such that $\hat{f} \cdot K = f$ on X. Since G' is abelian, so $(G, G) \subset \ker(\hat{f})$ by the above Remark. Let $P : G \to F_{ab}(x)$ defined by $P(a) = a(G, G)$ for all $a \in G$, and define $\bar{f} : F_{ab}(X) \to G'$by $\bar{f}(P(a)) = \hat{f}(a)$. Then $\bar{f}$ is well-defined by the above remark. Since $\hat{f}$ is a group homomorphism, so $\bar{f}$ is a group homomorphism : Because

$\bar{f}(P(a)P(b)) = \bar{f}(P(ab)) = \hat{f}(ab) = \hat{f}(a)\hat{f}(b) = \bar{f}(P(a))$ $\bar{f}(P(b))$. And then $\bar{f}$ is determined uniquely by f which $\bar{f} \cdot p = \hat{f}$.

Corollary. In Theorem Ⅵ. 1. $F_{ab}(X)$ is a tree abelian group on $\bar{K}(X)$.

Proof. Let G′ be an abelian group and f : $\bar{K}(X) \to G'$ be a function. Then $f \cdot \bar{K} : X \to G'$ is a function. By Theorem Ⅵ. 1., there is a unique group homomorphism $\bar{f} : F_{ab}(x) \to G'$ such taht $\bar{f} \cdot \bar{K} = f \cdot \bar{K}$ on X. And so $\bar{f} = f$ on $\bar{K}(X)$.

Literature Cited

Bourbaki. N. 1964. Agebra. Herman.

Clifford, A. H and G. B. Preston, 1964. TheAlgebraic Theory of Semigroups, vol. 1., 2nd, A. M. S

Lang S. 1984. Algebra, 2nd, Addison-Wesley,

Magid A. 1984. Lecture Note on Abstract Algebra, Unpublished, The University of Oklahoma.

國 文 抄 錄

이 논문에서는 다음과 같은 대수적 대상물에 대한 구조를 연구한다. 즉 (1) 자유마그마 (2) 자유반군 (3) 자유단위적 반군 (4) 자유군 (5) 자유 가환군