*Annales Univ. Sci. Budapest., Sect. Comp. 47 (2018) 141–146*

# SOME ACCESSIBLE TREATMENT OF ALGEBRAIC ISOMORPHISMS

**Soumyarup Banerjee, Bowen Li, Ruihan Liu, Yu Sun** (Jinan, China)
**Shigeru Kanemitsu** (Kitakyushu, Japan)

Communicated by Imre Kátai

(Received February 6, 2018; accepted May 25, 2018)

**Abstract.** In this note, we unify many well-known theorems in abstract algebra as a result on a principal ideal domain (PID), Theorem 1.3. The proof entails an elucidating argument which establishes several isomorphism theorems in the theory of groups and fields at a stretch. This includes the use of the direct sum to interpret the method of constructing an extension ring of a given ring $R$ as a quotient ring of the polynomial ring over $R$ modulo a non-zero ideal, which in turn includes the case of the ring consisting of degree 0 polynomials as elements of the ring $R$.

## 1. Introduction and the main result

In many books on algebra [2], [3], [5], [6] it is customary to state the following two theorems (or similar) as independent and prove them independently by applications of the ring homomorphism theorem and the (group) homomorphism theorem, respectively.

**Theorem 1.1.** *Let $K$ be a field of char $K = 0$ and let $K[x]$ denote the polynomial ring to which we refer below. Let $\theta$ be a root of an irreducible polynomial*

*Key words and phrases*: PID, homomorphism theorems, polynomial rings, direct sums, field theory.
*2010 Mathematics Subject Classification*: Primary: 20K25, 20K30; Secondary: 13B25.

*$f(x) \in K[x]$ of degree $n$ in an extension field $L$ of $K$ (e.g. in its algebraic closure). Then we have*

$$\varphi : K[x]/(f(x)) \simeq K(\theta) \tag{1.1}$$

*where $K(\theta)$ is the smallest extension field $\in L$ that contains $K$ and $\theta$ and is explicitly given as*

$$K(\theta) = K \oplus \cdots \oplus K\theta^{n-1}. \tag{1.2}$$

The construction of the extension field $K(\theta)$ in this theorem is not so immediate since it is not clear if an irreducible polynomial can be decomposed. An instructive example is the case of the polynomial $X^2 + 1$ which is irreducible over the field $\mathbb{R}$ of real numbers. $\mathbb{R}(i)$ as one of the constructions of $\mathbb{C}$. This cannot be formed if there is no algebraic closure and the only way is to interpret this as the polynomial ring $\mathbb{R}[X]/(X^2 + 1)$.

**Theorem 1.2.** *Suppose $G$ is a group written additively and let $a \in G$. We denote the cyclic subgroup generated by $a$ by $H = \{ma | m \in \mathbb{Z}\}$. Then we have*

$$\mathbb{Z}/(d) \simeq H. \tag{1.3}$$

*Here $d$ is a non-negative integer. If $d \in \mathbb{N}$, then $H$ is a finite group and we have*

$$d = \min\{m \in \mathbb{N} | ma = 0\}. \tag{1.4}$$

Theorem 1.2 entails

**Corollary 1.1.** *Let $R$ be an integral domain (or a field) and consider the subdomain generated by 1: $R_0 = \{m1 | m \in \mathbb{Z}\}$. Then $R_0 \simeq \mathbb{Z}$ or $R_0 \simeq \mathbb{Z}/(p)$, where $p$ is a prime.*

**Proof.** This is the case of Theorem 1.2 with $a = 1$, which implies $R_0 \simeq \mathbb{Z}/(d)$. If $d = 0$, then the right-hand side is $\mathbb{Z}$ and if $d \in \mathbb{Z}$, then $d$ must be a prime since $R_0$ is an integral domain. ■

This clarifies the well-known fact that the former is the characteristic 0 and the latter is the characteristic $p$ case In case they are fields, they contain $\mathbb{Q}$ and $\mathbb{F}_p = \mathbb{Z}/(p)$ as prime fields, respectively.

Our main result is unification of all these into the following theorem and providing a more elucidating proof.

**Theorem 1.3.** *Let $R$ be a PID and $R'$ an $R$-module [resp. additive Abelian groups] and let*

$$\varphi : R \to R' \tag{1.5}$$

*be an R-module homomorphism* [*resp. a group homomorphism*]. *Then*

$$\bar{\varphi} : R/\operatorname{Ker}\varphi \simeq \varphi(R)(\subset R'). \tag{1.6}$$

*In the case of PIDs, there exists a prime element* $p \in R$ *such that*

$$\bar{\varphi} : R/(p) \simeq \varphi(R). \tag{1.7}$$

**Proof.** By (1.5)

$$\varphi : R \to \varphi(R)(\subset R') \tag{1.8}$$

is a surjective homomorphism. It suffices to lift this up to an isomorphism by restricting the domain. Since $\varphi(a) = \varphi(b)$ amounts to $b - a \in \operatorname{Ker} f := N$ or $a + N = b + N$, The injectivity condition: $\varphi(a) = \varphi(b) \Longrightarrow a = b$ is realized in in reduced form in $G/N$. Hence the correspondence (1.6) is a bijection and so also an isomorphism.

If $R'$ is a PID, $\operatorname{Ker}\varphi$ must be a principal ideal, say $(p)$. Since $\varphi(R)$ is an integral domain, $(p)$ must be a prime ideal and *a fortiori* $p$ is a prime element and $(p)$ is also a maximal ideal, implying that $R/(p)$ is a field. ■

The above proof amounts to restricting the domain of the epimorphism to a factor group so that injectivity of the new map is assured. With this view, one can give more accessible proofs of many other results. We shall give some examples.

**Theorem 1.4.** (Homomorphism Theorem.) *If* $f$ *is a homomorphism from a group* $G$ *into a group* $G'$. *Then there exists an isomorphism* $\bar{f} : G/N \to \operatorname{Im} f$, *where* $N$ *is* $\operatorname{Ker} f \lhd G$.

Although the following theorem is a consequence of Theorem 1.4, we may give a direct and accessible proof.

**Theorem 1.5.** (The second homomorphism theorem.) *Let* $H$ *and* $N$ *be subgroups of* $G$ *and let* $N \lhd G$. *Then* $H \cap N \lhd H$ *and we have the isomorphism*

$$H/H \cap N \cong HN/N$$

*under the correspondence* $a(H \cap N) \longleftrightarrow aN$.

**Proof.** $f : HN \to H/H \cap N$ is an epimorphism. It is enough to realize injectivity in reduced form in $HN/N$. Hence the correspondence $HN/N \to$ $\to H/H \cap N$ is a bijection and so also an isomorphism. ■

## 2. Other algebraic systems

In earlier version of this note, we stated the theory of polynomials as terminating (formal) power series [1]. The novelty lies in the use of the constant term of a polynomial

**Corollary 2.1.** *Let $R \subset R[x]$ be a Euclidean domain and $R'$ an integral domain which is an $R$-module. Let $a \in R'$, $R(a) = \{ma \mid m \in R\}$ and let*

$$\varphi : R \to R(a); \quad \varphi(m) = (ma, 0, 0, \ldots). \tag{2.1}$$

*Then*

$$R/(a) \simeq R(a) \simeq \langle a \rangle. \tag{2.2}$$

**Proof.** A standard proof is as follows. Viewing (2.1) as $\varphi : R \to R(a)$; $\varphi(m) = ma$, we see that $\varphi$ is apparently a ring epimorphism. Since $\operatorname{Ker} f = \{m \in R | ma = 0\}$ is an ideal $(a)$, the group homomorphism theorem applies. ■

Theorem 1.2 follows from this by specifying $R = \mathbb{Z}$.

**Remark 2.1.** In [4], the left-hand side member of (2.2) is mentioned as a method for constructing an extension of a given field $K$. We interpret this passage in a slightly more generalized fashion, i.e. as a means to construct a new extension ring which contains $R$ as a subring. For any prime power $q = p^e$, the unique finite field $\mathbb{F}_q$ with $q$ elements is a splitting field of the polynomial $X^q - X$, which is therefore a 0-map over $\mathbb{F}_q$ and (2.2) is to mean that one can still construct a ring extension. Therefore, Theorem 1.1 serves as a tool for constructing an extension ring if $f$ is reducible and an extension field if $f$ is irreducible, which is the simple extension in $\bar{K}$ isomorphic to the left-hand side.

In the case of finite fields, the situation is rather special.

For any prime power $q = p^e$, there exists a unique finite field $\mathbb{F}_q$ with $q$ elements, which is a splitting field of $X^q - X$ and $\mathbb{F}_q^\times$ is a cyclic group of order $q - 1$.

If $e > 1$, one can choose an irreducible polynomial $f(X)$ over $\mathbb{F}_p$ which is a divisor of $X^q - X$. Let $\theta$ be a root of $f$. Then Theorem 1.1 holds in the following form

$$\mathbb{F}_q = \mathbb{F}_p 1 \oplus \cdots \oplus \mathbb{F}_p \theta^{e-1} = \mathbb{F}_p(\theta). \tag{2.3}$$

Fermat's little theorem, a typical example of a non-zero polynomial being a 0 map, says that $\mathbb{F}_p$ is a splitting field of $X^p - X$. In this case (2.3) holds as a trivial identity $\mathbb{F}_p = \mathbb{F}_p 1$.

We state some results on algebraic systems generated by their subsystems which have some flavor of homomorphism theorems and to which we may apply the method of proof of Theorem 1.3.

In any algebraic system $\mathcal{A}$, the subsystem $\langle S\rangle$ generated by a subset $S \subset \mathcal{A}$ is defined to be the smallest subsystem that contains $S$. It can be expressed as

$$\langle S\rangle = \cap_{\substack{H\supset S \\ \mathcal{A}\supset H:\text{subsystem}}} H. \tag{2.4}$$

We have seen several examples. $K(\theta)$ in (1.1) is the smallest subfield of $L \supset K$ that contains $K$ and $\theta$. The subdomain $R_0$ in Corollary 1.1 is the smallest subdomain that contains 1. $HN$ in Corollary 1.5 is the smallest subgroup of $G$ that contains $H$ and $N$. Suppose now we are given two subsystems $X$ and $Y$ of $\mathcal{A}$, that the intersection $X \cap Y$ is also a subsystem and that the subsystem generated by $X$ and $Y$ is denoted $X \cdot Y$. Further assume that the residue classes of subsystems $X \cdot Y/Y$ and $X/(X \cap Y)$ are formed and they are the algebraic systems with the same operations in $\mathcal{A}$ modulo $Y$ and $X \cap Y$, respectively. Then they are isomorphic as algebraic systems and their order relation between these equivalence classes is given by

**Theorem 2.1.** *We have*

$$X/(X \cap Y) \simeq (X \cdot Y)/Y; \quad |(X \cdot Y)/Y| = |X/(X \cap Y)|. \tag{2.5}$$

**Proof.** Define the epimorphism

$$\varphi : X \to (X \cdot Y)/Y; x \to x + Y. \tag{2.6}$$

Then the station where $\varphi$ is injective is $X/\operatorname{Ker}\varphi$ and $\operatorname{Ker}\varphi = X \cap Y$, whence the result. ■

To apply this, we take $X, Y$ to be additive groups and if necessary we add the multiplicativity $\varphi(ab) = \varphi(a)\varphi(b)$ extra.

Theorem 1.5 is an example of groups.

**Example 2.2.** Suppose $V$ is a linear space over a scalar field $K$ and $W_1, W_2$ be subspaces. Then the subspace generated by $W_1, W_2$ is $\langle W_1, W_2\rangle = W_1 + W_2$. Theorem 2.1 applies to give

$$W_1/(W_1 \cap W_2) \simeq (W_1 + W_2)/W_2, \quad |W_1/(W_1 \cap W_2)| = |(W_1 + W_2)/W_2|. \tag{2.7}$$

The order relation is a multiplicative analogue of the dimension formula

$$\dim(W_1 + W_2) = \dim W_1 + \dim W_2 - \dim(W_1 \cap W_s).$$

Both shows that the condition for $W_1 + W_2$ is isomorphic to the Cartesian product $W_1 \times W_2$ and hence to the direct sum $W_1 \oplus W_2$ is that $W_1 \cap W_2 = \{0\}$.

**Example 2.3.** Suppose $K, L$ are subfields of some field $F$. Then the subfield generated by $K, L$ is $\langle K, L\rangle = K \cdot L$. Theorem 2.1 applies to give

$$K/(K \cap L) \simeq (K \cdot L)/L, \quad |K/(K \cap L)| = |(K \cdot L)/L|. \tag{2.8}$$

The order relation amounts to the degree relation

$$[K \cdot L : L] = [K : K \cap L].$$

**Acknowledgement.** The referee has kindly suggested that the use of direct sums as polynomials is well-known and we removed that part in this version, resorting to [1] or [5]. In most of the books, the theory is stated using an indeterminate.

## References

[1] **Gal, I.** *Lectures on Number Theory*, Jones Letter Service, Minneapolis 1961.
[2] **Hattori, A.,** *Modern Algebra*, Asakura-shoten, Tokyo 1968.
[3] **Herstein, I.N.,** *Abstract Algebra*, Macmilan, New York 1986.
[4] **Kitaoka, Y.,** *An Introduction to Algebraic Number Theory*, in preparation.
[5] **Lang, S.,** *Algebra*, Addison-Wesley, Minneapolis 1965.
[6] **van der Waerden, R.L.,** *Algebra I*, 8th ed. Springer Verl., Berlin-Heidelberg-New York 1971; *Algebra II*, 5th ed. Springer Verl., Berlin-Heidelberg-New York 1967.

**S. Banerjee**
Harish-Chandra Research Institute
HBNI
Chhatnag Road, Jhunsi
Allahabad-211 019
India
soumyabanerjee@hri.res.in

**B. Li, R. Liu, Y. Sun**
Shandong University
Taishan School
Shanda Nanlu No. 27
Jinan-250110
People's Republic of China
463291366@qq.com
15194372798@163.com
778516650@qq.com

**S. Kanemitsu**
Department of Applied Science
Kyushu Institute of Technology
Kitakyushu
Japan
omnikanemitsu@yahoo.com