신 용 수 교수지도

석 사 학 위 논 문

# DIVISION RING

2009

성신여자대학교 교육대학원

교육학과 수학교육전공

최 연 주

# DIVISION RING

신 용 수 교수지도

이 논문을 석사학위논문으로 제출함.

2008월 11월

성신여자대학교 교육대학원

교육학과 수학교육전공

최 연 주

# 인 준 서

방지원의 석사학위 논문으로 인준함.

심사위원 _____ 인

심사위원 _____ 인

심사위원 _____ 인

성신여자대학교 교육대학원

# 목 차

## 국 문 초 록

# 나눗셈 환

성신여자대학교 교육대학원
교육학과 수학교육전공
최 연 주

$\mathbb{Z}$와 $\mathbb{Q}$가 각각 정수와 유리수 환이고, 또한 $\mathbb{Z}^+$가 모든 양의 정수의 집합이라고 할 때, 모든 유한 정역이 체라는 것은 잘 알려진 바이다.

이 논문에서는 영인자가 없는 모든 유한 환이 체라는 것을 갈로아 이론, 분해체, 분리 확대체 등 몇 개의 정의와 정리를 이용하여 증명하였다.

# DIVISION RING

YOUN-JOO CHOI

## 1. Introduction

In this thesis, let $\mathbb{Z}$ and $\mathbb{Q}$ be the rings of of integers and rational numbers, respectively. Also, $\mathbb{Z}^+$ is the set of all positive integers. It is well-know that every finite integral domain is a field (see Remark 8).

The goal of this thesis is to prove that every finite ring without divisors of 0 is a field (see Lemma 25, Theorems 46, and 47).

For this proof, we use several concepts and results of a field theory, that is, we need the following concepts: Galois theory, splitting fields, separable extensions, and normal extensions (see Theorem 41, Definitions 21, 32 and 38).

In Section 2, we introduce some preliminary definitions and notations. In Section 3, we study cyclotomic extensions and Galois theory. Finally, we prove that a finite division ring is always a field.

## 2. Preliminaries

In this section, we introduce some preliminary notations and results in [1] and [2] .

**Lemma 1** ([1]). *A subset $H$ of a group $G$ is a subgroup of $G$ if and only if*

(1) *$H$ is closed under the binary operation of $G$,*
(2) *the identity element $e$ of $G$ is in $H$ ,*
(3) *for all $a$ in $H$ it is true that $a^{-1}$ in $H$ also.*

We shall give the proofs of some of them for readers. Moreover, we will skip the proofs when they can be easily proved.

**Definition-Proposition 2** ([1]). Let $G$ be a group and let $S$ be any subset of $G$. Then

(a) $H_S = \{x \in G \mid sx = xs \quad \text{for all} \quad s \in S\}$ is a subgroup of $G$.
(b) The subgroup $H_G$ is an abelian group and $H_G := Z(G)$ is called the ***center of*** $G$.

*Proof.* (a) Let $e$ be the identity element in $G$. Then

$$e \cdot s = s \cdot e = s,$$

for every $s \in S$ , that is, $e$ is in $H_S$.
For every $x, y$ in $H_S$, $s \in S$, we have

$$(xy)s = x(ys) = x(sy) = (sx)y = s(xy),$$

which implies that

$$xy \in H_S.$$

For every $x \in H_S$ and $s \in S$,

$$\begin{aligned} & xs = sx \\ \Longrightarrow \quad & x^{-1}(sx)x^{-1} = x^{-1}(xs)x^{-1}, \\ \Longrightarrow \quad & x^{-1}s = sx^{-1}, \end{aligned}$$

and hence $x^{-1} \in H_S$, which follows from Lemma 1 that $H_S$ is a subgroup of $G$.

(b) By (a), $H_G$ is a subgroup of $G$. Moreover, by definition, every element in $H_G$ commutes with every element in $G$, and so every element in $H_G$ ($\subseteq G$) commutes in $H_G$, that is, $H_G$ is abelian. □

**Definition 3** ([1])**.** If $a$ and $b$ are two nonzero elements of a ring $R$ such that $ab = 0$ , then $a$ and $b$ are ***divisors of*** 0.

**Definition 4** ([1])**.** An ***integral domain*** $D$ is a commutative ring with unity $1 \neq 0$ which contains no ***divisors of*** 0 .

**Definition 5** ([1])**.** Let $R$ be a ring with unity $1 \neq 0$. An element $u$ in $R$ is a ***unit*** of $R$ if it has a multiplicative inverse in $R$ . If every nonzero element of $R$ is a unit, then $R$ is a ***division ring*** (or ***skew field***).

**Definition 6** ([1])**.** A ***field*** is a commutative ***division ring***.

**Remark 7** (Theorem 19.5, [1])**.** The cancellation laws holds in a ring $R$ if and only if $R$ has no divisors of 0.

Indeed, let $R$ be a ring in which the cancellation laws hold, and suppose $ab = 0$ for some $a, b \in R$. We must show that either $a$ or $b$ is 0. If $a \neq 0$, then $ab = a0$ implies that $b = 0$ by cancellation laws. Similarly, $b \neq 0$ implies that $a = 0$, so there can be no divisors of 0 if the cancellation laws holds.
Conversely, suppose that $R$ has no divisors of 0, and suppose that $ab = ac$ with $a \neq 0$. Then

$$ab - ac = a(b - c) = 0.$$

Since $a \neq 0$ and $R$ has no divisors of 0, we must have $b - c = 0$, so $b = c$. A similar argument shows that $ba = ca$ with $a \neq 0$ implies $b = c$.

**Remark 8** (Theorem 19.11, [1])**.** The main result is that any finite integral domain is a field.
In fact, let

$$0, 1, a_1, ..., a_n$$

be all the elements of a finite domain $D$ and let $D^* = D - \{0\}$. We need to show that for $a \in D$, where $a \neq 0$, there exists $b \in D$ such that $ab = 1$. Now consider

$$aD^* = \{a1, aa_1, ..., aa_n\}.$$

All these elements of $aD^*$ are distinct, because $aa_i = aa_j$ implies $a_i = a_j$ by the cancellation laws that hold in an integral domain by Remark 7. Also, since $D$ has no 0 divisors, none of these elements is 0. In other words, $aD^* \subset D^*$ and $|aD^*| = |D^*|$, and so $aD^* = D^*$. In particular, since $1 \in D^* = aD^*$, we have $aa_i = 1 (= aa_i)$ for some $i$. Thus $a$ has a multiplicative inverse.

**Definition 9** ([1])**.** A field $E$ is an ***extension field*** of a field $F$ if $F$ is a subfield of $E$, denoted by $F \leq E$.

**Definition 10** ([1])**.** Let $F$ be a field. A ***vector space over*** $F$ (or $F$***-vector space***) consists of an abelian group $V$ under addition together with an operation of scalar multiplication of each element of $V$ by each element of $F$ on the left, such that for all $a, b \in F$ and $\alpha, \beta \in V$ the following conditions are satisfied.

$\mathcal{V}_1$. $a\alpha \in V$.
$\mathcal{V}_2$. $a(b\alpha) = (ab)\alpha$.
$\mathcal{V}_3$. $(a + b)\alpha = (a\alpha) + (b\alpha)$.
$\mathcal{V}_4$. $a(\alpha + \beta) = (a\alpha) + (a\beta)$ .
$\mathcal{V}_5$. $1\alpha = \alpha$.

Elements of $V$ are called ***vectors*** and elements of $F$ are called ***scalars***.

**Remark 11** (Example 30.4, [1])**.** Let $E$ be an extension field of a field $F$ . Then $E$ can be regarded as a vector space over $F$, where addition of vectors is the usual addition in $E$ and scalar multiplication $a\alpha$ is the usual field multiplication in $E$ with $a \in F$ and $\alpha \in E$. The axioms follow immediately from the field axioms for $E$. Here our field of scalars is actually a subset of our space of vectors .

**Lemma 12** ([1])**.** *Let $G$ be a nonempty set and $\langle G, * \rangle$ be a binary structure satisfying the following three axioms as follows:*

1. *The binary operation $*$ on $G$ is associative.*
2. *There exists a left (right) identity element $e$ in $G$ such that $e * x = x$ for all $x \in G$.*
3. *For each $a \in G$, there exists a left (right) inverse $a'$ in $G$ such that $a' * a = e$.*

*Then $G$ is a group.*

**Lemma 13.** *Let $D$ be a ring. If $D$ is a finite ring which has no divisors of $0$, then $D$ is a division ring.*

*Proof.* For every $a$ in $D^* = D - \{0\}$, define a map

$$\varphi_a : D^* \longrightarrow D^*, x \longmapsto ax.$$

First, since $D$ has no 0-divisor, $\varphi_a$ is well-defined and one to one. Hence $|D^*| = |\phi_a[D^*]|$. Moreover, since $\varphi_a[D^*] \subset D^*$, we have

$\phi_a[D^*] = D^*$, which means that $\phi_a$ is surjective. Hence there exists a $a'$ in $D$, such that $aa' = 1$. In other words, $a$ has a right inverse in $D^*$.

Let $D^* = D - (0)$. Then $\langle D^*, \cdot \rangle$ is well defined and $D^* \neq \varnothing$. The associativity clearly holds. Moreover, there exists a right identity 1 in $D$. Hence by Lemma 28, $\langle D^*, \cdot \rangle$ is a group. Therefore $D$ is a division ring, as we wished. □

**Definition-Proposition 14.** If $R$ is any ring, then the ***center*** of $R$ is the set

$$\mathcal{C} = \{c \in R \mid cr = rc \text{ for all } r \in R\}.$$

Then $\mathcal{C}$ is easily seen to be a subring of $R$.

**Definition 15** ([1])**.** An element $\alpha$ of an extension field $F$ of a field $K$ is ***algebraic over*** $K$ if $f(\alpha) = 0$ for some nonzero polynomial $f(x) \in K[x]$.

**Theorem 16** ([1])**.** *Let $F$ be an extension field of $K$, and let $\alpha \in F$, where $\alpha$ is algebraic over $K$. Then there is an irreducible polynomial $p(x) \in K[x]$ such that $p(\alpha) = 0$. This irreducible polynomial $p(x)$ is uniquely determined up to a constant factor in $K$ and is a polynomial of minimal degree $\geq 1$ in $K[x]$ having $\alpha$ as a zero. If $f(\alpha) = 0$ for $f(x) \in K[x]$, with $f(x) \neq 0$, then $p(x)$ divides $f(x)$.*

**Definition 17** ([1])**.** An extension field $F$ of a field $K$ is an ***algebraic extension of*** $K$ if every element in $F$ is algebraic over $K$.

**Definition 18** ([1])**.** If an extension field $F$ of a field $K$ is of finite dimension $n$ as a vector space over $K$, then $F$ is a ***finite extension of degree n over*** $K$. We shall let $[F : K]$ be the degree $n$ of $F$ over $K$.

**Definition 19** ([1])**.** A field $K$ is ***algebraiclly closed*** if every non-constant polynomial in $K[x]$ has a zero in $K$.

**Theorem 20** (Theorem 31.17, [1])**.** *Every field $K$ has an algebraic closure, that is, an algebraic extension $\overline{K}$ of $K$ which is algebraiclly closed.*

**Definition 21** ([1])**.** Let $K$ be a field with algebraic closure $\overline{K}$. Let $\{f_i(x) \mid i \in I\}$ be a collection of polynomials in $K[x]$ . A field $F \leq \overline{K}$ is the ***splitting field*** of $\{f_i(x) \mid i \in I\}$ over $K$ if $F$ is the smallest subfield of $\overline{K}$ containing $K$ and all the zeros in $\overline{K}$ of each of the $f_i(x)$ for $i \in I$.
A field $E \leq \overline{K}$ is a ***splitting field*** over $K$ if it is the ***splitting field*** of some set of polynomials in $K[x]$.

**Definition 22** ([1])**.** Let $F$ be an extension field of $K$ such that the fixed field of the Galois group $\mathrm{Aut}_K F$ is $K$ itself. Then $F$ is said to be a ***Galois extension*** (field) of $K$ or to be ***Galois*** over $K$.

**Lemma 23.** *Let $F$ be an extension field of $K$ and $f \in K[x]$. If $u \in F$ is a root of $f$ and $\sigma \in Aut_K F$, then $\sigma(u) \in F$ is also a root of $f$.*

*Proof.* If $f = \sum_{i=1}^{n} k_i x^i$, then $f(u) = 0$ implies $0 = \sigma(f(u)) = \sigma(\Sigma k_i u^i) = \sum \sigma(k_i)\sigma(u^i) = \sum k_i \sigma(u)^i = f(\sigma(u))$. □

**Lemma 24.** *If $F$ is an extension field of $K$ and $E$ is an intermediate field of the extension such that $E$ is algebraic and Galois over $K$, then $E$ is stable (relative to $F$ and $K$), that is, for all $\sigma \in Aut_K F$, $\sigma(\alpha) \in E$, $\forall \alpha \in E$.*

*Proof.* If $u \in E$, let $f \in K[x]$ be the irreducible polynomial of $u$ and let $u = u_1, u_2, ..., u_r$ be the distinct roots of $f$ that lie in $E$. Then $r \leq n = \deg f$. If $\tau \in \mathrm{Aut}_K E$, then it follows from Lemma 23 that $\tau$ simply permutes the $u_i$. This implies that the coefficients of the monic polynomial $g(x) = (x - u_i)(x - u_2) \cdots (x - u_i) \in E[x]$ are fixed by every $\tau \in \mathrm{Aut}_K E$. Since $E$ is Galois over $K$, we must have $g \in K[x]$. Now $u = u_1$ is a root of g and hence $f \mid g$. Since $g$ is monic and $\deg g \leq \deg f$, we must have $f = g$. Consequently, all the roots of $f$ are distinct and lie in $E$. Now if $\sigma \in \mathrm{Aut}_K F$, then $\sigma(u)$ is a root of $f$ by Lemma 23, whence $\sigma(u) \in E$. Therefore, $E$ is stable relative to $F$ and $K$. □

**Lemma 25** (Theorem 3.11, [2]). *If $E$ is an extension field of $K$, then the following statements are equivalent.*

(1) *$E$ is algebraic and Galois over $F$;*
(2) *$E$ is separable over $F$ and $E$ is a splitting field over $F$ of a set $S$ of polynomials in $F[x]$;*
(3) *$E$ is a splitting field over $F$ of a set $T$ of separable polynomials in $F[x]$.*

**Lemma 26** (Theorem 5.3, [2]). *If $E$ is a field and $G$ is a finite subgroup of the multicative group of nonzero elements of $E$, then $G$ is a cyclic group. In particular, the multiplicative group of all nonzero elements of a finite field is cyclic.*

**Lemma 27** (Lemma 33.9, [2]). *If $F$ is a field of prime characteristic $p$, then $(\alpha+\beta)^{p^n} = \alpha^{p^n}+\beta^{p^n}$ for all $\alpha, \beta \in F$ and all positive intergers $n$.*

**Remark 28** (Remarks, [2]). (1) Let $K$ be a field and $n$ a positive integer. An element $\zeta \in K$ is said to be an ***nth root of unity*** provided $\zeta^n = 1$. It is easy to see that the set of all $n$th roots of unity in $K$ forms a multiplicative subgroup of the multiplicative group of nonzero elements of $K$. This subgroup is cyclic by lemma 26 and has order at most $n$. $\zeta \in K$ is said to be a ***primitive nth root of unity*** provided $\zeta$ is an $n$th root of unity and $\zeta$ has order $n$ in the multiplicative

group of $n$th root of unity. In particular, a primitive $n$th root of unity generates the cyclic group of all $n$th root of unity.

(2) If $\mathrm{char}(K) = p$ and $p \mid n$, then $n = p^k m$ with $(p, m) = 1$ and $m < n$. Thus $x^n - 1 = (x^m - 1)^{p^k}$. Consequently the $n$th roots of unity in $K$ coincide with the $m$th roots of unity in $K$. Since $m < n$, there can be no primitive $n$th root of unity in $K$.

## 3. Cyclotomic Extensions and Galois Theory.

First of all, we introduce the primitive $n$th root of unity and cyclotomic extension here.

**Lemma 29.** *Let $K$ be a field of characteristic $p > 0$. If $p \nmid n$, then*

(1) *$x^n - 1$ has $n$ distinct roots in any splitting field $F$ of $x^n - 1$ over $K$, and*

(2) *the cyclic group of $n$th roots of unity in $F$ has order $n$ and $F$ contains a primitive $n$th root of unity.*

(3) *In particular, if $K$ does contain a primitive $n$th root of unity, then $K$ contains $n$ distinst roots of $x^n - 1$, whence $F = K$.*

*Proof.* (1) Let $\alpha \in F$ and $\alpha^n - 1 = 0$. Note that $n \cdot \alpha^{n-1} \neq 0$ since $(p, n) = 1$.

Define

$$\begin{aligned} g(x) &= \frac{x^n - 1}{x - a} \\ &= (x^{n-1} + \alpha x^{n-2} + \cdots + \alpha^{n-2}x + \alpha^{n-1}) \in F[x]. \end{aligned}$$

Then

$$\begin{aligned} g(\alpha) &= \alpha^{n-1} + \cdots + \alpha^{n-1} \\ &= n \cdot \alpha^{n-1} \\ &\neq 0. \end{aligned}$$

Therefore $x^n - 1$ has $n$ distinct zeros in $F$.

(2) Let $G = \{\alpha_i \mid \alpha_i^n = 1,\ \alpha_i \in F,\ i = 1, ..., n\}$ be the set of all zeros of $x^n - 1$. Then $G$ is a finite subgroup of $F^*$, and hence $G$ is a cyclic group of order $n$ by Lemma 26. Thus $G$ has an element of order $n$, which is a primitive $n$th root of unity.

(3) Supose $K$ contains a primitive $n$th root of unity, $\alpha$. Then $\{1, \alpha, ..., \alpha^{n-1}\}$ is the set of zeros of $x^n - 1$ , that is, $K$ contains $n$ distinct zeros of $x^n - 1$, and hence

$$F = K(\alpha) = K.$$

□

**Definition 30** ([2])**.** A splitting field $E$ over a field $F$ of $x^n - 1 \in F[x]$ (where $n \geq 1$, 1 is a unity in $F$) is called a ***cyclotomic extension of order*** $n$ .

**Remark 31.** Let $G = \langle a \rangle$ be a cyclic group of order $n$. Then $a^k = e$ for some positive integer $k \in \mathbb{Z}^+$ if and only if $n \mid k$. In fact, let $k = nq + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < n$.

Then

$$\begin{aligned} & a^k = a^{nq+r} = (a^n)^q \cdot a^r = a^r = e \\ \Longrightarrow \quad & r = 0 \ (\because \mid a \mid = n) \\ \Longrightarrow \quad & n \mid k. \end{aligned}$$

Conversely, if $n \mid k$, i.e, $k = n \cdot q$ for some $q \in \mathbb{Z}^+$, then

$$a^k = a^{n \cdot q} = (a^n)^q = e^q = e.$$

**Definition 32** ([2])**.** Let $K$ be a field and $f \in K[x]$ an irreducible polynomial. The polynomial $f$ is said to be ***separable*** if in some splitting field of $f$ over $K$ every root of $f$ is a simple root.
If $F$ is an extension field of $K$ and $u \in F$ is algebraic over $K$, then $u$ is said to be ***separable*** over $K$ provided its irreducible polynomial is separable. If every element of $F$ is separable over $K$, then $F$ is said to be a ***separable extension*** of $K$.

**Lemma 33.** *Let $n$ be a positive integer and $F$ a field which contains a primitive $n$th root of unity $\zeta$.*

(1) *If $d \mid n$, then $\zeta^{n/d} = \eta$ is a primitive $d$th root unity in $F$.*
(2) *If $d \mid n$, $u$ is a nonzero root of $x^d - a \in F[x]$, then $x^d - a$ has $d$ distinct roots, namely $u, \eta u, \eta^2 u, ..., \eta^{d-1}$, where $\eta \in F$ is a primitive $d$th root of unity. Furthermore $F(u)$ is a splitting field of $x^d - a$ over $F$ and is Galois over $F$.*

*Proof.* (1) Note that $\langle\zeta\rangle$ is a cyclic group of order $n$. Hence, by Remark 31, $|\ \zeta^{\frac{n}{d}}\ | = \frac{n}{\langle n, \frac{n}{d}\rangle} = d$, that is, $\zeta^{\frac{n}{d}}$ is a primitive $d$-th root of unity.

(2) Note that $u, \eta u, \eta^2 u, ..., \eta^{d-1}$ are all zeros of $x^d - a$; for

$$\begin{aligned} & (u \cdot \eta^i)^d - a \\ = \ & u^d(\eta^d)^i - a \\ = \ & u^d - a \\ = \ & 0, \end{aligned}$$

for every $i = 0, 1, ..., d-1$.

Moreover, since $1, \eta, ..., \eta^{d-1}$ are all distinct, $u, u\eta, ..., u\eta^{d-1}$ are also all distinct, and $F(u)$ is a splitting field of a separable polynomial $x^d - a$ over $F$. Therefore $F(u)$ is Galois over $F$, as we wished. □

**Example 34.** Let $\alpha = \frac{-1+\sqrt{3}i}{2}$. Then $\alpha$ is the primitive 3rd root of unity, and $F = \mathbb{Q}(\alpha)$ contains a primitive 3rd root of unity. Hence, by Lemma 33, $x^3 - 2$ has 3 distinct roots, $\sqrt[3]{2}, \sqrt[3]{2}\alpha, \sqrt[3]{2}\alpha^2$ and $F(\sqrt[3]{2}) = \mathbb{Q}(\alpha, \sqrt[3]{2})$ is a splitting field of $x^3 - 2$ over $F$ and is Galois over $F$.

**Definition 35** ([1])**.** A finite extension $E$ of a field $K$ is a ***finite normal extension of*** $K$ if $E$ is a separable splitting field over $K$.

**Definition 36** ([1])**.** A finite normal extension of a field $K$ is abelian over $K$ if $\mathrm{Aut}_K E$ is an ***abelian*** group.

**Lemma 37.** *If $E$ is abelian over $K$ and $F$ is normal extension of $K$, where $K \leq F \leq E$, then $E$ is abelian over $K$ and $F$ is abelian over $K$.*

*Proof.* Since $E$ is abelian over $K$, we have that $\mathrm{Aut}_K E$ is abelian. Moreover, since $\mathrm{Aut}_F E \leq \mathrm{Aut}_K E$) we see that $\mathrm{Aut}_F E$ is also abelian, that is, $E$ is abelian over $F$.
Since $F$ is normal extension of $K$, by Galois Theory, we have $\mathrm{Aut}_K F \cong \mathrm{Aut}_K E/\mathrm{Aut}_F E$ which is also abelian. In other words, $F$ is abelian over $K$. □

**Definition 38** ([1])**.** A finite normal extension $E$ of a field $K$ is cyclic over $K$ if $\mathrm{Aut}_K E$ is a cyclic group.

**Lemma 39.** *If $E$ is cyclic over $K$ and $F$ is normal extension of $K$, where $K \leq F \leq E$, then $F$ is cyclic over $K$ and $E$ is cyclic over $F$.*

*Proof.* Since $\mathrm{Aut}_F E$ is a subgroup of a cyclic group $\mathrm{Aut}_K E$, $\mathrm{Aut}_F E$ is also a cyclic group. Moreover, since $E$ is a normal extension $F$, $E$ is cyclic over $F$. Since $F$ is a normal extension of $K$, by Galois Theory, we have that $\mathrm{Aut}_F E \lhd \mathrm{Aut}_K E$ and so $\mathrm{Aut}_K F \cong \mathrm{Aut}_K E/\mathrm{Aut}_F E$ is cyclic, and hence $F$ is also a cyclic extension of $K$. □

**Remark 40.** Let $G = \langle \alpha \rangle$ be a cyclic group of order $n < +\infty$ and let $i, j \in \mathbb{Z}$. Then

$$\begin{aligned} & a^i = a^j \\ \Leftrightarrow \quad & a^{i-j} = e \ (e : \text{identity of } G) \\ \Leftrightarrow \quad & n \mid (i-j) \\ \Leftrightarrow \quad & i \equiv j \pmod{n}. \end{aligned}$$

**Theorem 41** ([2])**.** *Fundamental Theorem of Galois Theory*
*If $F$ is a finite dimensional Galois extension of $K$ , then there is a one-to-one correspondence between the set of all intermediate fields of the extension and the set of all subgroups of the Galois group $Aut_K F$ (given by $E \mapsto E' = Aut_E F$) such that:*

(1) *the relative dimension of two intermediate fields is equal to the relative index of the corresponding subgroups; in particular, $Aut_K F$ has order $[F : K]$;*
(2) *$F$ is Galois over every intermediate field $E$, but $E$ is Galois over $K$ if and only if the corresponding subgroups $E' = Aut_E F$ is normal in $G = Aut_K F$; in this case $G/E'$ is (isomorphic to) the Galois group $Aut_K E$ of $E$ over $K$.*

**Theorem 42.** *Let $n$ be a positive integer, $F$ a field such that the characteristic of $F$ does not divide $n$ and $E$ a cyclotomic extension of $F$ of order $n$.*

(1) *$E = F(\zeta)$, where $\zeta \in E$ is a primitive nth root of unity.*

(2) *$E$ is an abelian extension of dimension $d$, where $d \mid \varphi(n)$ ($\varphi$ is the Euler function); if $n$ is prime, then $E$ is actually a cyclic extension.*

(3) *$Aut_F E$ is isomorphic to a subgroup of order $d$ of the multiplicative group of units of $\mathbb{Z}_n$.*

*Proof.* (1) Lemma 28 (2) shows that $E$ contains a primitive $n$th root of unity $\zeta$. By definition $1, \zeta, ..., \zeta^{n-1} \in F(\zeta)$ are the $n$ distinct roots of $x^n - 1$, hence $F(\zeta) = E$.

(2) Since the irreducible factors of $x^n - 1$ are separable, Lemma 25 implies that $E$ is Galois over $F$. If $\sigma \in \mathrm{Aut}_F E$, then $\sigma$ is completely determined by $\sigma(\zeta)$. Let $\mathrm{irr}(\zeta, \mathrm{F}) = a_0 + a_1 x + \cdots + a_n x^n = p(x)$. Since $\sigma(a) = a$, for every $a \in F$, we have

$$\begin{aligned} 0 &= \sigma(0) \\ &= \sigma(a_0 + a_1\zeta + \cdots + a_n\zeta^n) \\ &= a_0 + a_1\sigma(\zeta) + \cdots + a_n\sigma(\zeta)^n, \end{aligned}$$

and hence $p(\sigma(\zeta)) = 0$. In other words, $\sigma(\zeta) = \zeta^i$ for some $1 \leq i \leq n$ since $\mathrm{irr}(\zeta, \mathrm{F}) \mid x^n - 1$. Similarly $\sigma^{-1}(\zeta) = \zeta^j$, for some $j$, so that $\zeta^1 = \sigma^{-1}\sigma(\zeta) = \zeta^{ij}$. Hence by Remark 40, $i \cdot j \equiv 1 \pmod{n}$, so $i \in \mathbb{Z}_n$ is a unit. Let $\mathbb{Z}_n^*$ be the multiplicative group of units of the ring $\mathbb{Z}_n$. Then we obtain a monomorphism

$$\varphi : \quad \mathrm{Aut}_F E \longrightarrow \mathbb{Z}_n^*, \ \sigma \mapsto i.$$

Hence $G \cong G/\ker \cong \mathrm{Im}\varphi$, and so we have

$$\mid \mathrm{Aut}_F E \mid = \mid \mathrm{Im}\varphi \mid \ \Big| \ \mid \mathbb{Z}_n^* \mid = \varphi(n).$$

Moreover, since $\mathbb{Z}_n^*$ is a abelian group, $\mathrm{Aut}_F E \cong \mathrm{Im}\varphi \leq \mathbb{Z}_n^*$ is also an abelian. Furthermore, if $n$ is a prime, then $\mathbb{Z}_n^*$ is cyclic, and hence,

by Lemma 26, $\mathrm{Aut}_F E \cong \mathrm{Im}\varphi \leq \mathbb{Z}_n^*$ is also cyclic. Hence $E$ is a cyclic extension. □

**Definition 43** ([2])**.** Let $n$ be a positive integer, $F$ a field such that $\mathrm{char}(F)$ does not divide $n$ , and $E$ a cyclotomic extension of order $n$ of $F$. The ***n-th cyclotomic polynomial*** over $F$ is the monic polynomial $g_n = (x - \zeta_1)(x - \zeta_2) \cdots (x - \zeta_n)$ where $\zeta_1, \zeta_2, ..., \zeta_n$ are all the distinct primitive $n$th roots of unity in $E$.

**Theorem 44.** *Let $n$ be a positive integer, $F$ a field such that char(F) does not divide $n$ and $g_n(x)$ the $n$th cyclotomic polynomial over $F$.*

(1) $x^n - 1 = \prod_{d|n} g_d(x)$.
(2) *The coefficients of $g_n(x)$ lie in the prime subfield $P$ of $F$. If* $\mathrm{char}(F) = 0$ and $P$ is identified with the field $\mathbb{Q}$ of rationals, then the coefficients are actually integers.
(3) $\deg g_n(x) = \varphi(n)$, where $\varphi$ is the Euler function.

*Proof.* (1) Let $E$ be a cyclotomic extension of $F$ of order $n$ and $\zeta \in E$ a primitive $n$th root of unity. The cyclic group $G = \langle \zeta \rangle$ of all $n$th roots of unity contains all $d$th roots of unity for every divisor $d$ of $n$. In fact, if $\alpha \in E$ and $\alpha^d - 1$, then $\alpha^n - 1 = 0$. Hence $\alpha$ is a zero of $x^n - 1$, and hence $\alpha = \zeta^i$ for some $0 \leq i \leq n - 1$. Clearly, $\eta \in G$ is a primitive $d$th root of unity (where $d \mid n$) if and only if $\mid \eta \mid = d$. Therefore for each divisor $d$ of $n$.

$$g_d(x) = \prod_{\eta \in G, |\eta| = d} (x - \eta)$$

and

$$x^n - 1 = \prod_{\eta \in G}(x - \eta) = \prod_{d|\eta}(\prod_{\eta \in G, |\eta| = d}(x - \eta)) = \prod_{d|\eta} g_d(x).$$

(2) We prove the first statement by induction on $n$. Clearly,

$$g_1(x) = x - 1 \in P[x].$$

Assume that (2) is true for all $k < n$ and let

$$f(x) = \prod_{d|n, d<n} g_d(x).$$

Then $f(x) \in P[x]$ by the induction hypothesis and in $E[x]$,

$$x^n - 1 = f(x)g_n(x)$$

by (1). On the other hand $x^n - 1 \in P[x]$ and $f(x)$ is monic. Consequently, the division algorithm in $P[x]$ implies that

$$x^n - 1 = f(x)h(x) + r(x)$$

for some $h(x)$, $r(x) \in P[x] \subset F[x]$. Therefore, by the uniqueness of quotient and remainder (of the division algorithm applied in $E[x]$) we must have

$$\begin{aligned} x^n - 1 &= f(x)h(x) + r(x),\ h(x),\ r(x) \in P[x] \leq E[x] \\ &= f(x)g_n(x) \in E[x] \end{aligned}$$

and hence

$r(x) = 0$ and $g_n(x) = h(x) \in P[x]$. This completes the induction. If char $(F) = 0$ and $P = \mathbb{Q}$, then a similar inductive argument using the division algorithm in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ (instead of $P[x], F[x]$) shows

that $g_n(x) \in \mathbb{Z}[x]$ .
First,

$$g_1(x) = x - 1 \in \mathbb{Z}[x].$$

Note that $x^n - 1 = f(x)g_n(x)$ and $g_n(x) \in \mathbb{Q}[x]$, and $\alpha g_n(x) \in \mathbb{Z}[x]$ for some $\alpha \in \mathbb{Z}$. In other words,

$$\begin{aligned} & \alpha(x^n - 1) &=& \quad f(x) \cdot (\alpha g_n(x)) \\ \Rightarrow \quad & c(\alpha(x^n - 1)) &=& \ c(f(x) \cdot (\alpha g_n(x))) \\ & &=& \ c(f(x))c(\alpha g_n(x)) \\ \Rightarrow \quad & \alpha &=& \quad 1 \cdot c(\alpha g_n(x)), \end{aligned}$$

which means that $g_n(x) \in \mathbb{Z}[x]$.

(3) $\deg g_n(x)$ is clearly the number of primitive $n$th roots of unity. Let $\zeta$ be such a primitive root so that every other (primitive) root is a power of $\zeta$. Then $\zeta^i$ $(1 \leq i \leq n)$ is a primitive $n$th root of unity (that is, a generator of $G$) if and only if $(i, n) = 1$. But the number of such $i$ is by definition precisely $\varphi(n)$. □

**Remark 45** (Theorem 6.13, [2])**.** Let $D$ be a unique factorization domain with quotient field $F$ and $f(x)$ a primitive polynomial of positive degree in $D[x]$. Then $f(x)$ is irreducible in $D[x]$ if and only if $f(x)$ is irreducible in $F[x]$.

We now prove the main theorem here.

**Theorem 46.** *A finite division ring $D$ is a field.*

(a) *The center $K$ of $D$ is a field and $D$ is a vector space over $K$, whence $|D| = |K|^n$ for some $n \in \mathbb{Z}^+$.*

(b) *If $0 \neq a \in D$, then $N(a) = \{d \in D \mid da = ad\}$ is a subdivision ring of $D$ containing $K$. Furthermore, $|N(a)| = q^r$ for some $r \in \mathbb{Z}^+$ where $r \mid n$.*

(c) *If $0 \neq a \in D - K$, then $N(a)^*$ is the centralizer of $a$ in the group $D^*$ and $[D^* : N(a)^*] = (q^n - 1)/(q^r - 1)$ for some $r \in \mathbb{Z}^+$ such that $1 \leq r < n$ and $r \mid n$.*

(d) *$q^n - 1 = q - 1 + \sum_r (q^n - 1)/(q^r - 1)$, where the last sum taken over a finite number of integers $r$ such that $1 \leq r < n$ and $r \mid n$.*

(e) *For each primitive $n$-th root of unity $\zeta \in \mathbb{C}$, $|q - \zeta| > q - 1$, where $|a + bi| = \sqrt{a^2 + b^2}$ for $a + bi \in \mathbb{C}$. Consequently, $|g_n(q)| > q - 1$, where $g_n$ is the $n$-th cyclotomic polynomial over $\mathbb{Q}$.*

(f) *The equation in* (d) *is impossible unless $n = 1$, whence $K = D$.*

*Proof.* (a) $K = x \in D \mid xy = yx, \ for\ all\ y \in D$. Then it is obvious that $0 \in K$ and $1 \in K$. Assume $\alpha, \ \beta \in K$. Then for every $x \in D$,

$$\begin{aligned} (\alpha - \beta)x &= \alpha x - \beta x \\ &= x\alpha - x\beta \ (\because \alpha, \ \beta \in K) \\ &= x(\alpha - \beta), \end{aligned}$$

i.e, $\alpha - \beta \in K$. This means that $\langle K, + \rangle$ is an abelian group. Moreover,

$$\begin{aligned}(\alpha\beta)x &= \alpha(\beta x)\\ &= \alpha(x\beta)\ (\because \beta \in K)\\ &= (\alpha x)\beta\\ &= (x\alpha)\beta\ (\because \alpha \in K)\\ &= x(\alpha\beta),\end{aligned}$$

and so $\alpha\beta \in K$. Hence $k$ is a subring of $D$. Furthermore, for every $\alpha \in K - 0$, there exists $\alpha^{-1} \in D$ s.t $\alpha\alpha^{-1} = \alpha^{-1}\alpha = 1$. Hence, for every $x \in D$,

$$\begin{aligned}&\alpha x &&= x\alpha\ (\alpha \in K)\\ \Rightarrow\ &\alpha^{-1}(\alpha x)\alpha^{-1} &&= \alpha^{-1}(x\alpha)\alpha^{-1}\\ \Rightarrow\ &x\alpha^{-1} &&= \alpha^{-1}x,\end{aligned}$$

which means that $\alpha^{-1} \in K$, i.e, $K$ is a field. Note that, by Remark 11, $D$ is a vector space over $K$. Since $D$ is a finite division ring, $D$ is a finite dimensional vector space over $K$, say $n \in \mathbb{Z}^+$. In other words, $\mid D \mid = \mid K \mid^n$.

(b) By the similar method as in the proof of (a), one can show that $N(a)$ is a subdivision of $D$ containing $K$. Let $\mid K \mid = q$. Note that $K \leq N(a) \leq D$, that is, $[N(a) : K] \mid [D : K]$. Hence $\mid N(a) \mid = r$ for some $r = [N(a) : K]$ and $r \mid n$. Hence $\mid N(a) \mid = \mid K \mid^r = q^r$.

(c) Let $a \in D - K$. Then $N(a)^* = N(a) - 0\ (\lneq D^*)$ is clearly the centraliger of a in the group $D^*$, and

$$[D^* : N(a)^*] = \frac{\mid D^* \mid}{\mid N(a)^* \mid} = \frac{q^n - 1}{q^r - 1}$$

for some $r \in \mathbb{Z}^+$ s.t $1 \leq r < n$ and, by (b), $r \mid n$.

(d) Let $N(a_1)^*, ..., N(a_s)^*$ be the distinct centraligers of $a_1, ..., a_s \in D^* - K$. Then, by the class equation of $D^*$,

$$\begin{aligned} \mid D^* \mid &= \mid C(D^*) \mid + \textstyle\sum_{i=1}^{s} [D^* : N(a)^*] \\ &= \mid K^* \mid + \textstyle\sum_{i=1}^{s} [D^* : N(a)^*] \\ &= (q-1) + \textstyle\sum_r (q^n - 1)/(q^r - 1) \quad (\because (c)). \end{aligned}$$

(e) Note that $\zeta \in \mathbb{C} - \mathbb{R}$, and thus $b \neq 0$. Hence

$$\begin{aligned} \mid q - \zeta \mid &= \sqrt{(q-a)^2 + b^2} \\ &> \sqrt{(q-a)^2} \\ &= \mid q - a \mid \\ &> \mid q - 1 \mid \quad (\because 0 < a < 1). \end{aligned}$$

Moreover, since

$$g_n(q) = c \prod_{i=1}^{\varphi(n)} (x - \zeta_i)$$

where $c \in \mathbb{Z}$ and $\zeta_i$ are all primitive $n$th root of unity,

$$\begin{aligned} \mid g_n(q) \mid &= \mid c \mid \textstyle\prod_{i=1}^{\varphi(n)} \mid q - \zeta_i \mid \\ &> \mid c \mid \textstyle\prod_{i=1}^{\varphi(n)} \mid q - 1 \mid \\ &\geq \textstyle\prod_{i=1}^{\varphi(n)} \mid q - 1 \mid \\ &\geq \mid q - 1 \mid, \end{aligned}$$

i.e., $\mid g_n(q) \mid > (q-1)$.

(f) Note that since $f_r(x) = \frac{x^n - 1}{x^r - 1}$, $g_n(x) \mid f_r(x)$ and $(g_n(x), x^r - 1) = 1$, for every $r \mid n$ and $1 \leq r < n$. Hence $f_r(x) = g_n(x) h_r(x)$ with $h_r(x) \in \mathbb{Z}[x]$. In particular,

$$g_n(q) \mid f_r(q) = \Big(\frac{q^n - 1}{q^r - 1}\Big)$$

for such $r$. Thus

$$g_n(q) \mid (q^n - 1) = (q-1) + \sum_{r|n, r<n} \left(\frac{q^n - 1}{q^r - 1}\right)$$
$$\Rightarrow g_n(q) \mid (q-1) \quad \left(\because\ g_n(q) \mid \frac{q^n - 1}{q^r - 1}\right),$$

which is a contradiction if $n > 1$. Therefore, $n = 1$, that is, $D = K$, which completes the proof. □

**Theorem 47.** *Let $D$ be a finite ring with no divisors of 0. Then $D$ is a field.*

*Proof.* It is immediate from Lemma 25 and Theorem 46. □

## References

[1] John B. Fraleigh, *A first course in abstract algebra*, Addison-Wesley, Seventh edition(2003).

[2] T.W. Hungerford, *Algebra*, Springer-Verlag, (1973).

# ABSTRACT

Choi Youn Joo
Major in Mathemaitcs Education
Graduate school of Education
Sungshin Women's University
Supervised by Professor Shin Yong su Ph.D.

The goal of this thesis is to prove that every finite ring without divisors of 0 is a field. For this proof, we use several concepts and results of a field theory, that is, we need the following concepts: Galois theory, splitting fields, separable extensions, and normal extensions.
Finally, we prove that a finite division ring is always a field.