Ten Lectures on Galois Theory

Paul-Hermann Zieschang
Department of Mathematics
University of Texas Rio Grande Valley
Edinburg, TX 78520, U.S.A.

1. Preserving and Reversing Orders

Let X be a set. A binary relation on X is called an *order* if it is reflexive, antisymmetric, and transitive. If r is an order on X, the set X is called *ordered* with respect to r. If it is understood with respect to which order the set X is ordered, we just say that X is an ordered set. If X is ordered and a pair (y, z) of elements of X belongs to the order with respect to which X is ordered, we write $y \leq z$.

Let X be an ordered set, let W be a subset of X.

An element x of X is called an *upper bound* of W *in* X if $w \leq x$ for each element w in W. An upper bound u of W in X is called a *supremum* of W *in* X if $u \leq x$ for each upper bound x of W in X. An element v in W is called a *maximal* element of W if $w \leq v$ for each element w in W with $v \leq w$. An element v in W is called a *greatest* element of W if $w \leq v$ for each element w in W.

Note that W may have no, exactly one, or more than one upper bound in X and no, exactly one, or more than one maximal element while W never has two or more suprema in X and also never two or more greatest elements.

The terms *lower bound*, *infimum*, *minimal*, and *least* are defined correspondingly.

In this section, we consider maps the domain and the codomain of which both are ordered. All maps will be written exponentially.

Let Y and Z be ordered sets. A map ϕ from Y to Z is called *order preserving* if $v^\phi \leq w^\phi$ for any two elements v and w in Y with $v \leq w$.

Let X be a set and let α be a map from X to X. We denote by $\mathrm{Fix}_X(\alpha)$ the set of all elements x in X satisfying $x^\alpha = x$.

Lemma 1.1

Let X be an ordered set, assume that each subset of X has a supremum, and let α be an order preserving map from X to X. Then $\mathrm{Fix}_X(\alpha)$ contains a greatest element.

Proof. Set

$$U := \{x \in X \mid x \leq x^\alpha\},$$

and define w to be the supremum of U. Then $u \leq w$ for each element u in U. Thus, $u \leq u^\alpha \leq w^\alpha$ for each element u in U. Since w is the supremum of U, this implies that $w \leq w^\alpha$. It follows that $w^\alpha \leq (w^\alpha)^\alpha$, whence $w^\alpha \in U$. Since w is the supremum of U, this implies that $w^\alpha \leq w$.

From $w \leq w^\alpha$ and $w^\alpha \leq w$ we now obtain that $w^\alpha = w$, so $w \in \mathrm{Fix}_X(\alpha)$.

On the other hand, w is an upper bound of U, and $\mathrm{Fix}_X(\alpha) \subseteq U$. Thus, w is an upper bound of $\mathrm{Fix}_X(\alpha)$. Thus, w is the greatest element of $\mathrm{Fix}_X(\alpha)$. □

Recall that the inverse of an order is an order, too. Thus, Lemma 1.1 implies the

following. Let X be an ordered set, assume that each subset of X has an infimum, and let α be an order preserving map from X to X. Then $\mathrm{Fix}_X(\alpha)$ contains a least element.

Let X be a set, and recall that the power set $\mathcal{P}(X)$ of X is ordered with respect to set theoretic containment. Each subset $\mathcal{S}$ of $\mathcal{P}(X)$ has an infimum, it is the intersection of the sets which belong to $\mathcal{S}$. Each subset $\mathcal{S}$ of $\mathcal{P}(X)$ also has a supremum, it is the union of the sets which belong to $\mathcal{S}$.

Theorem 1.2 [F. Bernstein–R. Dedekind]
Let Y and Z be sets. Assume that there exists an injective map from Y to Z and an injective map from Z to Y. Then there exists a bijective map from Y to Z.

Proof. Let d be an injective map from Y to Z, let e be an injective map from Z to Y, and define

$$\alpha\colon\ \mathcal{P}(Y) \to \mathcal{P}(Y), \quad V \mapsto Y \setminus (Z \setminus V^d)^e.$$

Note that $U^\alpha \subseteq V^\alpha$ for any two subsets U and V of Y with $U \subseteq V$. Thus, by Lemma 1.2, Y contains a subset V with $V^\alpha = V$. From $V^\alpha = V$ we obtain that $Y \setminus V = (Z \setminus V^d)^e$.

Define $y^f := y^d$ for each element y in V. For each element y in $Y \setminus V$, define y^f to be the unique preimage of y under e. Then f is a bijective map from Y to Z. □

Let Y and Z be ordered sets.

A map ϕ from Y to Z is called *order reversing* if $w^\phi \leq v^\phi$ for any two elements v and w in Y with $v \leq w$.

Let γ be an order reversing map from Y to Z, and let ϕ be an order reversing map from Z to Y.

The pair (γ, ϕ) is called a *Galois pair* if $y \leq y^{\gamma\phi}$ for each element y in Y and $z \leq z^{\phi\gamma}$ for each element z in Z.

Assume that (γ, ϕ) is a Galois pair. Sometimes we want to mention the orders on Y and on Z with respect to which the pair (γ, ϕ) is a Galois pair. If this is the case and if s denotes the order on Y and t the order on Z, we say that (γ, ϕ) is a Galois pair *with respect to* (s, t).

Theorem 1.3 [Abstract Galois Correspondence]
Let Y and Z be ordered sets, let γ be a map from Y to Z, let ϕ be a map from Z to Y, and assume that (γ, ϕ) is a Galois pair. Then the following statements hold.

(i) *We have* $\mathrm{im}(\gamma) = \{z \in Z \mid z = z^{\phi\gamma}\}$ *and* $\mathrm{im}(\phi) = \{y \in Y \mid y = y^{\gamma\phi}\}$.

(ii) *For each element y in Y, we have $y^\gamma = y^{\gamma\phi\gamma}$; for each element z in Z, we have $z^\phi = z^{\phi\gamma\phi}$.*

(iii) *Let γ' denote the map from* $\mathrm{im}(\phi)$ *to* $\mathrm{im}(\gamma)$ *which maps each element y of* $\mathrm{im}(\phi)$ *to y^γ, and let ϕ' denote the map from* $\mathrm{im}(\gamma)$ *to* $\mathrm{im}(\phi)$ *which maps each element z of* $\mathrm{im}(\gamma)$ *to y^ϕ. Then γ' and ϕ' are bijective and inverses of each other.*

PROOF. (i) Let z be an element in $\mathrm{im}(\gamma)$. Then Y contains an element y such that $z = y^\gamma$. Since $y \in Y$ and (γ, ϕ) is a Galois pair, this implies that $y \leq y^{\gamma\phi} = z^\phi$. Thus, as γ is order reversing, $z^{\phi\gamma} \leq y^\gamma = z$. On the other hand, as $z \in Z$ and (γ, ϕ) is a Galois pair, $z \leq z^{\phi\gamma}$. Thus, $z = z^{\phi\gamma}$.

The proof of the second equation is obtained by interchanging the roles of Y and Z and γ and ϕ.

(ii) This follows from (i).

(iii) From (i) we obtain that $\gamma'\phi' = \mathrm{id}_{\mathrm{im}(\phi)}$ and that $\phi'\gamma' = \mathrm{id}_{\mathrm{im}(\gamma)}$. Thus, the claim follows. □

Let Y and Z be sets, let γ be a map from Y to Z, let ϕ be a map from Z to Y, and assume that (γ, ϕ) is a Galois pair.

An element y in Y is called *galois with respect to* (γ, ϕ) if $y = y^{\gamma\phi}$. Similarly, an element z in Z is called *galois with respect to* (γ, ϕ) if $z = z^{\phi\gamma}$.

We emphasize that galois elements can be elements in Y as well as elements in Z.

By Theorem 1.3(i), the elements which are galois with respect to (γ, ϕ) are exactly the elements in $\mathrm{im}(\gamma) \cup \mathrm{im}(\phi)$.

EXERCISES

1. Set $X := \{1, 2, 3\}$. For each of the eight subsets U of X, define $\gamma(U)$ to be the set of all permutations π of X satisfying $u^\pi = u$ for each element u in U. For each of the six subgroups H of $\mathrm{Sym}(X)$, define $\phi(H)$ to be the set of all elements x in X satisfying $x^\pi = x$ for each element π in H. Show that (ϕ, γ) is a Galois pair with respect to the set theoretic containment on the power set of X and the set theoretic containment on the power set of $\mathrm{Sym}(X)$. Determine the galois elements with respect to (γ, ϕ).

2. Let X be a set. For each subset U of X, define $\gamma(U)$ to be the set of all permutations π of X satisfying $u^\pi = u$ for each element u in U. For each set P of permutations of X, define $\phi(P)$ to be the set of all elements x in X satisfying $x^\pi = x$ for each element π in P. Show that (ϕ, γ) is a Galois pair with respect to the set theoretic containment on the power set of X and the set theoretic containment on the power set of $\mathrm{Sym}(X)$. Determine the galois elements with respect to (γ, ϕ).

2. Galois Pairs Arising from Monoids

Let M be a monoid.[1] We define

$$\mathrm{End}(M) := \mathrm{Hom}(M, M).$$

The elements in $\mathrm{End}(M)$ are called *monoid endomorphisms* (or just *endomorphisms*) of M, they are called *group endomorphisms* (or just *endomorphisms*) of M if M is a group.

Bijective monoid endomorphisms are called *monoid automorphisms* (or just *automorphisms*), bijective group endomorphisms are called *group automorphisms* (or just *automorphisms*).[2]

The set of all automorphisms of a monoid M will be denoted by $\mathrm{Aut}(M)$.

For the remainder of this section, the letter M stands for a monoid. All monoid endomorphisms will be written exponentially.

The set of all maps from M to M is denoted by $\mathrm{Map}(M)$. Note that $\mathrm{Map}(M)$ is a monoid with respect to composition.

---

[1] A *monoid* is defined to be a set together with an associative operation which has a neutral element. The operation of a monoid is usually written multiplicatively, so that $(jk)l = j(kl)$ for any three monoid elements j, k, and l. It is easy to see that a monoid cannot have two different neutral elements. The neutral element of a monoid is usually denoted by 1, so that $m{\cdot}1 = m = 1{\cdot}m$ for each monoid element. Occasionally, monoids are written additively. In this case, the associativity says that $(j + k) + l = j + (k + l)$ for any three monoid elements j, k, and l. Also, in an additive monoid, the neutral element is denoted by 0, so we have $m + 0 = m = 0 + m$ for each element m of an additive monoid.

Let m be an element of a monoid M. An element n of M is called an *inverse* of m if $mn = 1 = nm$. An element m of a monoid M is called a *unit* of M if it possesses an inverse. It is easy to see that a monoid element cannot have two different inverses. The inverse of an element m of a multiplicatively written monoid will always be denoted by m^{-1}, the inverse of an element m of an additively written monoid will always be denoted by $-m$. The set of all units of a monoid M is denoted by $M^\times$. A monoid M is called a *group* if $M^\times = M$. Note that $M^\times$ is a group with respect to the restriction of the multiplication of M to $M^\times \times M^\times$. This group will be called the *group of units* of M.

Monoids M are called *commutative* if $kl = lk$ for any two elements k and l of M.

A subset L of a monoid M is called a *submonoid* of M if $1 \in L$ and if, for any two elements j and k in L, $jk \in L$. Submonoids L of a monoid M are called *subgroups* if each element of L is a unit of M and has its inverse in L. Note that submonoids of monoids M are monoids with respect to the multiplication inherited from M. Similarly, subgroups of monoids M are groups with respect to the multiplication inherited from M.

Let M and M' be monoids. A map ϕ from M to M' is called a *monoid homomorphism* (or just *homomorphism*) if $(kl)^\phi = k^\phi l^\phi$ for any two elements k and l in M and $1^\phi = 1$. Monoid homomorphisms from M to M' are called *group homomorphisms* if M and M' are groups. The set of all monoid homomorphisms from M to M' is denoted by $\mathrm{Hom}(M, M')$. Bijective monoid homomorphisms are called *monoid isomorphisms* (or just *isomorphisms*).

[2] Notice that the monoid automorphisms (group automorphisms) are exactly the monoid isomorphisms (group isomorphisms) the domains of which are equal to their codomains.

Lemma 2.1

The following hold.

(i) *The set* $\mathrm{End}(M)$ *is a submonoid of* $\mathrm{Map}(M)$.

(ii) *We have* $\mathrm{Aut}(M) = \mathrm{End}(M)^\times$.

Proof. (i) Note that composites of endomorphisms of M are endomorphisms of M. Thus, as id_M is a monoid homomorphism from M to M, $\mathrm{End}(M)$ is a submonoid of $\mathrm{Map}(M)$.

(ii) Note that $\alpha^{-1} \in \mathrm{Aut}(M)$ for each element α in $\mathrm{Aut}(M)$. Thus, $\mathrm{Aut}(M) \subseteq \mathrm{End}(M)^\times$. Note that elements in $\mathrm{End}(M)^\times$ are bijective. Thus, we have $\mathrm{End}(M)^\times \subseteq \mathrm{Aut}(M)$. □

Lemma 2.1(ii) says that $\mathrm{Aut}(M)$ is the group of units of $\mathrm{End}(M)$. The group $\mathrm{Aut}(M)$ is called the *automorphism group* of M.

Let G be a subgroup of $\mathrm{Aut}(M)$. We define $\mathrm{Fix}_M(G)$ to be the intersection of the sets $\mathrm{Fix}_M(\alpha)$ with $\alpha \in G$. Note that $\mathrm{Fix}_M(G)$ is the set of all elements m in M satisfying $m^\alpha = m$ for each element α in G.

Lemma 2.2

Let G be a subgroup of $\mathrm{Aut}(M)$. *Then the following hold.*

(i) *The set* $\mathrm{Fix}_M(G)$ *is a submonoid of* M.

(ii) *Let m be an element in* $\mathrm{Fix}_M(G)$, *and assume that m is a unit of M. Then* $m^{-1} \in \mathrm{Fix}_M(G)$.

(iii) *If M is a group,* $\mathrm{Fix}_M(G)$ *is a subgroup of M.*

(iv) *For each element α in* $\mathrm{Aut}(M)$, *we have* $\mathrm{Fix}_M(G^\alpha) = \mathrm{Fix}_M(G)^\alpha$.

(v) *For each subgroup H of G, we have* $\mathrm{Fix}_M(G) \subseteq \mathrm{Fix}_M(H)$.

Proof. (i) Let j and k be elements in $\mathrm{Fix}_M(G)$. Then $j^\alpha = j$ and $k^\alpha = k$ for each element α in G. It follows that

$$(jk)^\alpha = j^\alpha k^\alpha = jk$$

for each element α in G, and that means that $jk \in \mathrm{Fix}_M(G)$.

For each element α in G, we have $1^\alpha = 1$, so $1 \in \mathrm{Fix}_M(G)$.

(ii) Let α be an element in G. Then, as $m \in \mathrm{Fix}_M(G)$, $m^\alpha = m$, so that

$$(m^{-1})^\alpha m = (m^{-1})^\alpha m^\alpha = (m^{-1}m)^\alpha = 1^\alpha = 1.$$

It follows that $(m^{-1})^\alpha = m^{-1}$.

Since α has been chosen arbitrarily in G, we have shown that $m^{-1} \in \mathrm{Fix}_M(G)$.

(iii) This is an immediate consequence of (i) and (ii).

(iv) Let α be an element in $\mathrm{Aut}(M)$, and let m be an element in $\mathrm{Fix}_M(G^\alpha)$. Then $m^{\alpha^{-1}\gamma\alpha} = m$ for each element γ in G. Thus, $(m^{\alpha^{-1}})^\gamma = m^{\alpha^{-1}\gamma} = m^{\alpha^{-1}}$ for each element γ in G, and that means that $m^{\alpha^{-1}} \in \mathrm{Fix}_M(G)$. It follows that $m \in \mathrm{Fix}_M(G)^\alpha$.

Since m has been chosen arbitrarily in $\mathrm{Fix}_M(G^\alpha)$, we have shown that $\mathrm{Fix}_M(G^\alpha) \subseteq \mathrm{Fix}_M(G)^\alpha$. The reverse containment follows similarly.

(v) Let m be an element in $\mathrm{Fix}_M(G)$. Then $m^\alpha = m$ for each element α in G. *A fortiori*, $m^\alpha = m$ for each element α in H, and that means that $m \in \mathrm{Fix}_M(H)$. □

Let G be a subgroup of $\mathrm{Aut}(M)$. The set $\mathrm{Fix}_M(G)$ is called the *fixed-point monoid* of G *in* M.

Let M and M' be monoids, and let L be a submonoid of M as well as of M'. A monoid homomorphism ϕ from M to M' is called an *L-homomorphism* if $l^\phi = l$ for each element l in L. Bijective L-homomorphisms from M to M' are called an *L-automorphism* if $M = M'$.

Let M be a monoid, and let L be a submonoid of M. The set of all L-automorphisms of M will be denoted by $\mathrm{Aut}_L(M)$.

Lemma 2.3

Let L be a submonoid of M. Then the following hold.

(i) *The set $\mathrm{Aut}_L(M)$ is a subgroup of $\mathrm{Aut}(M)$.*

(ii) *We have $L \subseteq \mathrm{Fix}_M(\mathrm{Aut}_L(M))$.*

(iii) *Let K be a submonoid of M with $K \subseteq L$. Then $\mathrm{Aut}_L(M) \subseteq \mathrm{Aut}_K(M)$.*

Proof. (i) It follows right from the definition of id_M that $\mathrm{id}_M \in \mathrm{Aut}_L(M)$.

Let α be an element in $\mathrm{Aut}_L(M)$. Then $l^\alpha = l$ for each element l in L. Thus,

$$l^{\alpha^{-1}} = (l^\alpha)^{\alpha^{-1}} = l^{\alpha\alpha^{-1}} = l$$

for each element l in L, and that means that $\alpha^{-1} \in \mathrm{Aut}_L(M)$.

Let β and γ be elements in $\mathrm{Aut}_L(M)$. Then $l^\beta = l$ and $l^\gamma = l$ for each element l in L. It follows that

$$l^{\beta\gamma} = (l^\beta)^\gamma = l^\gamma = l$$

for each element l in L, and that means that $\beta\gamma \in \mathrm{Aut}_L(M)$.

(ii) Let l be an element in L. Then $l^\alpha = l$ for each element α in $\mathrm{Aut}_L(M)$. Thus, $l \in \mathrm{Fix}_M(\mathrm{Aut}_L(M))$.

(iii) Let α be an element in $\mathrm{Aut}_L(M)$. Then $l^\alpha = l$ for each element l in L. *A fortiori*, $k^\alpha = k$ for each element k in K, and that means that $\alpha \in \mathrm{Aut}_K(M)$. □

Lemma 2.4

Let L be a submonoid of M, and let α be an element in $\mathrm{Aut}(M)$. Then the following hold.

(i) *The set L^α is a submonoid of M.*

(ii) *If L is a subgroup of M, so is L^α.*

(iii) *We have $\mathrm{Aut}_L(M)^\alpha = \mathrm{Aut}_{L^\alpha}(M)$.*

(iv) *If $L^\alpha = L$, then $\mathrm{Aut}_L(M)^\alpha = \mathrm{Aut}_L(M)$.*

PROOF. (i) and (ii) are obvious.

(iii) Let γ be an element in $\mathrm{Aut}_L(M)$. Then

$$(l^\alpha)^{\gamma^\alpha} = (l^\alpha)^{\alpha^{-1}\gamma\alpha} = l^{\gamma\alpha} = (l^\gamma)^\alpha = l^\alpha$$

for each element l in L. Thus, $\gamma^\alpha \in \mathrm{Aut}_{L^\alpha}(M)$.

Since γ has been chosen arbitrarily from $\mathrm{Aut}_L(M)$, we have shown that $\mathrm{Aut}_L(M)^\alpha \subseteq \mathrm{Aut}_{L^\alpha}(M)$.

Conversely, let γ be an element in $\mathrm{Aut}_{L^\alpha}(M)$. Then $l^{\alpha\gamma} = (l^\alpha)^\gamma = l^\alpha$ for each element l in L. Thus, $\gamma^{\alpha^{-1}} \in \mathrm{Aut}_L(M)$, and that is equivalent to $\gamma \in \mathrm{Aut}_L(M)^\alpha$.

(iv) This follows from (iii). □

Lemma 2.5

Let G be a subgroup of $\mathrm{Aut}(M)$. Then $G \subseteq \mathrm{Aut}_{\mathrm{Fix}_M(G)}(M)$.

PROOF. Let α be an element in G. Then $m^\alpha = m$ for each element m in $\mathrm{Fix}_M(G)$. Thus, $\alpha \in \mathrm{Aut}_{\mathrm{Fix}_M(G)}(M)$. □

Let $\mathcal{L}(M)$ denote the set of all submonoids of M, and let $\mathcal{G}(M)$ denote the set of all subgroups of $\mathrm{Aut}(M)$. Note that $\mathcal{L}(M)$ and $\mathcal{G}(M)$ both are ordered with respect to set theoretic containment.

We set

$$L^{\gamma_M} := \mathrm{Aut}_L(M)$$

for each element L in $\mathcal{L}(M)$ and

$$G^{\phi_M} := \mathrm{Fix}_M(G)$$

for each element G in $\mathcal{G}(M)$.

Theorem 2.6

The pair (γ_M, ϕ_M) is a Galois pair with respect to the orders defined on $\mathcal{L}(M)$ and $\mathcal{G}(M)$, respectively, by set theoretic containment.

PROOF. Set $\gamma := \gamma_M$ and $\phi := \phi_M$.

From Lemma 2.3(i) we know that γ is a map from $\mathcal{L}(M)$ to $\mathcal{G}(M)$, from Lemma 2.2(i) that ϕ is a map from $\mathcal{G}(M)$ to $\mathcal{L}(M)$.

In Lemma 2.3(ii), we saw that $L \subseteq L^{\gamma\phi}$ for each element L in $\mathcal{L}(M)$, in Lemma 2.5 that $G \subseteq G^{\phi\gamma}$ for each element G in $\mathcal{G}(M)$.

In Lemma 2.3(iii), we saw that $L^\gamma \subseteq K^\gamma$ for any two elements K and L in $\mathcal{L}(M)$ with $K \subseteq L$, and in Lemma 2.2(v), we saw that $G^\phi \subseteq H^\phi$ for any two elements G and H in $\mathcal{G}(M)$ with $H \subseteq G$. □

Let L be a submonoid of M, and recall from Section 1 that L is called galois with respect to (γ_M, ϕ_M) if $L = L^{\gamma_M\phi_M}$. Instead of saying that L is galois with respect to (γ_M, ϕ_M) one also says that M is *galois over* L. Thus, we have

$$L = \mathrm{Fix}_M(\mathrm{Aut}_L(M))$$

if and only if M is galois over L.

Note also that subgroups G of $\mathrm{Aut}(M)$ are galois with respect to (γ_M, ϕ_M) if

$$G = \mathrm{Aut}_{\mathrm{Fix}_M(G)}(M).$$

We will come back to the results of this section in the following section.

Exercises

1. (Just to warm up.) Set $X := \{1, 2, 3\}$. Define a to be the permutation of X which sends 1 to 1, 2 to 3, and 3 to 2. Define b to be the permutation of X which sends 1 to 2, 2 to 1, and 3 to 3. Show that $a^2 = \mathrm{id}_X$, that $b^2 = \mathrm{id}_X$, and that $aba = bab$. Set $d := aba$ and write down the complete multiplication table of $\mathrm{Sym}(X)$. [Similar to Exercise 1.9 in the Modern Algebra Notes, but with different notation.]

2. Define $G := \mathrm{Sym}(X)$, and determine the automorphism group $\mathrm{Aut}(G)$. [Here are the guidelines.]

   i. Define a as in Exercise 1. For each element g in G, define $\alpha_a(g) := a^{-1}ga$. Show that α_a is an automorphism of G.

   ii. Define b as in Exercise 1. For each element g in G, define $\alpha_b(g) := b^{-1}gb$. Show that α_b is an automorphism of G.

   iii. Define, for the remaining four elements of G, the maps similar to the maps α_a and α_b. Show these maps are all automorphisms of G. Are the resulting six automorphisms α_a, α_b, ... pairwise distinct?

   iv. Note that α_a permutes the elements of G. What are the fixed points of α_a in G? For instance $\alpha_a(b) := a^{-1}ba = aba$. (Recall that $a^{-1} = a$.) Thus, $\alpha_a(b) \neq b$, and that means that b is not a fixed point of α_a.

   v. Show that $\mathrm{Aut}(G) := \{\mathrm{id}_G, \alpha_a, \alpha_b, \ldots\}$ is a group with respect to composition. (It has six elements.) Write down the complete multiplication table of $\mathrm{Aut}(G)$.

3. Galois Pairs Arising from Rings

This section is similar to Section 2. Results which we established on monoids in Section 2 will now be established for rings.

Let R be a ring.[3] We define

$$\mathrm{End}(R) := \mathrm{Hom}(R, R).$$

The elements in $\mathrm{End}(R)$ are called *ring endomorphisms* (or just *endomorphisms*) of R.[4] Bijective ring endomorphisms are called *ring automorphisms* (or just *automorphisms*).[5] The set of all automorphisms of a ring R will be denoted by $\mathrm{Aut}(R)$.

---

[3] A *ring* is defined to be a set R endowed with two operations satisfying three conditions. The first operation is an addition, the second operation is a multiplication. The three conditions are the following. 1. With respect to its addition, R is a group. 2. With respect to its multiplication, R is a monoid. 3. Both, left distributivity as well as right distributivity must hold. The additive neutral element of a ring R is denoted by 0, its multiplicative neutral element by 1. We always assume that $0 \neq 1$.

It is easy to see that the addition of a ring is commutative, wheras the multiplication is not neccessarily commutative. Rings are called *commutative* if their multiplicative monoid is commutative.

An element of a ring R is called a *unit* of R if it is a unit of the multiplicative monoid of R. The set of all units of a ring R is denoted by $R^\times$. It is easy to see that $0 \cdot r = 0 = r \cdot 0$ for each element r in R. Thus, as $0 \neq 1$, $0 \notin R^\times$. Note that $R^\times$ is a group with respect to the restriction of the multiplication of R to $R^\times \times R^\times$. This group will be called the *group of units* of R. A ring R is called a *field* if $R^\times = R \setminus \{0\}$. (Fields are not necessarily commutative.)

A subset S of a ring R is called a *subring* of R if it is a subgroup of the additive group of R and a submonoid of the multiplicative monoid of R. Subrings S of R are called *subfields* if each element of $S \setminus \{0\}$ is a unit of R and has its multiplicative inverse in S. Note that subrings of rings R are rings with respect to the addition and multiplication inherited from R. Similarly, subfields of rings R are fields with respect to the addition and multiplication inherited from R.

Let R and R' be rings. A map ϕ from R to R' is called a *ring homomorphism* (or just *homomorphism*) if it is a group homomorphism from the additive group of R to the additive group of R' and, at the same time, a monoid homomorphism from the multiplicative monoid of R to the multiplicative monoid of R'. The set of all ring homomorphisms from R to R' is denoted by $\mathrm{Hom}(R, R')$.

Bijective ring homomorphisms are called *ring isomorphisms* (or just *isomorphisms*).

Ring homomorphisms from R to R' are called *field homomorphisms* if R and R' are fields. However, we will not use this term in these notes. We notice, though, that ring homomorphisms the domain of which is a field are necessarily injective, since a field R has only two ideals, namely $\{0\}$ and R, and each ring homomorphism sends 1 to 1.

[4] Although ring endomorphisms of a field R are injective, they are not necessarily surjective. In fact, given a prime number p, the so-called Frobenius automorphism automorphism of $\mathbb{F}_p(t)$ which sends each element of $\mathbb{F}_p(t)$ to its p-th power is not surjective, t is not in the image of this map. Also the field $\mathbb{C}$ contains subfields isomorphic to $\mathbb{C}$.

[5] Notice that the ring automorphisms are exactly the ring isomorphisms the domains of which are equal to their codomains.

For the remainder of this section, the letter R stands for a ring.

Lemma 3.1

The following hold.

(i) *The set* $\mathrm{End}(R)$ *is a submonoid of* $\mathrm{Map}(R)$.

(ii) *We have* $\mathrm{Aut}(R) = \mathrm{End}(R)^\times$.

PROOF. This follows from Lemma 2.1. □

Lemma 3.1(ii) says that $\mathrm{Aut}(R)$ is the group of units of the monoid $\mathrm{End}(R)$. The group $\mathrm{Aut}(R)$ is called the *automorphism group* of R.

There are rings which have a trivial automorphism group. These are rings R the only automorphism of which is the identity on R. The ring of integers is an example.

All ring endomorphisms will be written exponentially.

Recall from Section 2 that, for each subgroup G of $\mathrm{Aut}(R)$, $\mathrm{Fix}_R(G)$ is our notation of the set of all elements r in R satisfying $r^g = r$ for each element g in G.

Lemma 3.2

Let G *be a subgroup of* $\mathrm{Aut}(R)$. *Then the following hold.*

(i) *The set* $\mathrm{Fix}_R(G)$ *is a subring of* R.

(ii) *If* R *is a field,* $\mathrm{Fix}_R(G)$ *is a subfield of* R.

(iii) *For each element* α *in* $\mathrm{Aut}(R)$, *we have* $\mathrm{Fix}_R(G^\alpha) = \mathrm{Fix}_R(G)^\alpha$.

(iv) *For each subgroup* H *of* G, *we have* $\mathrm{Fix}_R(G) \subseteq \mathrm{Fix}_R(H)$.

PROOF. (i) From Lemma 2.2(iii) we know that $\mathrm{Fix}_R(G)$ is a subgroup of the additive group of R, from Lemma 2.2(i) that $\mathrm{Fix}_R(G)$ is a submonoid of the multiplicative monoid of R. Thus, $\mathrm{Fix}_R(G)$ is a subring of R.

(ii) This is obtained by applying Lemma 2.2(ii) to the multiplicative monoid of R.

(iii) This is obtained by applying Lemma 2.2(iv) to the additive group of R or to the multiplicative monoid of R.

(iv) This is obtained by applying Lemma 2.2(v) to the additive group of R or to the multiplicative monoid of R. □

Let R' be a ring, and let S be a subring of R as well as of R'. A ring homomorphism ϕ from R to R' is called an *S-homomorphism* if $s^\phi = s$ for each element s in S.[6] Bijective S-homomorphisms from R to R' are called *S-automorphisms* if $R = R'$.

[6]Note that an S-homomorphism from R to R' is nothing but an S-homomorphism from the additive group of R to the additive group of R' and, at the same time, an S-homomorphism from the multiplicative monoid of R to the multiplicative monoid of R'.

For each subring S of R, we will denote by $\mathrm{Aut}_S(R)$ the set of all S-automorphisms of R.

Lemma 3.3

Let S be a subring of R. Then the following hold.

(i) *The set $\mathrm{Aut}_S(R)$ is a subgroup of $\mathrm{Aut}(R)$.*

(ii) *We have $S \subseteq \mathrm{Fix}_R(\mathrm{Aut}_S(R))$.*

(iii) *Let T be a subring of R with $S \subseteq T$. Then $\mathrm{Aut}_T(R) \subseteq \mathrm{Aut}_S(R)$.*

PROOF. (i) This is obtained by applying Lemma 2.3(i) to the additive group of R or to the multiplicative monoid of R.

(ii) This is obtained by applying Lemma 2.3(ii) to the additive group of R or to the multiplicative monoid of R.

(iii) This is obtained by applying Lemma 2.3(iii) to the additive group of R or to the multiplicative monoid of R. □

Lemma 3.4

Let S be a subring of R, and let α be an element of $\mathrm{Aut}(R)$. Then the following hold.

(i) *The set S^α is a subring of R.*

(ii) *We have $\mathrm{Aut}_S(R)^\alpha = \mathrm{Aut}_{S^\alpha}(R)$.*

(iii) *If $S^\alpha = S$, then $\mathrm{Aut}_S(R)^\alpha = \mathrm{Aut}_S(R)$.*

PROOF. (i) By Lemma 2.4(ii), S^α is a subgroup of the additive group of R; by Lemma 2.4(i), S^α is a submonoid of the multiplicative monoid of R. Thus, S^α is a subring of R.

(ii) By Lemma 2.4(iii) the equation holds for the additive group of R in place of R as well as for the multiplicative monoid of R in place of R. Thus, the claim follows from the fact that the automorphisms of R are exactly the group automorphisms of the additive group of R which, at the same time, are monoid automorphisms of the multiplicative monoid of R.

(iii) This follows from (ii). □

Lemma 3.5

Let G be a subgroup of $\mathrm{Aut}(R)$. Then $G \subseteq \mathrm{Aut}_{\mathrm{Fix}_R(G)}(R)$.

PROOF. Let α be an element in G. Then $r^\alpha = r$ for each element r in $\mathrm{Fix}_R(G)$. Thus, $\alpha \in \mathrm{Aut}_{\mathrm{Fix}_R(G)}(R)$. □

Let $\mathcal{S}(R)$ denote the set of all subrings of R, and let $\mathcal{G}(R)$ denote the set of all subgroups of $\mathrm{Aut}(R)$. Note that $\mathcal{S}(R)$ and $\mathcal{G}(R)$ both are ordered with respect to set theoretic containment.

We set

$$S^{\gamma_R} := \mathrm{Aut}_S(R)$$

for each element S in $\mathcal{S}(R)$ and

$$G^{\phi_R} := \mathrm{Fix}_R(G)$$

for each element G in $\mathcal{G}(R)$.

Theorem 3.6

The following hold.

(i) *The pair (γ_R, ϕ_R) is a Galois pair with respect to the orders defined on $\mathcal{S}(R)$ and $\mathcal{G}(R)$, respectively, by set theoretic containment.*

(ii) *For each element α in $\mathrm{Aut}(R)$, we have $\gamma_R\alpha = \alpha\gamma_R$ and $\phi_R\alpha = \alpha\phi_R$.*

Proof. Set $\gamma := \gamma_R$ and $\phi := \phi_R$.

(i) From Lemma 3.3(i) we know that γ is a map from $\mathcal{S}(R)$ to $\mathcal{G}(R)$, from Lemma 3.2(i) that ϕ is a map from $\mathcal{G}(R)$ to $\mathcal{S}(R)$.

In Lemma 3.3(ii), we saw that $S \subseteq S^{\gamma\phi}$ for each element S in $\mathcal{S}(R)$, in Lemma 3.5 that $G \subseteq G^{\phi\gamma}$ for each element G in $\mathcal{G}(R)$.

In Lemma 3.3(iii), we saw that $T^\gamma \subseteq S^\gamma$ for any two elements S and T in $\mathcal{S}(R)$ with $S \subseteq T$, and in Lemma 3.2(iv), we saw that $G^\phi \subseteq H^\phi$ for any two elements G and H in $\mathcal{G}(R)$ with $H \subseteq G$.

(ii) Let α be an element in $\mathrm{Aut}(R)$.

For each element S in $\mathcal{S}(R)$, we have

$$S^{\gamma\alpha} = (S^\gamma)^\alpha = \mathrm{Aut}_S(R)^\alpha = \mathrm{Aut}_{S^\alpha}(R) = (S^\alpha)^\gamma = S^{\alpha\gamma};$$

cf. Lemma 3.4(ii). Thus, $\gamma\alpha = \alpha\gamma$.

For each element G in $\mathcal{G}(R)$, we have

$$G^{\phi\alpha} = (G^\phi)^\alpha = \mathrm{Fix}_R(G)^\alpha = \mathrm{Fix}_R(G^\alpha) = (G^\alpha)^\phi = G^{\alpha\phi};$$

cf. Lemma 3.2(iii). Thus, $\phi\alpha = \alpha\phi$. □

Theorem 3.6(i) shows that each ring gives rise to a Galois pair. The Galois pair discovered in Theorem 3.6(i) is the one which gave Galois Theory its name.

Let S be a subring of R, and recall from Section 1 that S is called galois with respect to (γ_R, ϕ_R) if $S = S^{\gamma_R\phi_R}$. Instead of saying that S is galois with respect to (γ_R, ϕ_R) one also says that R is *galois over* S. (This is similar to the terminology suggested in Section 2.) Thus, R is galois over S if and only if

$$S = \mathrm{Fix}_R(\mathrm{Aut}_S(R)).$$

Note also that a subgroup G of $\mathrm{Aut}(R)$ is galois with respect to (γ_R, ϕ_R) if

$$G = \mathrm{Aut}_{\mathrm{Fix}_R(G)}(R).$$

(This latter observation implies that $\{1\}$ is always galois.)

We now utilize Theorem 1.3(i) to give a different sufficient and necessary condition for subrings of R and subgroups of $\mathrm{Aut}(R)$ to be galois with respect to (γ_R, ϕ_R).

Lemma 3.7

We have the following.

(i) *Let S be a subring of R. Then R is galois over S if and only if there exists a subgroup G of $\mathrm{Aut}(R)$ such that $S = \mathrm{Fix}_R(G)$.*

(ii) *Let G be a subgroup of $\mathrm{Aut}(R)$. Then G is galois if and only if there exists a subring S of R such that $G = \mathrm{Aut}_S(R)$.*

PROOF. Considering Theorem 3.6(i) this follows from Theorem 1.3(i). □

The second part of the following lemma is a partial converse of Lemma 3.4(iii).

Lemma 3.8

Let S be a subring of R, and assume that R is galois over S. Let α be an element in $\mathrm{Aut}(R)$. Then the following hold.

(i) *The ring R is galois over S^α.*

(ii) *If $\mathrm{Aut}_S(R)^\alpha = \mathrm{Aut}_S(R)$, then $S^\alpha = S$.*

PROOF. Since R is assumed to be galois over S, $S = \mathrm{Fix}_R(\mathrm{Aut}_S(R)$. Thus,

$$S^\alpha = \mathrm{Fix}_R(\mathrm{Aut}_S(R))^\alpha = \mathrm{Fix}_R(\mathrm{Aut}_S(R)^\alpha);$$

cf. Lemma 3.2(iii).

(i) From Lemma 3.4(ii) we know that $\mathrm{Aut}_S(R)^\alpha = \mathrm{Aut}_{S^\alpha}(R)$. Thus, by the above equation, $S^\alpha = \mathrm{Fix}_R(\mathrm{Aut}_{S^\alpha}(R))$ and that means that R is galois over S^α.

(ii) Assume that $\mathrm{Aut}_S(R)^\alpha = \mathrm{Aut}_S(R)$. Then, the above equation yields

$$S^\alpha = \mathrm{Fix}_R(\mathrm{Aut}_S(R)) = S;$$

recall that R is assumed to be galois over S. □

Lemma 3.9

Let S and T be subrings of R with $S \subseteq T$, and assume that R is galois over S and over T. Assume that $\mathrm{Aut}_T(R)$ is normal in $\mathrm{Aut}_S(R)$. Then T is galois over S.

PROOF. Set $G := \mathrm{Aut}_S(R)$ and $H := \mathrm{Aut}_T(R)$.

Since H is assumed to be normal in G, we have $H^g = H$ for each element g in G. Thus, by Lemma 3.8(ii), $T^g = T$ for each element g in G.

Since $T^g = T$ for each element g in G, there exists, for each element g in G, an element k_g in $\mathrm{Aut}(T)$ which coincides with g on T. We define $K := \{k_g \mid g \in G\}$. Then $K \subseteq \mathrm{Aut}_S(T)$. Thus, as R is assumed to be galois over S, we obtain from Lemma 3.3(ii) and Lemma 3.2(iv) that

$$S \subseteq \mathrm{Fix}_T(\mathrm{Aut}_S(T)) \subseteq \mathrm{Fix}_T(K) \subseteq \mathrm{Fix}_R(G) = S.$$

It follows that $S = \mathrm{Fix}_T(\mathrm{Aut}_S(T))$, and that means that T is galois over S. □

Exercises

1. Define $\zeta := -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$. Compute ζ^2 and ζ^3.
2. Define $\mathbb{Q}[i] := \{a + bi \mid a, b \in \mathbb{Q}\}$.
   i. Is $3 - i \in \mathbb{Q}[i]$? How about $\frac{1}{2} + \frac{1}{3}i$, $\frac{1}{21} + \pi i$, $\frac{1}{\pi} + \frac{2}{3}i$, $\sqrt{2} + \frac{17}{3}i$, $\frac{5}{2}$, i, 17, 17, $\sqrt{17}$?
   ii. Show that $\mathbb{Q}[i]$ is a ring. Is $\mathbb{Q}[i]$ a field?
   iii. Show that $\kappa : \mathbb{Q}[i] \to \mathbb{Q}[i]$, $s + ti \mapsto s - ti$ is a bijective map.
   iv. Show that κ (as defined in iii.) is a ring homomorphism.
   v. From ii. and iii. we know that κ (as defined in iii.) is a ring automorphism. What are the fixed points of κ?

4. Finiteness and Integrality

Let R be a ring.

Let M be a module over R, let B be a non-empty subset of M.[7]

We define BR to be the intersection of all submodules of M which contain B. It is easy to see that BR consists of all finite sums $b_1r_1 + \ldots + b_nr_n$ with b_1, …, $b_n \in B$ and r_1, …, $r_n \in R$.

If $M = BR$, one says that the R-module M is *generated* by B or that B *generates* the R-module M.

Let S be a subring of R. Then R is a module over S. Let B be a non-empty subset of R. Then BS is the S-submodule of the S-module R generated by B. So, by the above, BS consists of all finite sums $b_1s_1 + \ldots + b_ns_n$ with b_1, …, $b_n \in B$ and s_1, …, $s_n \in S$. In the following lemma, we look at non-empty subsets of rings R which generate R as a module over a subring of R.

Lemma 4.1

Let U be a ring, and let S and T be subrings of U with $S \subseteq T$. Let B be a non-empty subset of T with $T = BS$, let C be a non-empty subset of U with $U = CT$, and define $D := \{bc \mid b \in B, c \in C\}$. Then we have $U = DS$.

Proof. It is clear that $DS \subseteq U$. To show that $U \subseteq DS$, we choose an element in U and denote it by u. We have to show that $u \in DS$.

Since $u \in U$ and $U = CT$, there exist elements c_1, …, c_n in C and t_1, …, t_n in T such that

$$u = c_1t_1 + \ldots c_nt_n.$$

Let j be an element in $\{1, \ldots, n\}$. Then, as $t_j \in T$ and $T = BS$, there exist elements

[7] Let G be a group, let R be a ring. A map from $G \times R$ to G is called a *scalar multiplication induced by R on G*.

Let R be a ring, let M be an additively written group endowed with a scalar multiplication induced by R. The set M is called a *right module over R* (or just a *module over R*) if $m \cdot 1 = m$ for each element m in M, if $(ms)t = m(st)$ and $m(s + t) = ms + mt$ for any three elements m in M and s and t in R, and $(k + l)r = kr + lr$ for any three elements k and l in M and r in R. Instead of right modules over R one also speaks about *right R-modules* (or just *R-modules*).

If R in the above definition is a field, the module M is called a *vector space* over R.

Modules naturally arise from rings and subrings. In fact, let R be a ring, and let S be a subring of R. Then R is a module over S. (In particular, if S is a subfield of R, R is a vector space over S.) The addition of the module R is just the addition of the ring R. The scalar multiplication is the restriction of the multiplication of R to $R \times S$.

A subgroup L of an R-module M is called an *R-submodule* (or just a *submodule*) of M if $lr \in L$ for any two elements l in L and r in R. Note that submodules of R-modules M are modules over R with respect to the addition and the scalar multiplication inherited from M.

b_{1j}, ..., $b_{m(j)j}$ in B and s_{1j}, ..., $s_{m(j)j}$ in S such that

$$t_j = b_{1j}s_{1j} + \ldots + b_{m(j)j}s_{m(j)j}.$$

It follows that

$$u = c_1b_{11}s_{11} + \ldots + c_1b_{m(1)1}s_{m(1)1} + \ldots + c_nb_{1n}s_{1n} + \ldots + c_nb_{m(n)n}s_{m(n)n},$$

and this proves the lemma. □

Let R be a ring, and let M be a module over R.

Let B be a non-empty subset of M. One says that B *generates* M *over* R or that M is *generated by* B *over* R if $M = BR$. The R-module M is said to be *finitely generated over* R if M is generated by a finite set over R. This means that M contains a finite set B such that $M = BR$.

Lemam 4.1 implies that a ring U is finitely generated over a subring S of U if U contains a subring T such that U is finitely generated over T and T is finitely generated over S. We will often just refer to this transitivity condition when we quote Lemma 4.1.

A subset B of M is called *linearly independent* if $r_1 = \ldots = r_k = 0$ for any k elements b_1, ..., b_k in B and any k elements r_1, ..., r_k in R satisfying $b_1r_1 + \ldots + b_kr_k = 0$.

A linearly independent subset of M which generates M over R is called a *basis* of M *over* R.

Note that finitely generated modules have finite bases. A fundamental result of E. Steinitz says that, if R is a field and M is finitely generated over R, then any two bases of M over R have the same cardinality. This cardinality is called the *dimension* of M *over* R and denoted by $\dim_R(M)$.

The concept of the dimension of a vector space plays an important role in the investigation of rings and their subfields.

Lemma 4.2

Let U be a ring, and let S and T be subfields of U with $S \subseteq T$. Assume that $\dim_S(T)$ *and* $\dim_T(U)$ *are finite. Then* $\dim_S(U) = \dim_S(T) \cdot \dim_T(U)$.

Proof. We are assuming that $\dim_S(T)$ is finite. Thus, T contains elements b_1, ..., b_m in T such that $B := \{b_1, \ldots, b_m\}$ is a basis of T over S. Similarly, as $\dim_T(U)$ is assumed to be finite, U contains elements c_1, ..., c_n such that $C := \{c_1, \ldots, c_n\}$ is a basis of U over T. We claim that

$$D := \{b_ic_j \mid i \in \{1, \ldots, m\},\ j \in \{1, \ldots, n\}\}$$

is a basis of U over S.

From Lemma 4.1 we know that $U = DS$. Thus, we shall be done if we succeed in showing that D is linearly independent over S.

Assume that S contains elements s_{ij} with $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, n\}$ such that

$$\sum_{j=1}^{n} \sum_{i=1}^{m} c_j b_i s_{ij} = 0.$$

Then, as C is a basis of U over T, we have

$$\sum_{i=1}^{m} b_i s_{ij} = 0$$

for each element j in $\{1, \ldots, n\}$. Thus, as B is a basis of T over S, we have $s_{ij} = 0$ for any two elements i in $\{1, \ldots, m\}$ and j in $\{1, \ldots, n\}$. □

Let T be a commutative ring, and let S be a subring of T.

An element t of T is called *algebraic over* S if S contains elements s_0, …, s_n such that

$$s_n t^n + s_{n-1} t^{n-1} + \cdots + s_1 t + s_0 = 0.$$

It is called *integral over* S if S contains elements s_0, …, s_{n-1} such that

$$t^n + s_{n-1} t^{n-1} + \cdots + s_1 t + s_0 = 0.$$

It is obvious that elements of T are algebraic over S if they are integral over S. Note also that the converse holds if S is a subfield of T. Thus, if S is a subfield of T, it does not make a difference whether an element of T is integral or algebraic over S. In this case, one usually prefers the latter terminlogy.

If S is a subfield of T, the elements in T which are not algebraic over S are called *transcendental over* S.

Note that elements in T which are integral (algebraic) over S are integral (algebraic) over each subring of T which contains S.

Here are examples of ring elements which are integral over a subring.

Set

$$\alpha := \sqrt{2} \qquad \text{and} \qquad i := \sqrt{-1}.$$

Then α and i are complex numbers which are integral over $\mathbb{Z}$. In fact, we have

$$\alpha^2 - 2 = 0 \qquad \text{and} \qquad i^1 + 1 = 0.$$

Other complex numbers which are integral over $\mathbb{Z}$ are

$$\zeta := -\frac{1}{2} + \frac{\sqrt{-3}}{2}, \qquad \omega := \frac{1}{2} + \frac{\sqrt{-3}}{2}, \qquad \sigma := -\frac{1}{2} + \frac{\sqrt{5}}{2}, \qquad \tau := \frac{1}{2} + \frac{\sqrt{5}}{2},$$

and $\rho := e^{2\pi i/5}$. In fact, we have

$$\zeta^2 + \zeta + 1 = 0, \qquad \omega^2 - \omega + 1 = 0, \qquad \sigma^2 + \sigma - 1 = 0, \qquad \tau^2 - \tau - 1 = 0,$$

and $\rho^5 = 1$.

Let T be a commutative ring, and let S be a subring of T.

We define $I_T(S)$ to be the set of all elements in T which are integral over S.

Note that

$$S \subseteq I_T(S) \subseteq T.$$

If $I_T(S) = T$, one says T is *integral over* S.[8]

If T is integral over S and S is a subfield of T and not just a subring of T, one also says that T is *algebraic over* S.

Note that $I_U(S) \subseteq I_U(T)$ for each commutative ring U and any two subrings S and T of U with $S \subseteq T$.

Lemma 4.3

Let T be an integral domain, let S be a subring of T, and assume that T is integral over S.[9] *Then S is a field if and only if T is a field.*

Proof. Assume first that S is a field, and let t be an element in $T \setminus \{0\}$. We have to show that t has a multiplicative inverse in T.

Since T is assumed to be integral over S, S contains elements s_0, ..., s_{n-1} such that

$$t^n + s_{n-1}t^{n-1} + \ldots + s_1 t + s_0 = 0.$$

We choose n as small as possible. Then, as T is assumed to be an integral domain, $s_0 \neq 0$. Thus, as S is assumed to be a field, s_0 is invertible. Thus, as

$$t(t^{n-1} + s_{n-1}t^{n-2} + \ldots + s_1) = t^n + s_{n-1}t^{n-1} + \ldots + s_1 t = -s_0,$$

$(t^{n-1} + s_{n-1}t^{n-2} + \ldots + s_1)(-s_0)^{-1}$ is a multiplicative inverse of t.

Assume now that T is a field. In order to show that then S is a field, we choose an element s in $S \setminus \{0\}$. We have to show that $s^{-1} \in S$.

Since T is assumed to be integral over S, s^{-1} is integral over S. Thus, S contains elements s_0, ..., s_{n-1} such that

$$s^{-n} + s_{n-1}s^{-(n-1)} + \ldots + s_1 s^{-1} + s_0 = 0.$$

[8] If $S = I_T(S)$, S is said to be *integrally closed in* T. Integrally closed subrings of commutative rings play an important role in ring theory, in particular rings which are intergrally closed in their field of fractions. However, they do not play a role in the present note.

[9] A commutative ring R is called an *integral domain* if products of non-zero elements of R are different from 0. The ring $\mathbb{Z}$ is an integral domain, the rings $\mathbb{Z}_6$ and $\mathbb{Z} \times \mathbb{Z}$ both are commutative, but they both are not integral domains.

Multiplying this equation by s^{n-1} we obtain

$$s^{-1} + s_{n-1} + s_{n-2}s + \ldots + s_1 s^{n-2} + s_0 s^{n-1} = 0.$$

It follows that

$$s^{-1} = -(s_{n-1} + s_{n-2}s + \ldots + s_1 s^{n-2} + s_0 s^{n-1}) \in S,$$

and that finishes the proof. □

Lemma 4.4

Let R be a commutative ring, let n be a positive integer, let M be an $n \times n$-matrix with entries in R, and let v be an element in R^n with $vM = 0$. Then $v\det(M) = 0$.

Proof. This follows easily by induction. □

Lemma 4.5

Let T be a commutative ring, and let S be a subring of T. Assume that T is finitely generated over S. Then T is integral over S.

Proof. Since T is finitely generated over S, T contains a finite subset B such that $T = BS$. Note that B is not empty.

Let t be an element in T. We have to show that t is integral over S.

Since B is a non-empty finite set, there exist elements b_1, …, b_n in T such that

$$B = \{b_1, \ldots, b_n\}.$$

Let j be an element in $\{1, \ldots, n\}$. Then, $b_j t \in T$. Thus, as $T = BS$, $b_j t \in BS$. Thus, for each element i in $\{1, \ldots, n\}$, there exists an element s_{ij} in S such that

$$b_j t = b_1 s_{1j} + \ldots + b_n s_{nj}.$$

We define

$$v := (b_1, \ldots, b_n).$$

and

$$M := \begin{pmatrix} s_{11} & s_{12} & \ldots & s_{1n} \\ s_{21} & s_{22} & \ldots & s_{2n} \\ \vdots & \vdots & & \vdots \\ s_{n1} & s_{n2} & \ldots & s_{nn} \end{pmatrix}.$$

Then

$$vt = (b_1, \ldots, b_n)t = (b_1, \ldots, b_n) \begin{pmatrix} s_{11} & s_{12} & \ldots & s_{1n} \\ s_{21} & s_{22} & \ldots & s_{2n} \\ \vdots & \vdots & & \vdots \\ s_{n1} & s_{n2} & \ldots & s_{nn} \end{pmatrix} = vM.$$

It follows that $v(tI - M) = 0$. Thus, by Lemma 4.4, $v \det(tI - M) = 0$. Thus, as $v = (b_1, \ldots, b_n)$, $b_i \det(tI - M) = 0$ for each element i in $\{1, \ldots, n\}$. Thus, as $1 \in T = BS$, $\det(tI - M) = 0$.

Now observe that $\det(tI - M)$ is of the form

$$t^n + s_{n-1}t^{n-1} + \cdots + s_1 t + s_0$$

with $s_0, \ldots, s_{n-1} \in S$. Thus, t is integral over S. □

Let T be a commutative ring. For each subset A of T, we define $S[A]$ to be the intersection of all subrings of T which contain $S \cup A$ as a subset. If A consists of a single element a, then we write $S[a]$ instead of $S[A]$.

Proposition 4.6

Let T be a commutative ring, let S be a subring of T, and let A be a finite subset of T. Then the following conditions are equivalent.

(a) *We have $A \subseteq I_T(S)$.*

(b) *The ring $S[A]$ is finitely generated over S.*

(c) *The ring $S[A]$ is integral over S.*

Proof. (a) ⇒ (b) There is nothing to show if A is empty. Therefore, we assume that A is not empty, and we choose an element a in A.

By induction, $S[A]$ is finitely generated over $S[a]$. Thus, we shall be done if we succeed in showing that $S[a]$ is finitely generated over S; cf. Lemma 4.1.

Since $a \in I_T(S)$, we find elements $s_0, \ldots, s_{n-1}$ in S such that

$$a^n + s_{n-1}a^{n-1} + \ldots + s_1 a + s_0 = 0.$$

Set $A' := \{a^0, \ldots, a^{n-1}\}$. Then $a^n \in A'S$. Thus,

$$S[a] \subseteq A'S.$$

On the other hand, we obviously have $A'S \subseteq S[a]$. Thus, $S[a] = A'S$, so that $S[a]$ is finitely generated over S.

(b) ⇒ (c) This is a consequence of Lemma 4.5.

(c) ⇒ (a) This follows from the definition of the set $I_T(S)$. □

A common application of Proposition 4.6 is the following. Let T be an integral domain, let S be a subfield of T, and let t be an element in $I_T(S)$. Then, by Proposition 4.6, $S[t]$ is integral over S. Thus, as S is a field, so is $S[t]$; cf. Lemma 4.3.

The following theorem is similar to Lemma 4.1. It will have a counterpart also in Theorem 9.7. It says that integrality is transitive.

Theorem 4.7 [R. Dedekind]

Let U be a commutative ring, and let S be a subring of U. Assume that U contains a subring T such that T is integral over S and U is integral over T. Then U is integral over S.

Proof. Let u be an element in U. We have to show that u is integral over S.

Since U is assumed to be integral over T, T contains elements t_0, ..., t_{n-1} such that

$$u^n + t_{n-1}u^{n-1} + \ldots + t_1 u + t_0 = 0.$$

Set $A := \{t_0, \ldots, t_{n-1}\}$. Then $A \subseteq T$. Thus, as T is assumed to be integral over S, $A \subseteq I_U(S)$. Thus, by Proposition 4.6, $S[A]$ is finitely generated over S.

On the other hand, $u \in I_U(S[A])$. Thus, by Proposition 4.6, $S[A][u]$ is finitely generated over $S[A]$.

Now, as $S[A][u]$ is finitely generated over $S[A]$ and $S[A]$ is finitely generated over S, $S[A][u]$ is finitely generated over S; cf. Lemma 4.1. Thus, by Proposition 4.6, $S[A][u]$ is integral over S. In particular, u is integral over S. □

Theorem 4.8 [R. Dedekind]

Let T be a commutative ring, and let S be a subring of T. Then $I_T(S)$ is a subring of T.

Proof. Let p and q be elements in $I_T(S)$, and set $A := \{p, q\}$. Then, by Proposition 4.6, $S[A] \subseteq I_T(S)$.

Since p, $q \in S[A]$ and $S[A]$ is a subring of T, $p - q \in S[A]$ and $pq \in S[A]$. Thus, $p - q \in I_T(S)$ and $pq \in I_T(S)$. □

Lemma 4.9

Let T be a commutative ring, let S be a subring of T, let t be an element of T, and assume that t is transcendental over S. Let R be a commutative ring, let ϕ be a ring homomorphism from S to R, and let r be an element in R. Then there exists exactly one ring homomorphism from $S[t]$ to $S^\phi[r]$ which coincides with ϕ on S and sends t to r.

Proof. Each element of $S[t]$ has the form $s_n t^n + \ldots + t_1 r + t_0$ with s_0, s_1, ..., s_n in S. We define

$$\chi(s_n t^n + \ldots + s_1 t + s_0) = \phi(s_n)r^n + \ldots + \phi(s_1)r + \phi(s_0)$$

for any $n+1$ elements s_0, s_1, ..., s_n in S. Then χ is a ring homomorphism from $S[t]$ to $S^\phi[r]$, and it is also the only ring homomorphism from $S[t]$ to $S^\phi[r]$.

The definition of χ also implies that $\chi|_S = \phi$. □

We emphasize that it does not matter whether, in Lemma 4.9, the element r in R is integral over S^ϕ or not.

Let T be a commutative ring, let S be a subfield of T, let t be an element of T, and assume that t is transcendental over S. Let R be a commutative ring, let ϕ be a ring homomorphism from S to R, and let r be an element in R. We want to fix notation and terminology for two specific cases.

If r is transcendental over S^ϕ, the uniquely determined ring homomorphism from $S[t]$ to $S^\phi[r]$ which coincides with ϕ on S and sends t to r will be denoted by $\hat{\phi}$. If we follow the common practice to denote ring elements which are transcendental over subfields by X, then $\hat{\phi}$ denotes the uniquely determined ring homomorphism from $S[t]$ to $S^\phi[r]$ which sends each element s in S to s^ϕ and X to X.

If ϕ happens to be the identity on S and r is algebraic over S^ϕ, the uniquely determined ring homomorphism from $S[X]$ to $S[r]$ which fixes each element in S and sends X to r is called the *substitution homomorphism defined by* S and t. (Note that the substitution homomorphism defined by S and t is an S-homomorphism in the sense of Section 3.)

Exercises

1. (Just to warm up.) Verify the five equations on top of page 20.
2. Give the definition of $I_{\mathbb{Q}}(\mathbb{Z})$, answer the following questions, and give reasons for your answers.
   i. Is $\frac{1}{2}$ integral over $\mathbb{Z}$?
   ii. Let n be a positive integer. Is $\frac{1}{n}$ integral over $\mathbb{Z}$?
   iii. Let m and n be integers, and assume that $n \neq 0$. Is $\frac{m}{n}$ integral over $\mathbb{Z}$?
   iv. Which rational numbers belong to $I_{\mathbb{Q}}(\mathbb{Z})$?

5. The Minimal Polynomial

Let T be a commutative ring, let S be a subfield of T, and let t be an element in $I_T(S)$.

From Lemma 4.9 we know that that there exists a uniquely determined S-homomorphism from the polynomial ring $S[X]$ to $S[t]$ which maps X to t. Recall that this S-homomorphism is called the substitution homomorphism defined by S and t.

Let ϕ denote the substitution homomorphism defined by S and t.

Recall that $\ker(\phi)$ is an ideal of $S[X]$. Moreover, as $t \in I_T(S)$, $\ker(\phi) \neq \{0\}$. On the other hand, since S is assumed to be a commutative field, $S[X]$ is a euclidean domain and, thus, a principal ideal domain. It follows that $S[X]$ contains exactly one monic polynomial p satisfying $\ker(\phi) = pS[X]$. This polynomial is called the *minimal polynomial* of t *over* S and will be denoted by $\min_S(t)$.

The following lemma shows that minimal polynomials are the source of useful information as soon as T is an integral domain. It is for this reason that, within this section, all commutative rings are integral domains.[10]

Let R be a commutative ring, and let q be a polynomial with coefficients in R. Then q is called a polynomial *over* R. If a polynomial p over R divides a polynomial q over R in the polynomial ring over R, we also say that p *divides* q *over* R.

Lemma 5.1

Let T be an integral domain, let S be a subfield of T, and let t be an element in $I_T(S)$. Then the following hold.

(i) *The polynomial $\min_S(t)$ is irreducible over S.*

(ii) *Set $n := \deg(\min_S(t))$. Then $\{1, t, t^2, \ldots, t^{n-1}\}$ is a basis of $S[t]$ over S.*

(iii) *We have $\deg(\min_S(t)) = \dim_S(S[t])$.*

Proof. (i) Set $p := \min_S(t)$. Then $p \neq 0$. Let ϕ denote the substitution homomorphism defined by S and t. Then, by definition, $\ker(\phi) = pS[X]$.

On the other hand, as $S[X]/\ker(\phi) \cong \mathrm{im}(\phi)$ is an integral domain, we obtain that $\ker(\phi)$ is a prime ideal of $S[X]$. Thus, as $\ker(\phi) = pS[X]$, $pS[X]$ is a prime ideal of $S[X]$. Thus, as $p \neq 0$, p is prime over S.

Recall that S is assumed to be a field. Thus, $S[X]$ is an integral domain. Thus, as p is prime over S, p is irreducible over S.

(ii) Set $B := \{1, t, t^2, \ldots, t^{n-1}\}$ and $p := \min_S(t)$.

From $p = \min_S(t)$ we obtain that $n = \deg(p)$. Thus, there exist elements s_0, …, s_{n-1}

[10] In the first four results, we always have the same setting: T is an integral domain, S is a subfield of T, and t is an element in $I_T(S)$.

in S such that

$$p = X^n + s_{n-1}X^{n-1} + \ldots + s_1X + s_0.$$

Let ϕ denote the substitution homomorphism defined by S and t. Then $\phi(X) = t$, so

$$\begin{aligned}\phi(p) &= \phi(X^n + s_{n-1}X^{n-1} + \ldots + s_1X + s_0)\\ &= \phi(X)^n + \phi(s_{n-1})\phi(X)^{n-1} + \ldots + \phi(s_1)\phi(X) + \phi(s_0)\\ &= t^n + s_{n-1}t^{n-1} + \ldots + s_1t + s_0.\end{aligned}$$

On the other hand, $p \in \ker(\phi)$. Thus, $\phi(p) = 0$. It follows that

$$t^n + s_{n-1}t^{n-1} + \ldots + s_1t + s_0 = 0.$$

This shows that $t^n \in BS$. Induction now yields $S[t] = BS$.

To prove that B is linearly independent over S we choose elements s_0, s_1, …, s_{n-1} in S with

$$s_{n-1}t^{n-1} + \ldots + s_1t + s_0 = 0.$$

By way of contradiction, we assume that $\{s_0, s_1, \ldots, s_{n-1}\} \neq \{0\}$.

Define

$$q := s_{n-1}X^{n-1} + \ldots + s_1X + s_0.$$

Then $q \neq 0$ and $\deg(q) \leq n-1$. Furthermore,

$$\begin{aligned}\phi(q) &= \phi(s_{n-1}X^{n-1} + \ldots + s_1X + s_0)\\ &= \phi(s_{n-1})\phi(X)^{n-1} + \ldots + \phi(s_1)\phi(X) + \phi(s_0)\\ &= s_{n-1}t^{n-1} + \ldots + s_1t + s_0,\end{aligned}$$

whence $\phi(q) = 0$. It follows that $q \in \ker(\phi)$. Thus, as $\ker(\phi) = pS[X]$, p divides q in $S[X]$. As a consequence, $\deg(p) \leq \deg(q) \leq n-1$, contradiction.

This shows that $s_i = 0$ for each element i in $\{0, \ldots, n-1\}$. Thus, B is linearly independent over S.

(iii) This follows from (ii). □

It might be worth mentioning that Lemma 5.1(i) is false if T is just a commutative ring and not an integral domain. For instance, if $T = S \times S$ and $t := (1, 0)$. Then t is a root of $X^2 - X$, but $X^2 - X$ is not irreducible.

Let T be an integral domain, let S be a subfield of T.

Let q be a polynomial over S. An element t of T is said to be a *root* of q in T if q is in the kernel of the substitution homomorphism defined by S and t.

Note that, if u and v are elements of T and v is a root of $\min_S(u)$, then $\min_S(u) = \min_S(v)$.

Let T and R be integral domains, let S be a subfield of T, let t be an element in T, let r be an element in R, and let ϕ be a ring isomorphism from S to R. Under which circumstances can ϕ be extended to $S[t]$ in such a way that t is mapped to r?[11] In other words, we want to know under which conditions one can find a ring homomorphism from $S[t]$ to $S^\phi[r]$ which coincides with ϕ on S and maps t to r. (Since each ring homomorphism from $S[t]$ to a commutative ring is uniquely determined by its values on S and on t, we certainly cannot have two distinct such homomorphisms.)

From Lemma 4.9 we know that such a ring homomorphism exists if t is transcendental, no matter whether r is trancendental over S^ϕ or not. In the second part of the following lemma, we will see that, if t is algebraic over S, then such a ring homomorphism exists if and only if r is algebraic over U and the minimal polynomials of t and r "are equal modulo $\hat{\phi}$".

Lemma 5.2 [Homomorphisms and Minimal Polynomials]
Let T be an integral domain, let S be a subfield of T, and let t be an element in $I_T(S)$. Then we have the following.

(i) *Let ϕ be a ring homomorphism from T to a commutative ring, and set $\iota := \phi|_S$. Then $t^\phi \in I_{T^\phi}(S^\phi)$ and $\min_S(t)^{\hat{\iota}} = \min_{S^\phi}(t^\phi)$.*

(ii) *Let R be an integral domain, and let ι be a ring homomorphism from S to R. Let r be an element in $I_R(S^\iota)$, and assume that $\min_S(t)^{\hat{\iota}} = \min_{S^\iota}(r)$. Then there exists exactly one ring homomomorphism from $S[t]$ to R which coincides with ι on S and sends t to r.*

Proof. Let χ denote the substitution homomorphism defined by S and t, and set $p := \min_S(t)$. Then $\ker(\chi) = pS[X]$.

(i) The composite $\chi\phi$ is a ring homomorphism from $S[X]$ to $S^\phi[t^\phi]$. Since $\hat{\iota}$ is a ring isomorphism from $S[X]$ to $S^\phi[X]$, $\psi := \hat{\iota}^{-1}\chi\phi$ is a ring homomorphism from $S^\phi[X]$ to $S^\phi[t^\phi]$. Since χ is an S-homomorphism, ψ is an S^χ-homomorphism. Note also that $X^\psi = t^\phi$. Thus, ψ is the substitution homomorphism defined by S^ϕ and t^ϕ.

Since $p \in \ker(\chi)$, $p^\chi = 0$. Thus, $(p^{\hat{\iota}})^\psi = p^{\hat{\iota}\psi} = p^{\chi\phi} = 0$. Since ψ is the substitution homomorphism defined by S^ϕ and t^ϕ, this implies that $\min_{S^\phi}(t^\phi)$ divides $p^{\hat{\iota}}$ over S^ϕ.

On the other hand, as p is irreducible and monic and $\hat{\iota}$ is a ring isomorphism, $p^{\hat{\iota}}$ is irreducible and monic. Thus, as $\min_{S'}(t^\phi)$ is monic, $p^{\hat{\iota}} = \min_{S^\phi}(t^\phi)$.

(ii) Let ψ denote the substitution homomorphism defined by S^ι and r. We are assuming that $p^{\hat{\iota}} = \min_{S^\iota}(r)$. Thus, r is a root of $p^{\hat{\iota}}$. It follows that $p^{\hat{\iota}} \in \ker(\psi)$, and then that $p \in \ker(\hat{\iota}\psi)$.

From $\ker(\chi) = pS[X]$ and $p \in \ker(\hat{\iota}\psi)$ we obtain that $\ker(\chi) \subseteq \ker(\hat{\iota}\psi)$. Thus, as χ is

[11] The question is reasonable also under the weaker hypothesis that T and R are just commutative rings and S is a subring of T.

surjective, there exists a ring homomorphism ϕ from $S[t]$ to R such that $\chi\phi = \hat{\iota}\psi$.[12] Since χ is an S-homomorphism and ψ an S^ι-homomorphism, we now have

$$s^\phi = (s^\chi)^\phi = s^{\chi\phi} = s^{\hat{\iota}\psi} = (s^\iota)^\psi = s^\iota$$

for each element s in S. From $X^\chi = t$ and $X^\psi = r$ we also obtain that

$$t^\phi = (X^\chi)^\phi = X^{\chi\phi} = X^{\hat{\iota}\psi} = (X^{\hat{\iota}})^\psi = r.$$

The uniqueness of ϕ follows from the fact that each S homomorphism from $S[t]$ to R is determined by the image of t. □

Lemma 5.2(ii) should be seen in connection with Lemma 7.10 and Lemma 7.12.

We now apply Lemma 5.2 to a specific situation.

Corollary 5.3

Let T be an integral domain, let S be a subfield of T, and let t be an element in $I_T(S)$. Then we have the following.

(i) *Each S-homomorphism from $S[t]$ to T sends t to a root of $\min_S(t)$.*

(ii) *For each root u of $\min_S(t)$ in T, there exists exactly one S-homomorphism from $S[t]$ to T which sends t to u.*

(iii) *The number of roots of $\min_S(t)$ in T is equal to the number of S-homomorphisms from $S[t]$ to T.*

Proof. (i) Let ϕ be an S-homomorphism from $S[t]$ to T. Applying Lemma 5.2(i) to $S[t]$ in place of T we obtain that $t^\phi \in I_T(S)$ and $\min_S(t) = \min_S(t^\phi)$. Thus, as t^ϕ is a root of $\min_S(t^\phi)$, t^ϕ is a root of $\min_S(t)$.

(ii) Let u be a root of $\min_S(t)$ in T. Then applying Lemma 5.2(ii) to T and u in place of R and r, we obtain that there exists exactly one S-homomorphism from $S[t]$ to T which sends t to u.[13]

(iii) From (i) we know that there exists a map from the set of all S-homomorphism from $S[t]$ to T to the set of all roots of $\min_S(t)$ in T which sends each S-homomorphism ϕ from $S[t]$ to T to $\phi(t)$. By (ii), this map is bijective. □

The following corollary is related to Corollary 8.3.

Corollary 5.4

[12] Let u be an element in $S[t]$. Since χ is surjective, $S[X]$ contains an element q such that $q^\chi = u$. We define $u^\phi := q^{\hat{\iota}\psi}$ and claim that ϕ does not depend on the choice of q in $S[X]$. Let o be an element in $S[X]$ with $o^\chi = u$. Then $(q-o)^\chi = q^\chi - o^\chi = 0$, so $q - o \in \ker(\chi) \subseteq \ker(\hat{\iota}\psi)$. It follows that $q^{\hat{\iota}\psi} = o^{\hat{\iota}\psi}$.

[13] The map from S to T which sends each element of S to itself takes over the role of ι in the application of Lemma 5.2(ii).

Let T be an integral domain, let S be a subfield of T, and let q be a polynomial over S. Then $\mathrm{Aut}_S(T)$ acts on the set of the roots of q in T.

PROOF. Let t be a root of q in T, and let α be an element in $\mathrm{Aut}_S(T)$. We have to show that t^α is a root of q in T.

Set $\phi = \alpha|_{S[t]}$. Then ϕ is an S-homomorphism from $S[t]$ to T. Thus, by Corollary 5.3(i), t^ϕ is a root of $\min_S(t)$. Thus, as $t^\alpha = t^\phi$, t^α is a root of $\min_S(t)$.

Since t is a root of q in T, q is in the kernel of the substitution homomorphism defined by S and t. Thus, $\min_S(t)$ divides q over S. Thus, as t^α is a root of $\min_S(t)$ in T, t^α is a root of q in T. □

We continue with two applications of Corollary 5.4 which will be needed only in Section 12. We will apply Lemma 5.5 in Lemma 12.5 and Lemma 5.6 in Lemma 12.2.

Let R be a commutative field.

An element r in R is called a *root of unity* if $r^k = 1$ for some positive integer k.

Note that roots of unity of R are nothing but elements of $R \setminus \{0\}$ which have a finite order in the group of units $R^\times$ of R.

Let n be a positive integer.

An element r in R which satisfies $r^n = 1$ is called an n-th *root of unity*. An n-th root of unity r is called *primitive* if $r^m \neq 1$ for each element m in $\{1, \ldots, n-1\}$.

Note that a primitive n-th root of unity of R is nothing but an element of order n in the group of units $R^\times$ of R. Thus, R contains a primitive n-th root of unity if and only if $R^\times$ contains a finite cyclic subgroup of order n.[14]

Lemma 5.5

Let T be a commutative field, let S be a subfield of T, and let t be a root of unity of T. Then $\mathrm{Aut}_S(S[t])$ is isomorphic to a subgroup of $\mathrm{Aut}(\langle t\rangle)$. (In particular, $\mathrm{Aut}_S(S[t])$ is commutative.)

PROOF. Since t is a root of unity of T, there exists a positive integer k such that $t^k = 1$. Let n denote the smallest positive integer k satisfying $t^k = 1$. Then $u^n = 1$ for each element u in $\langle t\rangle$. Thus, the n elements of $\langle t\rangle$ are exactly the roots of $X^n - 1$ in T.

Now recall from Corollary 5.4 that $\mathrm{Aut}_S(T)$ acts on the set of the roots of $X^n - 1$ in T. Thus, $\mathrm{Aut}_S(T)$ acts on $\langle t\rangle$. In other words, we have $t^g \in \langle t\rangle$ for each element g in $\mathrm{Aut}_S(S[t])$. It follows that

$$\phi\colon\ \mathrm{Aut}_S(S[t]) \to \mathrm{Aut}(\langle t\rangle),\ g \mapsto g|_{\langle t\rangle}$$

[14]From Theorem 5.8 we will see that the group of units $R^\times$ of R has at most one cyclic subgroup of order n. Thus, the set of all n-th roots of unity is a cyclic subgroup of $R^\times$. Any generator of this group is a primitive n-th root of unity.

is a group homomorphism.

Since the identity on $S[t]$ is the only element in $\mathrm{Aut}_S(S[t])$ which fixes each element in $\langle t\rangle$, $\ker(\phi) = \{1\}$. Thus, ϕ is injective. It follows that $\mathrm{Aut}_S(S[t])$ is isomorphic to a subgroup of $\mathrm{Aut}(\langle t\rangle)$.

Since $\langle t\rangle$ is cyclic, $\mathrm{Aut}(\langle t\rangle)$ is commutative.[15] Thus, as $\mathrm{Aut}_S(S[t])$ is isomorphic to a subgroup of $\mathrm{Aut}(\langle t\rangle)$, $\mathrm{Aut}_S(S[t])$ is commutative. □

The following lemma is related to Lemma 10.5.

Lemma 5.6

Let T be a commutative field, let S be a subfield of T, let t be an element in $T \setminus \{0\}$, and let s be an element in $S \setminus \{0\}$. Assume that there exists a positive integer n with $t^n \in S$ and $s^n = 1$. Then

$$\phi\colon\ \mathrm{Aut}_S(T)\ \to\ \langle s\rangle,\ g\ \mapsto\ t^{-1}t^g$$

is a group homomorphism with $\ker(\phi) = \mathrm{Aut}_{S[t]}(T)$.

Proof. Set $G := \mathrm{Aut}_S(T)$ and $q := X^n - t^n$. Since $t^n \in S$, q is a polynomial over S. Thus, by Corollary 5.4, G acts on the set of the roots of q in T.

Note that $\{t, st, \ldots, s^{n-1}t\}$ is the set of the roots of q in T. Thus, we have $t^{-1}t^g \in \langle s\rangle \subseteq S$ for each element g in G, so that $(t^{-1}t^d)^e = t^{-1}t^d$ for any two elements d and e in G. Now

$$\phi(de) = t^{-1}t^{de} = t^{-1}(t^d)^e = t^{-1}t^e(t^{-1})^e(t^d)^e = (t^{-1}t^e)(t^{-1}t^d)^e = \phi(d)\phi(e)$$

for any two elements d and e in G, and that shows that ϕ is a group homomorphism.

Let g be an element in $\ker(\phi)$. Then $\phi(g) = 1$, so $t^{-1}t^g = 1$, and that means that $t^g = t$. Then $g \in \mathrm{Aut}_{S[t]}(T)$. Conversely, for each element g in $\mathrm{Aut}_{S[t]}(T)$, we have $t^g = t$, and then $t^{-1}t^g = 1$. Thus, $\phi(g) = 1$, so $g \in \ker(\phi)$. It follows that $\ker(\phi) = \mathrm{Aut}_{S[t]}(T)$. □

An example of Lemma 5.6 is

$$T = \mathbb{C}, \qquad S = \mathbb{Q}, \qquad t = \sqrt[3]{2}, \qquad s = -\frac{1}{2} + \frac{\sqrt{-3}}{2}, \qquad \text{and} \qquad n = 3.$$

Let R be a commutative field, and let G be a subgroup of $\mathrm{Aut}(R)$.

Recall from Section 2 that $\mathrm{Fix}_R(G)$ is our notation of the set of all elements r in R satisfying $r^g = r$ for each element g in G. From Lemma 3.2(i) we know that $\mathrm{Fix}_R(G)$ is a subring of R. From Lemma 3.2(ii) we know that $\mathrm{Fix}_R(G)$ is even a subfield of R, since R is a field. By Theorem 1.3(i), R is also galois over $\mathrm{Fix}_R(G)$.

Note that G acts on R, and recall that r^G is our notation of the set of all elements r^g with $g \in G$.

[15] This is an easy observation.

Lemma 5.7

Let T be a commutative field, let G be a subgroup of $\mathrm{Aut}(T)$, and set $S := \mathrm{Fix}_T(G)$. Let t be an element in T, assume that $|t^G|$ is finite, and set

$$p := \prod_{u \in t^G} (X - u).$$

Then the following hold.

(i) *We have $p \in S[X]$.*

(ii) *The element t is algebraic over S.*

(iii) *We have $p = \min_S(t)$.*

(iv) *We have $\dim_S(S[t]) = |t^G|$.*

Proof. (i) Let g be an element in G. Recall that $\hat{g}$ is our notation of the uniquely defined ring automorphism of $T[X]$ which satisfies $\hat{g}|_T = g$ and $X^{\hat{g}} = X$. Since g acts on t^G, $\hat{g}$ acts on t^G. Since $\hat{g}$ fixes X, $\hat{g}$ fixes p. Thus, $\hat{g}$ fixes each coefficient of p. Thus, as $\hat{g}|_T = g$, g fixes each coefficient of p.

Since g has been chosen arbitrarily in G, we have shown that all coefficients of p belong to S. Thus, $p \in S[X]$.

(ii) Let ϕ denote the substitution homomorphism defined by S and t. From (i) we know that $p \in S[X]$. Thus, ϕ applies to p. Since $t \in t^G$, $p^\phi = 0$, and this means that $p \in \ker(\phi)$. It follows that $\ker(\phi) \neq \{0\}$, so that t is algebraic over S.

(iii) Let ϕ denote the substitution homomorphism defined by S and t. From (i) we know that $p \in S[X]$. Thus, ϕ applies to p. Since $t \in t^G$, $p^\phi = 0$, and this means that $p \in \ker(\phi)$. Thus, by definition, $\min_S(t)$ divides p in $S[X]$.

Let g be an element in G. Then, as t is a root of $\min_S(t)$, t^g is a root of $\min_S(t)$ in T; cf. Corollary 5.4. Thus, $X - t^g$ divides $\min_S(t)$ in $T[X]$. Thus, as g has been chosen arbitrarily in G, we conclude that p divides $\min_S(t)$ in $T[X]$. Thus, as p and $\min_S(t)$ both are monic, $p = \min_S(t)$.

(iv) From Lemma 5.1(iii) we know that $\deg(\min_S(t)) = \dim_S(S[t])$. From (iii) we obtain $\deg(\min_S(t)) = |t^G|$. Thus, $\dim_S(S[t]) = |t^G|$. □

Let R be a commutative field, and let G be a subgroup of $\mathrm{Aut}(R)$. From Lemma 5.7(ii) we obtain that R is algebraic over $\mathrm{Fix}_R(G)$. Later, we will see that R is even finitely generated over $\mathrm{Fix}_R(G)$ if G is a finite group. In fact, in Theorem 6.4(ii), we will see that the dimension of R over $\mathrm{Fix}_R(G)$ is just $|G|$.

The following theorem will needed in Lemma 5.9 and in Theorem 9.9. Both of these results, however, will not be needed in the remainder of these notes. We will take advantage of Theorem 5.8 in Section 11, Section 12, and Section 13.

Theorem 5.8

Let R be an integral domain. Then each finite subgroup of $R^\times$ is cyclic.

PROOF. Let G be a finite subgroup of $R^\times$. We choose an element r in G such that the order of r is as large as possible and set $n := o(r)$. Then, $o(g)$ divides n for each element g in G.[16] It follows that $g^n - 1 = 0$ for each element g in G. Thus, each element in G is a root of $X^n - 1$, so $X^n - 1$ has at least $|G|$ roots in R. On the other hand, we know that $X^n - 1$ has at most n roots in R. Thus, $|G| \leq n$.

Now recall that $n = o(r)$ implies that $|\langle r\rangle| = n$. Thus, as $\langle r\rangle \subseteq G$, $G = \langle r\rangle$, and that shows that G is cyclic. □

As a consequence of Theorem 5.8 one obtains that the group of units of a finite integral domain is cyclic.[17] Later (in Theorem 11.2) we will see that finite fields are generally commutative, so that the group of units of each finite field is cyclic.

Theorem 5.8 is also useful in the proof of the following lemma.

A commutative field T is said to be *primitive over* a subfield S of T if $T = S[t]$ for some element t in $I_T(S)$.[18]

Recall from Proposition 4.6 that a commutative ring T is finitely generated over a subring S of T if T is primitive over S. The following lemma is a partial converse of this observation. It will not be needed in the remainder of these notes.

Lemma 5.9 [E. STEINITZ–E. ARTIN]

Let T be a commutative field, let S be a subfield of T, and assume that T is finitely generated over S. Assume that T possesses just finitely many subfields containing S. Then T is primitive over S.

PROOF. The field T is clearly primitive over S if $S = T$. Therefore, we assume that $S \neq T$. In this case, we find an element t in T such that $t \notin S$.

We are assuming that T is finitely generated over S. Thus, by Lemma 4.5, T is algebraic over S. In particular, $S[t]$ is algebraic over S. Thus, as S is a field, so is $S[t]$; cf. Lemma 4.3. Thus, by induction (on the number of subfields of T containing S), T contains an element u such that $T = S[t][u] = S[t, u]$.

Assume first that $|S|$ is finite. Then T is finite, since T is assumed to be finitely generated over S. Thus, by Theorem 5.8, $T^\times$ is cyclic. It follows that $T = S[r]$ for each generator r of the cyclic group $T^\times$.

[16] Let g be an element in G, and let p be a prime divisor of $o(g)$. Then there exist natural numbers d and e and positive integers m and n such that g.c.d.$(p, mn) = 1$, $o(g) = p^d m$, and $o(r) = p^e n$. Set $k := g^m$ and $l := r^{p^e}$. Then $o(k) = p^d$ and $o(l) = n$. Thus, as G is assumed to be commutative and p does not divide n, $o(kl) = p^d n$. Thus, the choice of r forces $d \leq e$. Since p has been chosen arbitrarily among the prime divisors of $o(g)$, we have shown that $o(g)$ divides $o(r)$.

[17] Finite integral domains are commutative fields.

[18] It is reasonable to define a commutative ring T to be primitive over a subring S of T if $T = S[t]$ for some element t in $I_T(S)$. However, we do not need this more general definition.

Assume now that $|S|$ is infinite. Then, as T is assumed to have just finitely many subfields containing S, there exist elements p and q in S such that $p \neq q$ and

$$S[t + pu] = S[t + qu].$$

It follows that $(q-p)u \in S[t+qu]$. Thus, as $q-p \in S \setminus \{0\}$, $u \in S[t+qu]$. (Recall that S is a field.) Thus, as $q \in S$, $qu \in S[t+qu]$. It follows that $t \in S[t+qu]$, so that

$$T = S[t, u] \subseteq S[t + qu] \subseteq T.$$

This finishes the proof. □

Exercises

1. Determine the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$.
2. Determine the minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}$.
3. Determine the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$.
   i. Set $x := \sqrt{2} + \sqrt{3}$. Bring $\sqrt{2}$ to the other side.
   ii. Square the resulting equation.
   iii. Bring the linear part on one side, the quadratic part and the absolute part on the other side.
   iv. Square the resulting equation.
   v. Show that the resulting polynomial is irreducible over $\mathbb{Q}$.
4. Determine $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\sqrt{2} + \sqrt{3}])$.
   i. Show first that $\mathbb{Q}[\sqrt{2} + \sqrt{3}] = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. (This is easy, since, by definition, $\sqrt{2} + \sqrt{3} \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$, so $\mathbb{Q}[\sqrt{2}+\sqrt{3}] \subseteq \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. On the other hand, $(\sqrt{2}+\sqrt{3})(\sqrt{2}-\sqrt{3}) = -1$, so $\sqrt{2} - \sqrt{3} = (\sqrt{2} + \sqrt{3})^{-1}$. Now recall that, by Lemma 4.3 together with Proposition 4.6, $\mathbb{Q}[\sqrt{2} + \sqrt{3}]$ is a field. Thus, $(\sqrt{2} + \sqrt{3})^{-1} \in \mathbb{Q}[\sqrt{2} + \sqrt{3}]$. Thus, $\sqrt{2}-\sqrt{3} \in \mathbb{Q}[\sqrt{2}+\sqrt{3}]$. Thus, $\sqrt{2} = \sqrt{3}+(\sqrt{2}-\sqrt{3}) \in \mathbb{Q}[\sqrt{2}+\sqrt{3}]$, and then also $\sqrt{3} = (\sqrt{2}+\sqrt{3})-\sqrt{2}) \in \mathbb{Q}[\sqrt{2}+\sqrt{3}]$. It follows that $\mathbb{Q}[\sqrt{2}+\sqrt{3}] = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.)
   ii. Compute the possible images of $\sqrt{2}$ and $\sqrt{3}$ under an automorphism of $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$. (Let α be an automorphism of $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$, and set $c^2 := \alpha(\sqrt{2})$. Then $c^2 = \alpha(\sqrt{2})^2 = \alpha(\sqrt{2}^2)^2 = \alpha(2) = 2$. It follows that $c := \pm\sqrt{2}$.)
5. Determine $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\sqrt[3]{2}])$.
6. Determine $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta, \sqrt[3]{2}])$, where $\zeta := -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$.

i. Note that $\min_{\mathbb{Q}}(\zeta) = x^2+x+1$. Furthermore, the roots of x^2+x+1 are ζ and ζ^2. Thus, each automorphism of $\mathbb{Q}[\zeta, \sqrt[3]{2}]$ must map ζ to ζ or to ζ^2; cf. Corollary 5.3(i). Similarly, $\min_{\mathbb{Q}}(\sqrt[3]{2}) = x^3 - 2$, and the roots of $x^3 - 2$ are $\sqrt[3]{2}$, $\zeta\sqrt[3]{2}$, and $\zeta^2\sqrt[3]{2}$. Let α denote the automorphism of $\mathbb{Q}[\zeta, \sqrt[3]{2}]$ with

$$\alpha : \zeta \mapsto \zeta^2, \ \sqrt[3]{2} \mapsto \sqrt[3]{2},$$

and let β denote the automorphism of $\mathbb{Q}[\zeta, \sqrt[3]{2}]$ with

$$\beta : \zeta \mapsto \zeta, \ \sqrt[3]{2} \mapsto \zeta\sqrt[3]{2}.$$

ii. Compute α^2, β^2, and β^3. Show that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta, \sqrt[3]{2}]) = \{\mathrm{id}_{\mathbb{Q}[\zeta, \sqrt[3]{2}]}, \beta, \beta^2, \alpha, \alpha\beta, \alpha\beta^2\}$. (We read the composition from left to right. For instance $\alpha\beta$ is the map which applies α first and then β.)

iii. Set $G := \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta, \sqrt[3]{2}])$. Compute all subgroups of G. (If you write h for α and k for $\alpha\beta$, you will recognize the group G and remember what the subgroups of G are.)

iv. Determine $\mathrm{Fix}_{\mathbb{Q}[\zeta, \sqrt[3]{2}]}(H)$ for each of the six subgroups H of G.

7. Let T be an integral domain, let S be a subfield of T. Assume that T is finitely generated over S. Show that $\mathrm{Aut}_S(T)$ is a finite group. [HINT: Find a non-empty finite set B with $T = BS$. Consider the product of the minimal polynomials of the elements of B. Then use Corollary 5.3.]

8. Let T be an integral domain, let S be a subfield of T, let q be a polynomial over S, let t be a root of q in T, and set $G := \mathrm{Aut}_S(T)$. Show that $|t^G| \leq \deg(q)$.

6. Finite Galois Correspondence

In Theorem 1.3(iii), we have seen that Galois pairs give rise to bijective order reversing maps. In Theorem 3.6, we have seen a Galois pair defined by the ordered set of all subrings of a given ring R and the ordered set of all subgroups of $\mathrm{Aut}(R)$. In this section, we look at this Galois pair, but we assume that the ring R is a commutative field.

Let U be a commutative field.

Let S and T be subfields of R with $S \subseteq T$. From Lemma 3.3(iii) we know that then $\mathrm{Aut}_T(R) \subseteq \mathrm{Aut}_S(R)$. In Theorem 6.3(i), we will see that, if U is galois over S and $\dim_S(T)$ is finite, then the index of $\mathrm{Aut}_T(R)$ in $\mathrm{Aut}_S(R)$ is finite and equal to $\dim_S(T)$.

Let H and K be subgroups of $\mathrm{Aut}(R)$ with $H \subseteq K$. From Lemma 3.2(iv) we know that then $\mathrm{Fix}_R(K) \subseteq \mathrm{Fix}_R(H)$. In Theorem 6.3(ii), we will see that, if H is galois and $|K/H|$ is finite, then $\mathrm{Fix}_R(H)$ has finite dimension over $\mathrm{Fix}_R(K)$ and this dimension is equal to $|K/H|$.[19]

Lemma 6.1

Let U be a commutative field, let S and T be subfields of U with $S \subseteq T$, and assume that T is finitely generated over S. Set $K := \mathrm{Aut}_S(U)$ and $H := \mathrm{Aut}_T(U)$. Then $|K/H| \leq \dim_S(T)$.

Proof. If $S = T$, $K = H$, and there is nothing to show. Thus, we assume that $S \neq T$, and we choose an element t in $T \setminus S$.

Assume first that $S[t] \neq T$. In this case, we set $J := \mathrm{Aut}_{S[t]}(U)$. Then, by induction,

$$|K/H| = |K/J| \cdot |J/H| \leq \dim_S(S[t]) \cdot \dim_{S[t]}(T) = \dim_S(T),$$

cf. Lemma 4.2.

Assume now that $S[t] = T$. Since T is assumed to be finitely generated over S, T is integral over S; cf. Lemma 4.5. It follows that $t \in I_T(S)$. Now, by Lemma 5.1(iii), $\deg(\min_S(t)) = \dim_S(T)$.

Let B denote the set of the roots of $\min_S(t)$ in U. Then $t \in B$ and, by Corollary 5.4, K acts on B. From $S[t] = T$ we also obtain that $K_t = H$. Thus,

$$|K/H| = |t^K| \leq |B| \leq \deg(\min_S(t)) = \dim_S(T).$$

(The first equation refers to the orbit formula.) □

Lemma 6.2 [E. Artin]

Let U be a commutative field, let K and H be subgroups of $\mathrm{Aut}(U)$ with $H \subseteq K$, and assume that $|K/H|$ is finite. Set $S := \mathrm{Fix}_U(K)$ and $T := \mathrm{Fix}_U(H)$. Then $\dim_S(T) \leq |K/H|$.

Proof. Set $n := |K/H|$, and let $\{k_1, \ldots, k_n\}$ be a right transversal of H in K.

Assume, by way of contradiction, that $n + 1 \leq \dim_S(T)$, and let $\{t_1, \ldots, t_{n+1}\}$ be a subset of T which is linearly independent over S.

[19] From Lemma 3.2(ii) we know that $\mathrm{Fix}_R(K)$ is a subfield of $\mathrm{Fix}_R(H)$.

Set

$$M := \begin{pmatrix} t_1^{k_1} & t_1^{k_2} & \dots & t_1^{k_n} \\ t_2^{k_1} & t_2^{k_2} & \dots & t_2^{k_n} \\ \vdots & \vdots & & \vdots \\ t_{n+1}^{k_1} & t_{n+1}^{k_2} & \dots & t_{n+1}^{k_n} \end{pmatrix},$$

and let ϕ denote the linear map from T^{n+1} to T^n which sends $(x_1, x_2, \dots, x_{n+1})$ to $(x_1, x_2, \dots, x_{n+1})M$. Then $\ker(\phi) \neq \{0\}$. Among the non-zero elements in $\ker(\phi)$ we choose $(a_1, a_2, \dots, a_{n+1})$ which has as many zeros as possible.

We may assume that $a_1 = 1$. Then

$$(1, a_2, \dots, a_{n+1}) \in \ker(\phi).$$

We assume that $k_1 = 1$. Then

$$t_1 a_1 + \dots + t_{n+1} a_{n+1} = 0.$$

If $\{a_1, a_2, \dots, a_{n+1}\} \subseteq S$, then $\{t_1, \dots, t_{n+1}\}$ is not linearly independent over S, since $a_1 = 1$. Thus, we may assume that $a_2 \notin S$. Thus, K contains an element k with $a_2^k \neq a_2$.

Set

$$N := \begin{pmatrix} t_1^{k_1 k} & t_1^{k_2 k} & \dots & t_1^{k_n k} \\ t_2^{k_1 k} & t_2^{k_2 k} & \dots & t_2^{k_n k} \\ \vdots & \vdots & & \vdots \\ t_{n+1}^{k_1 k} & t_{n+1}^{k_2 k} & \dots & t_{n+1}^{k_n k} \end{pmatrix},$$

and let ψ denote the linear map from T^{n+1} to T^n which sends $(x_1, x_2, \dots, x_{n+1})$ to $(x_1, x_2, \dots, x_{n+1})N$. Then

$$(1, a_2^k, \dots, a_{n+1}^k) \in \ker(\psi).$$

Since $\{k_1, \dots, k_n\}$ is a right transversal of H in K, we also have $\ker(\phi) = \ker(\psi)$. Thus, as $a_2 - a_2^k \neq 0$,

$$(0, a_2 - a_2^k, a_3 - a_3^k, \dots, a_{n+1} - a_{n+1}^k)$$

is a non-zero element in $\ker(\phi)$ which has more zeros than $(a_1, a_2, \dots, a_{n+1})$, contrary to the choice of $(a_1, a_2, \dots, a_{n+1})$. □

Theorem 6.3

Let U be a commutative field. Then the following hold.

(i) *Let S and T be subfields of U with $S \subseteq T$, and assume that T is finitely generated over S. Assume that U is galois over S. Then U is galois over T and, setting $K := \mathrm{Aut}_S(U)$ and $H := \mathrm{Aut}_T(U)$, we have $|K/H| = \dim_S(T)$.*

(ii) *Let K and H be subgroups of $\mathrm{Aut}(U)$ with $H \subseteq K$, and assume that $|K/H|$ is finite. Assume that H is galois. Then K is galois and, setting $S := \mathrm{Fix}_U(K)$ and $T := \mathrm{Fix}_U(H)$, we have $\dim_S(T) = |K/H|$.*

Proof. (i) From Lemma 6.1 and Lemma 6.2 we obtain that

$$\dim_{\mathrm{Fix}_U(K)}(\mathrm{Fix}_U(H)) \leq |K/H| \leq \dim_S(T).$$

We are assuming that U is galois over S, and that means that $S = \mathrm{Fix}_U(K)$. From Lemma 3.3(ii) we also know that $T \subseteq \mathrm{Fix}_U(H)$. Thus,

$$\dim_S(T) \leq \dim_{\mathrm{Fix}_U(K)}(\mathrm{Fix}_U(H)).$$

It follows that $T = \mathrm{Fix}_U(H)$ and that $|K/H| = \dim_S(T)$. The former equation means that U is galois over T.

(ii) From Lemma 6.1 and Lemma 6.2 we obtain that

$$|\mathrm{Aut}_S(U)/\mathrm{Aut}_T(U)| \leq \dim_S(T) \leq |K/H|.$$

We are assuming that H is galois, and that means that $H = \mathrm{Aut}_T(U)$. Now recall from Lemma 3.5 that $K \subseteq \mathrm{Aut}_S(U)$. Then

$$|K/H| \leq |\mathrm{Aut}_S(U)/\mathrm{Aut}_T(U)|.$$

It follows that $K = \mathrm{Aut}_S(U)$ and that $\dim_S(T) = |K/H|$. The former equation means that K is galois. □

The following result is a special case of Theorem 6.3.

Theorem 6.4 [R. Dedekind]

Let T be a commutative field. Then the following hold.

(i) *Let S be a subfield of T, and assume that T is finitely generated and galois over S. Then $|\mathrm{Aut}_S(T)| = \dim_S(T)$.*

(ii) *Let G be a finite subgroup of $\mathrm{Aut}(T)$, and set $S := \mathrm{Fix}_T(G)$. Then $G = \mathrm{Aut}_S(T)$ and $\dim_S(T) = |G|$.*

Proof. (i) This is the case $T = U$ in Theorem 6.3(i).

(ii) This is the case $H = \{1\}$ in Theorem 6.3(ii). □

Let R be a commutative field. Theorem 6.4(ii) implies that each finite subgroup of $\mathrm{Aut}(R)$ is galois.

Our next result is an arithmetic characterization of commutative fields which are finitely generated and galois over one of their subfields. In Theorem 10.1, we will see an algebraic characterization of commutative fields which are algebraic and galois over subfields.

Theorem 6.5

Let U be a commutative field, let S be a subfield of U, and assume that U is finitely generated over S. Then U is galois over S if and only if $|\mathrm{Aut}_S(U)| = \dim_S(U)$.

Proof. If U is galois over S, the equation $|\mathrm{Aut}_S(U)| = \dim_S(U)$ is obtained from Theorem 6.4(i).

To show that U is galois over S if $|\mathrm{Aut}_S(U)| = \dim_S(U)$ we set $G := \mathrm{Aut}_S(U)$ and $T := \mathrm{Fix}_U(G)$. We have to show that $S = T$.

Since U is assumed to be finitely generated over S, G is finite; cf. Lemma 6.1. Then, by Theorem 6.4(ii), $G = \mathrm{Aut}_T(U)$ and $\dim_T(U) = |G|$. As a consequence $\dim_T(U) = |\mathrm{Aut}_T(U)|$.

Now recall from Theorem 1.3(ii) that $\mathrm{Aut}_S(U) = \mathrm{Aut}_T(U)$ and that we are assuming that $|\mathrm{Aut}_S(U)| = \dim_S(U)$. Thus, $\dim_S(U) = \dim_T(U)$, so $S = T$. □

Let R be a commutative field.

Recall from Section 3 that $\mathcal{S}(R)$ is our notation of the set of all subrings of R and $\mathcal{G}(R)$ stands for the set of all subgroups of $\mathrm{Aut}(R)$. Recall that the sets $\mathcal{S}(R)$ and $\mathcal{G}(R)$ both are ordered with respect to set theoretic containment, and that we defined $S^{\gamma_R} := \mathrm{Aut}_S(R)$ for each element S in $\mathcal{S}(R)$ and $G^{\phi_R} := \mathrm{Fix}_R(G)$ for each element G in $\mathcal{G}(R)$.

In Theorem 3.6(i), we saw that the pair (γ_R, ϕ_R) is a Galois pair with respect to the orders defined on $\mathcal{S}(R)$ and $\mathcal{G}(R)$, respectively, by set theoretic containment.

Theorem 6.6 [Finite Galois Correspondence]

Let R be a commutative field, let $\mathcal{S}'(R)$ denote the set of all subfields S of R such that R is finitely generated and galois over S, and let $\mathcal{G}'(R)$ denote the set of all finite subgroups of $\mathrm{Aut}(R)$. *Define $S^\gamma := \mathrm{Aut}_S(R)$ for each element S in $\mathcal{S}'(R)$ and $G^\phi := \mathrm{Fix}_R(G)$ for each element G in $\mathcal{G}'(R)$. Then the following hold.*

(i) *The map γ is a bijective order-reversing map from $\mathcal{S}'(R)$ to $\mathcal{G}'(R)$.*

(ii) *The map ϕ is a bijective order-reversing map from $\mathcal{G}'(R)$ to $\mathcal{S}'(R)$.*

(iii) *The maps γ and ϕ are inverses of each other.*

(iv) *Let T and U be elements in $\mathcal{S}'(R)$ with $T \subseteq U$, let K and H be elements in $\mathcal{G}'$ with $T^\gamma = K$ and $U^\gamma = H$ (or, what is the same, with $K^\phi = T$ and $H^\phi = U$). Then $|K/H| = \dim_T(U)$.*

Proof. (i) We define $\mathcal{S}^\circ(R)$ to be the set of all subfields S of R such that R is finitely generated over S. By $\mathcal{G}^\circ(R)$ we denote the set of all finite subgroups of $\mathrm{Aut}(R)$. Note that $\mathcal{S}^\circ(R) \subseteq \mathcal{S}(R)$ and $\mathcal{G}^\circ(R) \subseteq \mathcal{G}(R)$.

From Lemma 6.1 we obtain that γ_R sends elements of $\mathcal{S}^\circ(R)$ to $\mathcal{G}^\circ(R)$, from Lemma 6.2 that ϕ_R sends elements of $\mathcal{G}^\circ(R)$ to $\mathcal{S}^\circ(R)$.

Define γ° to be the map from $\mathcal{S}^\circ(R)$ to $\mathcal{G}^\circ(R)$ which coincides with γ_R on $\mathcal{S}^\circ(R)$. Define ϕ° to be the map from $\mathcal{G}^\circ(R)$ to $\mathcal{S}^\circ(R)$ which coincides with ϕ_R on $\mathcal{G}^\circ(R)$. Then $(\gamma^\circ, \phi^\circ)$ is a Galois pair with respect to the orders defined on $\mathcal{S}(R)^\circ$ and $\mathcal{G}(R)^\circ$, respectively, by set theoretic containment.

From Theorem 6.4(ii) we obtain that $\mathcal{S}'(R) = \mathrm{im}(\phi^\circ)$. From Theorem 6.4(i) we obtain that $\mathcal{G}'(R) = \mathrm{im}(\gamma^\circ)$. Thus, γ is the map from $\mathrm{im}(\phi)$ to $\mathrm{im}(\gamma)$ which maps each element S of $\mathrm{im}(\phi)$ to S^γ, and ϕ is the map from $\mathrm{im}(\gamma)$ to $\mathrm{im}(\phi)$ which maps each element G of $\mathrm{im}(\gamma)$ to G^ϕ. Thus, by Theorem 1.3(iii), γ and ϕ are bijective and inverses of each other.

(ii) This follows from Theorem 6.3(i) or Theorem 6.3(ii). □

Corollary 6.7

Let R be a commutative field, let S be a subfield of R, and assume that R is finitely generated

and galois over S. Let $\mathcal{S}_S(R)$ denote the set of all subfield of R containing S, let $\mathcal{G}_S(R)$ denote the set of all subgroups of $\mathrm{Aut}_S(R)$. Then the following hold.

(i) *The maps*

$$\gamma\colon\ \mathcal{S}_S(R) \to \mathcal{G}_S(R), \quad T \mapsto \mathrm{Aut}_T(R)$$

and

$$\phi\colon\ \mathcal{G}_S(R) \to \mathcal{S}_S(R), \quad G \mapsto \mathrm{Fix}_R(G)$$

are bijective, order-reversing, and inverses of each other.

(ii) *Let T and U be elements in $\mathcal{S}_S(R)$ with $T \subseteq U$, let K and H be elements in $\mathcal{G}_S$ with $T^\gamma = K$ and $U^\gamma = H$ (or, what is the same, with $K^\phi = T$ and $H^\phi = U$). Then $|K/H| = \dim_T(U)$.*

Proof. This follows from Theorem 6.6. □

The essential part of Corollary 6.7 is that, given a commutative field R and a subfield S of R such that R is finitely generated and galois over S, then the ordered set of all subfields of R containing S can be studied via the ordered set of all subgroups of the finite group $\mathrm{Aut}_S(R)$.

At this point, we have reached our first goal, the study of commutative fields T together with subfields S such that T is finitely generated and galois over S. From Lemma 4.5 we know that a commutative field which is finitely generated over one of its subfields is algebraic over that subfield. We now will look at commutative fields T together with subfields S such that T is algebraic and galois over S. The main goal will be Theorem 10.1, a theorem which provides two ring theoretic characterizations of those subfields of a commutative field R over which R is algebraic and galois.

Exercises

1. Let R and R' be integral domains, let S be a subfield of R, let r be an element in $I_R(S)$, and let ϕ be a ring homomomorphism from $S[r]$ to R'. Show that $\phi|_S$ is injective, that $r^\phi \in I_{R'}(S^\phi)$ and that $\min_{S^\phi}(r^\phi)$ divides $\min_S(r)^{\hat{\phi}}$.

2. Let R be a commutative field, let S be a subfield of R, and assume that R is finitely generated over S. Set $T := \mathrm{Fix}_R(\mathrm{Aut}_S(R))$. Show that $\dim_T(R) = |\mathrm{Aut}_S(R)|$. [Hint: Use Lemma 3.3(ii), and then Theorem 3.7(i) and Theorem 6.5.]

   Solution: From Lemma 3.3(ii) we know that $S \subseteq T$. Thus, as R is assumed to be finitely generated over S, R is finitely generated over T. From Theorem 3.7(i) we know that R is galois over T. Thus, by Theorem 6.5, $\dim_T(R) = |\mathrm{Aut}_T(R)|$. Now the claim follows since we have $\mathrm{Aut}_S(R) = \mathrm{Aut}_T(R)$.

   Here is another solution: Since R is assumed to be finitely generated over S, G is finite; cf. Lemma 6.1. Then, by Theorem 6.4(ii), $G = \mathrm{Aut}_T(R)$ and $\dim_T(R) = |G|$. As a consequence $\dim_T(R) = |\mathrm{Aut}_T(R)|$. Now recall from Theorem 1.6.4(ii) that $\mathrm{Aut}_S(R) = \mathrm{Aut}_T(R)$.