Chapter 2. Algebraic Number Fields

2.1 Definition: When F and K are fields with $F \subseteq K$, the field K is a vector space over the field F, and we write $[K : F] = \dim_F K$.

2.2 Theorem: *Let F, K and L be fields with $F \subseteq K \subseteq L$. Then $[L : F] = [K : F][L : K]$. Indeed if U is a basis for K over F and V is a basis for L over K then*

$$W = \big\{uv \,\big|\, u \in U, v \in V\big\}$$

is a basis for K over F.

Proof: The proof is left as an exercise.

2.3 Definition: When R and S are commutative rings with $R \subseteq S$ and U is a subset of S, the **subring of S generated by U over R**, denoted by $R[U]$, is the smallest subring of S which contains $R \cup U$. When $U = \{u_1, u_2, \cdots, u_n\}$ we write $R[U]$ as $R[u_1, u_2, \cdots, u_n]$, and we have

$$R[u_1, u_2, \cdots, u_n] = \big\{f(u_1, u_2, \cdots, u_n) \,\big|\, f \in R[x_1, x_2, \cdots, x_n)\big\}.$$

When $S = F[u_1, u_2, \cdots, u_n]$ for some $u_1, u_2, \cdots, u_n \in S$, we say that S is **finitely generated** as a ring over R. When F and K are fields with $F \subseteq K$ and $U \subseteq K$, the **subfield of K generated by U over F**, denoted by $F(U)$, is the smallest subfield of K which contains $F \cup U$. When $U = \{u_1, u_2, \cdots, u_n\}$ we write $F(U)$ as $F(u_1, u_2, \cdots, u_n)$, and we have

$$F(u_1, \cdots, u_n) = \left\{ \frac{f(u_1, \cdots, u_n)}{g(u_1, \cdots, u_n)} \,\middle|\, f, g \in F[x_1, \cdots, x_n] \text{ and } g(u_1, \cdots, u_n) \neq 0 \right\}.$$

When $K = F(u_1, \cdots, u_n)$ for some $u_1, \cdots, u_n \in K$, we say that K is **finitely generated** as a field over F.

2.4 Definition: Let F and K be fields with $F \subseteq K$. For $a \in K$, we say that a is **algebraic** over F when there exists a polynomial $f(x) \in F[x]$ such that $f(a) = 0$ in K, otherwise we say that a is **transcendental** over F. We say that K is **algebraic** over F when every element $a \in K$ is algebraic over F, otherwise we say that K is **transcendental** over F.

2.5 Theorem: *Let F and K be fields with $F \subseteq K$ and let $a \in K$.*

(1) If a is transcendental over F then we have

$$F[a] \cong F[x] \quad \text{and} \quad F(a) \cong F(x).$$

In this case $[F(a) : F] = \infty$ and the set $\{1, a, a^2, \cdots\}$ is linearly independent over F.

(2) If a is algebraic over F then there is a unique monic irreducible polynomial $f(x) \in F[x]$ with $f(a) = 0$, the ideal generated by this polynomial in $F[x]$ is $\langle f \rangle = \big\{g \in F[x] \,\big|\, g(a) = 0\big\}$ and we have

$$F(a) = F[a] \cong F[x]/\langle f \rangle$$

and for $n = \deg(f)$ the set $\{1, a, a^2, \cdots, a^{n-1}\}$ is a basis for $F(a)$ over F and we have $[F(a) : F] = n$.

Proof: The proof is left as an exercise.

2.6 Definition: When F and K are fields with $F \subseteq K$ and $a \in K$ is algebraic over F, the unique monic irreducible polynomial $f(x) \in K[x]$ with $f(a) = 0$ in K is called the **minimal polynomial** of a over F.

2.7 Corollary: *Let F, K and L be fields with $F \subseteq K \subseteq L$ and let $a \in L$. If $f(x) \in F[x]$ is the minimal polynomial for a over F and $g(x) \in K[x]$ is the minimal polynomial for a over K, then we have $g(x) \big| f(x)$ in $K[x]$.*

Proof: The proof is left as an exercise.

2.8 Corollary: *Let F and K be fields with $F \subseteq K$, Then $[K : F]$ is finite if and only if K is algebraic and finitely generated as a field over F.*

Proof: The proof is left as an exercise.

2.9 Corollary: *Let F, K and L be fields with $F \subseteq K \subseteq L$. If L is algebraic over K and K is algebraic over F then L is algebraic over F.*

Proof: The proof is left as an exercise.

2.10 Definition: Let R be a commutative ring. A **module** over R (or an R-module) is a set A with an element $0 \in A$, an operations $+ : A \times A \to A$ where for $a, b \in A$ we write $+(a, b)$ as $a + b$, and an operation $\times : R \times A \to A$ where for $r \in R$ and $a \in A$ we write $\times(r, a)$ as $r \cdot a$ or as ra, such that

(1) $+$ is associative: for all $a, b, c \in A$ we have $(a + b) + c = a + (b + c)$,
(2) $+$ is commutative: for all $a, b \in A$ we have $a + b = b + a$,
(3) 0 is an additive identity: for all $a \in A$ we have $a + 0 = a$,
(4) every $a \in A$ has a negative: for every $a \in A$ there exists $b \in A$ such that $a + b = 0$,
(5) $\times$ in R is associative with $\times$ in A: for all $r, s \in R$ and all $a \in A$ we have $(rs)a = r(sa)$,
(6) $1 \in R$ is a multiplicative identity: for all $a \in R$ we have $1 \cdot a = a$,
(7) $\times$ is distributive over $+$ in A: for all $r \in R$ and all $a, b \in A$ we have $r(a+b) = ra+rb$,
(8) $\times$ is distributive over $+$ in R: for all $r, s \in R$ and all $a \in A$ we have $(r+s)a = ra+sa$.

A **submodule** of an R-module A is a subset $B \subseteq A$ which is also an R-module using the (restrictions of the) same operations that are used in A. In order for a subset B of A to be a submodule, it is necessary and sufficient that $0 \in B$ and that for all $a, b \in B$ and $r \in R$ we have $ra + bnB$ and $ra \in B$.

2.11 Example: When F is a field, a module over F is the same thing as a vector space over F. A module over $\mathbf{Z}$ is the same thing as an abelian group. For a commutative ring R, the sets $\{0\}$ and R are both R-modules, and more generally the set R^n is an R-module for $n \in \mathbf{N}$. An ideal of R is the same thing as a submodule of the R-module R. When R is a subring of S, every S-module is also an R-module, and in particular S is an R-module.

2.12 Definition: Let R be a commutative ring, let A be an R-module, and let U be a subset of A. The **submodule of A generated by** U is the smallest submodule of A which contains the set U, namely the set

$$\mathrm{Span}_R(U) = \left\{ \sum_{k=0}^{n} r_i u_i \,\middle|\, n \in \mathbf{N}\,, \text{ each } r_i \in R\,, \text{ each } u_i \in X \right\}$$

where in the case that $n = 0$ we take the sum to be equal to $0 \in A$. We say that U **generates A over R** (or that U **spans A over R**) when $A = \mathrm{Span}_R(U)$. We say that A is **finitely generated** (as an R-module) when $A = \mathrm{Span}_R(U)$ for some finite set U.

2.13 Theorem: *Let R be a subring of S and let A be an S-module. Suppose that $S = \text{Span}_R(U)$ and $A = \text{Span}_S(V)$. Then $S = \text{Span}_R\{uv | u \in U, v \in V\}$.*

Proof: Given $u \in U$ and $v \in V$, we have $uv \in A$ because $u \in S$, $v \in A$ and A is an S-module. It follows that $\text{Span}_R\{uv | u \in U, v \in V\} \subseteq A$.

Given $a \in A$, since $A = \text{Span}_S(V)$ we can write $a = \sum_{j=1}^{m} s_j v_j$ with each $s_j \in S$ and each $v_j \in V$, and then since $S = \text{Span}_R(U)$, for each index j we can write $s_j = \sum_{i=1}^{n} r_{i,j} u_i$ (where we can use the same value of n for each index j by allowing some of the elements $r_{i,j}$ to be zero), and then we have $a = \sum_{i=1}^{n} \sum_{j=1}^{m} r_{i,j} u_i v_j$. It follows that $A \subseteq \text{Span}_R\{uv | u \in U, v \in V\}$.

2.14 Definition: Let R be a commutative ring, let A be an R-module. For a subset $U \subseteq A$, we say that U is **linearly independent** (over R) when it has the property that for all $n \in \mathbf{Z}^+$, for all $r_1, r_2, \cdots, r_n \in R$, and for all distinct $u_1, u_2, \cdots, u_n \in U$, if $\sum_{i=1}^{n} r_i u_i = 0$ then $r_1 = r_2 = \cdots = r_n = 0$, otherwise we say that U is **linearly dependent** (over R). For $U \subseteq A$, we say that U is a **basis** for A (over R) when U is linearly independent over R and $\text{Span}_R(U) = A$. We say that A is a **free** R-module when there exists a subset $U \subseteq A$ which is a basis for A over R.

2.15 Example: When R is a commutative ring and $n \in \mathbf{N}$, the set R^n is a free R-module with the usual standard basis $\{e_1, e_2, \cdots, e_n\}$.

2.16 Example: For $n \in \mathbf{Z}^+$, the ring $\mathbf{Z}_n$ is a $\mathbf{Z}$-module, but it is not free (since the empty set does not span $\mathbf{Z}_n$ and every nonempty subset of $\mathbf{Z}_n$ is linearly dependent).

2.17 Definition: Let R and S be commutative rings with $R \subseteq S$. For $a \in S$, we say the a is **integral** over R when there exists a monic polynomial $f(x) \in R[x]$ such that $f(a) = 0$. We say that S is **integral** over R when every element $a \in S$ is integral over R.

2.18 Theorem: *Let R and S be commutative rings with $R \subseteq S$ and let $a \in S$. Then the following are equivalent.*

(1) a is integral over R,
(2) the ring $R[a]$ is finitely generated as an R-module, and
(3) $a \in T$ for some ring T which is finitely generated as an R-module with $R \subseteq T \subseteq S$.

Proof: I may include a proof later.

2.19 Corollary: *Let R, S and T be commutative rings with $R \subseteq S \subseteq T$. If T is integral over S and S is integral over R then T is integral over R.*

Proof: Suppose that T is integral over S and that S is integral over R. Let $a \in T$. Since a is integral over S, we can choose a monic polynomial $f(x) = \sum_{i=0}^{n} c_i x^i$ with each $c_i \in S$ and $c_n = 1$ such that $f(a) = 0$ in T. We have a tower of extension rings

$$R \subseteq R[c_0] \subseteq R[c_0, c_1] \subseteq \cdots \subseteq R[c_0, c_1, \cdots, c_{n-1}] \subseteq R[c_0, c_1, \cdots, c_{n-1}, a].$$

Each ring is finitely generated as a module over the previous ring by the above theorem, and so $R[c_0, c_1, \cdots, c_{n-1}, a]$ is finitely generated over R by Theorem 2.4. Thus a is integral over R by the above theorem.

2.20 Corollary: *Let R and S be commutative rings with $R \subseteq S$. Then the set*

$$\overline{R} = \big\{ a \in S \big| a \text{ is integral over } R \big\}$$

is a ring.

Proof: Let $a, b \in \overline{R}$. In the tower of rings $R \subseteq R[a] \subseteq R[a,b]$, each ring is finitely generated as a module over the previous ring, and so $R[a,b]$ is finitely generated over R. It follows that every element in $R[a,b]$ is integral over R, and in particular, the elements $a \pm b$ and ab are integral over R. Thus $a \pm b \in \overline{R}$ and $ab \in \overline{R}$ and so $\overline{R}$ is a subring of S.

2.21 Definition: When R and S are commutative rings with $R \subseteq S$, the ring

$$\overline{R} = \big\{ a \in S \big| a \text{ is integral over } R \big\}$$

is called **integral closure** of R in S. We say that R is **integrally closed** in S when $R = \overline{R}$ (that is when every element in S which is integral over R already lies in R). Note that $\overline{\overline{R}} = R$ and so the ring $\overline{R}$ is integrally closed in S. When R is an integral domain, we say that R is **integrally closed** when R is integrally closed in its quotient field.

2.22 Definition: For $a \in \mathbf{C}$, we say that a is **algebraic** when it is algebraic over $\mathbf{Q}$, and we say that a is **integral** when it is integral over $\mathbf{Z}$. An **algebraic number field** is a field K with $\mathbf{Q} \subseteq K \subseteq \mathbf{C}$ such that $[K : \mathbf{Q}]$ is finite. In other words, an algebraic number field is a subfield of $\mathbf{C}$ which is algebraic and finitely generated as a field over $\mathbf{Q}$. The **ring of integral elements** in an algebraic number field K, denoted by $\mathcal{O}_K$, is the integral closure of $\mathbf{Z}$ in K, that is

$$\mathcal{O}_K = \big\{ a \in K \,\big|\, a \text{ is integral over } \mathbf{Z} \big\}.$$

2.23 Theorem: *Let $a \in \mathbf{C}$. Then a is integral if and only if a is algebraic and its minimal polynomial lies in $\mathbf{Z}[x]$.*

Proof: If a is algebraic and its minimal polynomial lies in $\mathbf{Z}[x]$, then of course a is integral. Suppose that a is integral. Choose a monic polynomial $f(x) \in \mathbf{Z}[x]$ such that $f(a) = 0$. Write $f(x) = g_1(x)g_2(x)\cdots g_n(x)$ where each $g_i(x)$ is a monic irreducible polynomial in $\mathbf{Z}[x]$. Since $0 = f(a) = g_1(a)g_2(a)\cdots g_n(a)$, we must have $g_k(a) = 0$ for some index k. Since $g_k(x)$ is monic and irreducible in $\mathbf{Z}[x]$, it is also irreducible in $\mathbf{Q}[x]$ by Gauss' Lemma. Thus $g_k(x)$ is equal to the minimal polynomial of a over $\mathbf{Q}$, so the minimal polynomial of a over $\mathbf{Q}$ does indeed lie in $\mathbf{Z}[x]$.

2.24 Theorem: *Let $d \in \mathbf{Z}^+$ be square-free. Let $K = \mathbf{Q}(\sqrt{d})$. Then $\mathcal{O}_K = \mathbf{Z}[\omega]$ where*

$$\omega = \begin{cases} \sqrt{d} & \text{if } d \neq 1 \bmod 4, \\ \frac{1+\sqrt{d}}{2} & \text{if } d = 1 \bmod 4. \end{cases}$$

Proof: I may include a solution later.

2.25 Definition: A **quadratic number field** is an algebraic number field of the form $K = \mathbf{Q}(\sqrt{d})$ for some square-free $d \in \mathbf{Z}^+$. A **quadratic integer ring** is a ring of the form $\mathbf{Z}[\omega] = \mathcal{O}_K$ for some quadratic number field K.

2.26 Theorem: *Let K be an algebraic number field. For every $u \in K$ there exists $b \in \mathbf{Z}^+$ such that $bu \in \mathcal{O}_K$.*

Proof: Let $u \in K$. Since u is algebraic over $\mathbf{Q}$, we can choose a polynomial $f(x) \in \mathbf{Q}[x]$ such that $f(a) = 0$. By multiplying by a common denominator of the coefficients of $f(x)$, and then by multiplying by -1 if necessary, we obtain a polynomial $g(x) = \sum_{k=0}^{n} c_k x^k$ with each $c_k \in \mathbf{Z}$ and $c_n \in \mathbf{Z}^+$ such that $g(a) = 0$. Multiply both sides of the equality $0 = g(a) = \sum_{k=0}^{n} c_k a^k$ by ${c_n}^{n-1}$ to get $0 = \sum_{k=1}^{n} c_k {c_n}^{n-1} u^k = \sum_{k=0}^{n} c_k {c_n}^{n-k-1} (c_n u)^k$. It follows that $c_k u$ is a root of the polynomial $g(x) = \sum_{k=0}^{n} c_k {c_n}^{n-k-1} x^k$ which lies in $\mathbf{Z}[x]$ and is monic. Thus $c_n u$ is integral over $\mathbf{Q}$ and so $c_n u \in \mathcal{O}_K$.

2.27 Corollary: *An algebraic number field K is equal to the quotient field of its ring of integers $\mathcal{O}_K$. In particular, the ring $\mathcal{O}_K$ is integrally closed.*