Number Fields

January 16, 2020

1 Algebraic Numbers and Algebraic Integers; Number Fields

Here, we will use F to denote any field containing $\mathbb{Q}$, for instance $F = \mathbb{C}$. Recall that an element $\alpha \in F$ is ***algebraic*** (over $\mathbb{Q}$) if it is the root of some polynomial in $\mathbb{Q}[x]$. If so, there is a unique monic polynomial $m_\alpha \in \mathbb{Q}[x]$ of minimal degree with $m_\alpha(\alpha) = 0$, called the ***minimal polynomial*** of α. The ***degree*** of α is the degree of m_α

Proposition 1.1. *Suppose $\alpha \in F$ is algebraic. Then m_α is irreducible in $\mathbb{Q}[x]$, and if $f \in \mathbb{Q}[x]$, then $f(\alpha) = 0 \iff m_\alpha | f$.*

Proof. If $m_\alpha = fg$, then $f(\alpha)g(\alpha) = 0$, and since fields are integral domains we have $f(\alpha) = 0$ or $g(\alpha) = 0$. By minimality of degree, f or g is constant.

If $f(\alpha) = 0$, we write $f = gm_\alpha + h$, with $g, h \in \mathbb{Q}[x]$, and $\deg h < \deg m_\alpha$. Then $h(\alpha) = f(\alpha) - g(\alpha)m_\alpha(\alpha) = 0$, and so by minimality $h = 0$ and $m_\alpha | f$.

I.e. $\{f : f(\alpha) = 0\}$ is a principal ideal in $\mathbb{Q}[x]$ generated by m_α □

If $\alpha \in F$, define $\mathbb{Q}(\alpha)$ to be the smallest subfield of F containing α. Explicitly, it can be shown that $\mathbb{Q}(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in \mathbb{Q}[x], g(\alpha) \neq 0 \right\}$.

Proposition 1.2. *If $\alpha \in F$ is algebraic of degree n, then $1, \alpha, \ldots, \alpha^{n-1}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(\alpha)$. Conversely, if $[\mathbb{Q}(\alpha : \mathbb{Q}] \coloneqq \dim_{\mathbb{Q}} \mathbb{Q}(\alpha)$ is finite, say n, then α is algebraic of degree n.*

Proof. Consider the homomorphism $\phi : \mathbb{Q}[x] \to F; f \mapsto f(\alpha)$. Then $\ker(\phi) = (m_\alpha)$ which is maximal, so $\operatorname{im} \phi$ is a field, and hence equal to $\mathbb{Q}(\alpha)$. As $\deg m_\alpha = n$, a basis for $\mathbb{Q}[x]/(m_\alpha)$ is $1, x, \ldots, x^{n-1}$, and hence $1, \alpha, \ldots, \alpha^{n-1}$ is a basis for $\mathbb{Q}(\alpha)$.

For the converse part, if $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n < \infty$, then $1, \alpha, \ldots, \alpha^n$ are linearly dependent and so α is algebraic of some degree. By the first part, this degree is n. □

Proposition 1.3. *$\{\alpha \in F : \alpha$ algebraic$\}$ is a subfield of F.*

Galois theory. It is enough to prove that it is closed under $+, \times$ and inverse. For $+$ and $\times$ see **1.6** below for a stronger statement. If $0 \neq \alpha$ is algebraic, then $\sum^n b_j \alpha^j = 0 \implies \sum^n b_{n-j}(\alpha^{-1})^j = 0$, and so α^{-1} is algebraic. □

$\alpha \in F$ is an ***algebraic integer*** if there exists a monic polynomial $f \in \mathbb{Z}[x]$ with $f(\alpha) = 0$.

Lemma 1.5.

1. *Let $\alpha \in F$. Then the following are equivalent:*
   (a) *α is an algebraic integer*
   (b) *α is algebraic and $m_\alpha \in \mathbb{Z}[x]$*
   (c) *$\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module*

   If these hold, then $1, \alpha, \ldots, \alpha^{d-1}$ is a $\mathbb{Z}$-bases for $\mathbb{Z}[\alpha]$, with $d = \deg \alpha$.
2. *$\alpha \in \mathbb{Q}$ is an algebraic integer $\iff$ $\alpha \in \mathbb{Z}$*

Recall the notation that, if $\alpha_1, \ldots, \alpha_n \in F$, then $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ is the smallest subring of F containing $\{\alpha_i : i \in [n]\}$, i.e. the set of all finite sums of terms of the form $A\alpha_1^{i_1} \ldots \alpha_n^{i_n}$ for $A, i_1, \ldots, i_n \in \mathbb{Z}$.

Proof.

1. $\underline{a. \implies b.}$ Suppose $f(\alpha) = 0, f \in \mathbb{Z}[x]$, f monic. Then **1.1** gives that $f = gm_\alpha$ for some $g \in \mathbb{Q}[x]$ necessarily monic. Gauss's lemma from GRM gives us that m_α, g are in $\mathbb{Z}[x]$.

   $\underline{b. \implies c.}$ Write $m_\alpha = x^d + \sum_{j=1}^{d-1} b_j x^j$, for $b_j \in \mathbb{Z}$. Then $\alpha^d = -\sum_{j=1}^{d-1} b_j \alpha^j$, from which we say that every α^n is a $\mathbb{Z}$-linear combination of $1, \alpha, \ldots, \alpha^{d-1}$. So $\mathbb{Z}[\alpha]$ is generated by $1, \alpha, \ldots, \alpha^{d-1}$ as a $\mathbb{Z}$-module. There is no linear relation between $1, \alpha, \ldots, \alpha^{d-1}$, as $d = \deg \alpha$. So $\mathbb{Z}[\alpha]$ is finitely generated and $1, \alpha, \ldots, \alpha^{d-1}$ is a $\mathbb{Z}$-basis.

   $\underline{c. \implies a.}$ Assume $\mathbb{Z}[\alpha]$ is finitely generated by $g_1(\alpha), \ldots, g_r(\alpha)$. For some $g_i \in \mathbb{Z}[x]$. Let $k = \max\{\deg g_i\}$. Then $\mathbb{Z}[\alpha]$ is certainly generated by $1, \alpha, \ldots, \alpha^k$ as a $\mathbb{Z}$-module. So $\alpha^{k+1} = \sum_{j=0}^{k} b_j \alpha^j$ for $b_j \in \mathbb{Z}$, and so α is an algebraic integer.
2. $\alpha \in \mathbb{Q} \implies m_\alpha = x - \alpha$, and so α is an algebraic integer $\iff$ $\alpha \in \mathbb{Z}$ using $(a) \iff (b)$.

□

Theorem 1.6. *If $\alpha, \beta \in F$ are algebraic integers, then so are $\alpha\beta, \alpha \pm \beta$.*

Proof. The $\mathbb{Z}$-module $\mathbb{Z}[\alpha, \beta]$ is generated by $\{\alpha^i \beta^j : 0 \leq i < \deg \alpha; 0 \leq j < \deg \beta\}$, and so is finitely generated. Hence so is the submodule $\mathbb{Z}[\alpha\beta] \subseteq \mathbb{Z}[\alpha, \beta]$. So $\alpha\beta$ is an algebraic integer by **1.4**. The same applies for $\alpha + \beta, \alpha - \beta$. □

Now to introduce the main characters of this course:

An ***algebraic number field*** (or just ***number field***) is a field $K \supset \mathbb{Q}$ which is a finite extension, i.e. $[K : \mathbb{Q}] < \infty$. The ***ring of integers of K***, written $\mathfrak{o}_K$, is the set of algebraic integers in K. By **1.6** it is a ring. It is useful to have the converse:

Theorem 1.7 (Primitive Element)**.** *If K is a number field, then $K = \mathbb{Q}(\alpha)$ for some $\alpha \in K$.*

Proof. Done in Galois theory. □