International Journal of Engineering, Science and Mathematics
Vol. 5 Issue 4, December 2016
ISSN: 2320-0294 Impact Factor: 6.238
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

A STUDY ON NUMBER FIELDS WITH SPECIAL REFERENCE TO GALOIS THEORY OF NUMBER FIELDS

Seema
Research Scholar, Calorx Teachers' University
Ahmedabad (India)

Abstract: A *number field K* is a fit field extension of Q. Its *degree* is [K: Q]. i.e. its dimension as Q-vector a space. An algebraic number is an *algebraic integer* if it satisfies a ionic polynomial with integer coefficients, equivalently. Its minimal polynomial over Q should have integer coefficients.

Definition: Let *K* be a number field. Its *ring of integers Qk* consists of the elements of *K* which are algebraic integers.

Proposition 3.1: (i) Qk is a Noetherian ring.

(ii) $\operatorname{rank}_{\mathbb{Z}} \mathcal{O}_K = [K:\mathbb{Q}]$. i.e. $\mathcal{O}_K$ is a finitely generated abelian group under addition, and isomorphic to $\mathbb{Z}^{\oplus[K:\mathbb{Q}]}$

(iii) For every $\alpha \in K$ there exists $n \in N$ with $\alpha n \in \mathcal{O}_K$

(iv) $\mathcal{O}_K$ is the maximal subring of *K* which is finitely generated as an abelian group.

(v) $\mathcal{O}_K$ is integrally closed, i.e.. ii" $f(X) \in \mathcal{O}_K[X]$ is ionic and $f(\alpha) = 0$ for some $\alpha \in K$ then $\alpha \in \mathcal{O}_K$

Example:

Number field K	Ring of integers $\mathcal{O}_K$
$\mathbb{Q}$	$\mathbb{Z}$
$\mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z} - \{0,1\}$ squarefree	$\mathbb{Z}[\sqrt{d}]$ if $d \equiv 2,3 \pmod 4$,
	$\mathbb{Z}[(1+\sqrt{d})/2]$ if $d \equiv 1 \pmod 4$
$\mathbb{Q}(\zeta_n)$, ζ_n a primitive nth root of unity	$\mathbb{Z}[\zeta_n]$

Example: $K = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$ since $\zeta_3 = (-1+\sqrt{-3})/2$, $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$

UNITS

Definition. A *unit*, in a number field *K* is an element such that The group of units in *K* is denoted by $\mathcal{O}_K^\times$ $\alpha \in \mathcal{O}_K$ $\alpha^{-1} \in \mathcal{O}_K$

Example: For $K = \mathbb{Q}$ we have $\mathcal{O}_K = \mathbb{Z}$ and $\mathcal{O}_K^\times = \{\pm 1\}$.

For we $K = \mathbb{Q}(\sqrt{-3})$ have $\mathcal{O}_K = \mathbb{Z}[(1+\sqrt{-3})/2]$ and $\mathcal{O}_K^\times = \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$

Theorem 3.1 (Dirichlet's I nit Theorem). Lt^t *K* be a number field. Then $\mathcal{O}_K^\times$ is a finitely generated abelian group. More precisely $\mathcal{O}_K^\times = \Delta \times \mathbb{Z}^{r_1+r_2-1}$

where is the finite group of roots of unity in K. and r\ and or denote the number of real embedding $K \hookrightarrow \mathbb{R}$ and complex conjugate embedding with image not contained in R. so $r_1 + 2r_2 = [K : \mathbb{Q}]$

Corollary 3.1: The only number fields with finitely many units' art;

Q and $\mathbb{Q}(\sqrt{-D})$

$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

$D > 0$

FACTORISATION

Example. Z lias unique factorisation. We do not have this luxury in $\mathcal{O}_K$ in general, e.g.. let $K = \mathbb{Q}(\sqrt{-5})$ with $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ then where $2, 3, 1 \pm \sqrt{-5}$ are $1 \pm \sqrt{-5}$ irreducible and 2,3 are not equal to up to units.

Theorem 3.2 (Unique Factorisation of Ideals): Let *K* be a number field. Then every non-zero ideal of admits a factorisation into prime ideals $\mathcal{O}_K$. This factorisation is unique up to order.

Example: In $K = \mathbb{Q}(\sqrt{-5})$

(6) = $(2)(3) = (2, 1+\sqrt{-5})^2(3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$

$(1+\sqrt{-5})(1-\sqrt{-5}) = (2, 1+\sqrt{-5})(3, 1+\sqrt{-5})(2, 1+\sqrt{-5})(3, 1-\sqrt{5})$

Where $(2, 1+\sqrt{-5})$, $(3, 1+\sqrt{-5})$, $(3, 1-\sqrt{-5})$ are prime ideals.

Definition: Let $A, B \subset \mathcal{O}_K$ be ideals. Then *A divides D* $A \mid B$. If there exists $C \subset \mathcal{O}_K$ such that *A* . *C* = *D.* equivalently. IL 'in the prime factorisations

$$A = P_1^{m_1} \cdots P_k^{m_k}, \qquad B = P_1^{n_1} \cdots P_k^{n_k}$$

we have $m_i \le m_i$ for all $1 \le i \le k$

Remark. (i) For = $\alpha, \beta \in \mathcal{O}_K$ (α) if and only if $\alpha = \beta u$ for some $u \in \mathcal{O}_K^\times$

(ii) For ideals $A, B \subset \mathcal{O}_K$. $A \mid B$ if and only if $A \supset B$

(iii; To multiply ideals, just multiply their generators, e.g.

$$(2)(3) = (6)$$
$$(2, 1+\sqrt{-5})(3, 1+\sqrt{-5}) = (6, 2+2\sqrt{-5}, 3+3\sqrt{-5}, -4+2\sqrt{-5})$$
$$= (6, 1+\sqrt{-5})$$
$$= (1+\sqrt{-5}).$$

(iv) Addition of ideals works completely differently, simply combine the generators.

e.g., $(2)+(3) = (2,3) = (1) = \mathcal{O}_K.$

IDEAL CLASS GROUPS

Let K be a number field. Define an equivalence relation ~ on non-zero ideals by $A \sim B$ if $A = \lambda B$ for some $\lambda \in K^\times$. The *ideal class group* $\mathrm{Cl}(K)$ of K is the set of equivalence classes. This is in fact a group, the group structure conies from multiplication of ideals. That identity clement is the; class of principal ideals.

In particular $\mathcal{O}_K$ is a unique factorisation domain if and only ii" $\mathrm{Cl}(K) = 1$ $\mathrm{Cl}(K)$ is finite.

Exercise: Let $K = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic field. Then two non-zero ideals belong to the same class in $\mathrm{Cl}(K)$ if and only if the lattices they give in C are homothetic. I.e. related bv scaling and rotation about 0.

PRIMES AND MODULAR ARITHMETIC

Definition. A *prime* P in a number field K is a non-zero prime ideal in $\mathcal{O}_K$. Its *residue field* is $\mathcal{O}_K/P$

Example: where $K = \mathbb{Q}, \mathcal{O}_K = \mathbb{Z}, P = (p), \mathcal{O}_K/P = \mathbb{Z}/(p) = \mathbb{F}_p,$ p is a prime number.

Definition. That; *absolute residue degree* of P is $[\mathcal{O}_K/P : \mathbb{F}_p],$ where p = $\mathcal{O}_K/P$ char

EXAMPLE: QUADRATIC NUMBER FIELDS

Before we consider number fields in general, let us begin with the fairly concrete ease of quadratic number fields. A *quadratic number field* is an extension K of $\mathbb{Q}$ of degree 2. The fundamental examples (in fact, as we shall see in a moment the only example) arc fields of the form

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$$

where $d \in \mathbb{Q}$ is not the square of another rational number.

There is an issue that arises as soon as we write down these fields, and it is important that we deal with it immediately: what exactly do we mean by $\sqrt{d}?$. There are several possible answers to this question. The most obvious is that by $\sqrt{d}$ we mean a specific choice of a complex square root of *d*. $\mathbb{Q}(\sqrt{d})$ is then defined as a sub field of the complex numbers. The difficulty with this is that the notation is "$\sqrt{d}$" ambiguous; d has two complex square roots, and there is no algebraic way to tell them apart.

Algebraists have a standard way to avoid this sort of ambiguity; we can simply define

$$\mathbb{Q}(\sqrt{d}) = \mathbb{Q}[x]/(x^2 - d).$$

There is no ambiguity with this notation $\sqrt{d}$; really means *x*, and *x* behaves as a formal algebraic object with the property that $x^2 = d$

This second definition is somehow the algebraically correct one, as there is no ambiguity and it allows $\mathbb{Q}(\sqrt{d})$ to exist completely independently of the complex numbers. However, it is far easier to think about $\mathbb{Q}(\sqrt{d})$ as a subfield of the complex numbers. The ability to think of $\mathbb{Q}(\sqrt{d})$ as a subfield of the complex numbers also becomes important when one wishes to compare fields $\mathbb{Q}(\sqrt{d_1})$ and $\mathbb{Q}(\sqrt{d_2})$ for two different numbers *d* and the abstract algebraic fields $\mathbb{Q}[x]/(x^2 - d_1)$ and $\mathbb{Q}[y]/(y^2 - d_2)$ have no natural relation to each other, while these same fields viewed as sub fields of can be compared more easily.

The best approach, then, seems to be to pretend to follow the formal algebraic option, but to actually view everything as sub fields of the complex numbers. We can do this through the notion of a *complex embedding*; this is simply an injection

$$\sigma : \mathbb{Q}[x]/(x^2 - d) \hookrightarrow \mathbb{C}.$$

As we have already observed, there are exactly two such maps, one for each complex square root of *d.*

Before we continue we really ought to decide which complex number we mean by $\sqrt{d}$. There is unfortunately no consistent way to do this, in the sense that we cannot arrange to have

$\sqrt{d_1}\sqrt{d_2} = \sqrt{d_1 d_2}$ for all $d_1, d_2 \in \mathbb{Q}$.

In order to be concrete, let us choose $\sqrt{d}$ to be the positive square root of *d* for all $d > 0$ and $\sqrt{d}$ to be the positive square root of —*d* times *I* for all $d < 0$. (There is no real reason to prefer these choices, but since it doesn't really matter anyway we might as well fix ideas.) With this choice, our two complex embedding arc simply

$$\sigma_1 : \mathbb{Q}[x]/(x^2 - d) \hookrightarrow \mathbb{C}$$
$$\sigma_2 : \mathbb{Q}[x]/(x^2 - d) \hookrightarrow \mathbb{C}$$

defined by

$$\sigma_1(a + bx) = a + b\sqrt{d};$$
$$\sigma_2(a + bx) = a - b\sqrt{d}.$$

Given any $a + bx \in \mathbb{Q}[x]/(x^2 - d)$, we define its *conjugates* to be the images $\sigma_1(a + bx) = a + b\sqrt{d}$ and $\sigma_2(a + bx) = a - b\sqrt{d}.$

Note that these maps have the same image. This gives us yet another way to view the ambiguity: we can take $\mathbb{Q}(\sqrt{d})$ to be the subfield of $\{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ and $\mathbb{C},$ we remember that $\mathbb{Q}(\sqrt{d})$ has an *auto morphism* $a + b\sqrt{d} \mapsto a - b\sqrt{d}.$

This is the approach we will take; that is, we will regard $\mathbb{Q}(\sqrt{d})$ as a subfield of $\mathbb{C}$ via our choice of $\sqrt{d},$ but we always remember that $\sqrt{d}$ is ambiguous, and thus that we have an auto morphism of this field exchanging $\sqrt{d}$ and $-\sqrt{d}$. From this point of view, the conjugates of an element $a + b\sqrt{d}$ are $a + b\sqrt{d}$ and $a - b\sqrt{d}$

Let us now analyse these fields $K = \mathbb{Q}(\sqrt{d})$. Note first that every $\alpha \in K$ has degree either 1 or 2 over $\mathbb{Q}$, and it has degree 1 if and only if it is actually in $\mathbb{Q}$. In particular, if $\alpha \notin \mathbb{Q}$ then we must have $K = \mathbb{Q}(\alpha)$

Let us now compute the norms and traces from *K* to $\mathbb{Q}$. We take 1 $\sqrt{d}$, as our basis for *K* over $\mathbb{Q}$. Multiplication by $\alpha = a + b\sqrt{d}$ takes 1 to $a + b\sqrt{d}$ and $\sqrt{d}$ to $bd + a\sqrt{d},$ so the matrix for the linear transformation m_α is

$$\begin{bmatrix} a & bd \\ b & a \end{bmatrix}$$

The characteristic polynomial of this matrix is

$$x^2 - 2ax + (a^2 - bd^2).$$

Thus

$$\mathrm{N}_{K/\mathbb{Q}}(\alpha) = a^2 - bd^2$$

And

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 2a.$$

Note also that we have

$$\mathrm{N}_{K/\mathbb{Q}}(\alpha) = (a + b\sqrt{d})(a - b\sqrt{d})$$

And

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = (a + b\sqrt{d}) + (a - b\sqrt{d})$$

That is, the norm of ∞ is the product of its conjugates and the trace of ∞ is the sum of its conjugates. This follows immediately from the fact that the conjugates of ∞ are the two roots of the characteristic polynomial of ∞.

GALOIS THEORY OF NUMBER FIELDS

Let *K* be a Galois extension of Q of degree *n.* Recall that this means $\sigma_1, \ldots, \sigma_n$ that if denote the complex embedding of K, then the σ_i all have the same image in C. Let us denote this image by *KQ* for the remainder of this section. We wish to reinterpret the complex embedding as auto morphisms of K.

To do this, fix one embedding, say $\sigma_1 : K \to K_0$. Consider the *n* maps

$$\sigma_1^{-1} \circ \sigma_i : K \to K.$$

These maps are all auto morphisms of *K* (that is, is morphisms from *K* to *K)* since they σ_i are all isomorphism's from *K* to *KQ.*

We claim that in fact these arc all of the auto morphisms of K. So suppose $\sigma : K \to K$ that is any auto morphism of K. Then $\sigma_1 \circ \sigma : K \to K_0 \hookrightarrow \mathbb{C}$ is a complex embedding of K, and thus equals one of the σ_i. Thus $\sigma = \sigma_1^{-1} \circ \sigma_i$, as claimed. In general, if *M* is any sort of object, then the set of auto morphisms of *M* form a group with composition as the group law; this is because the composition of two auto morphisms and the inverse of an auto morphism arc again auto morphisms.

We define the *Galois group* $\mathrm{Gal}(K/\mathbb{Q})$ of *K* over Q to be the group of auto morphisms of K; our above arguments show that as a set $\mathrm{Gal}(K/\mathbb{Q})$ is just the maps: $\sigma_1^{-1} \circ \sigma_i$: $K \to K$. Note in particular that

$$(\sigma_1^{-1} \circ \sigma_i) \circ (\sigma_1^{-1} \circ \sigma_j)$$

And

$$(\sigma_1^{-1} \circ \sigma_i)^{-1} = \sigma_i^{-1} \circ \sigma_1$$

are again of the form $\sigma_1^{-1} \circ \sigma_k$ for some *k*, although it is not at all clear which *k* it is.

Note that $\mathrm{Gal}(K/\mathbb{Q})$ has order *n;* even if *K* is not Galois one could still consider the auto morphisms of K, but the above construction no longer works and it is somewhat harder to determine how many auto morphisms there are.

When one actually computes Galois groups, it is usually much simpler to consider the fields as subfields of C. So let *K* be a Galois number field which is also a subfield of C. The auto morphisms of *K* are now simply its complex embedding $\sigma_i : K \to K \subseteq \mathbb{C}$. (With our earlier notation, we really are just considering the case where σ_1 is the identity map.) Note in particular that $\sigma_i \circ \sigma_j$ and σ_i^{-1} are also complex embedding of K, although it is not immediately clear which.

To determine which, let ∞. be a primitive element for *K* over Q and let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$. be its conjugates, so that the complex embedding of *K* are given by $\sigma_i(\alpha) = \alpha_i$. We can now determine $\sigma_i \circ \sigma_j$ simply by determining for which k we have

$$\sigma_i \circ \sigma_j(\alpha) = \alpha_k;$$

we then have

$$\sigma_i \circ \sigma_j = \sigma_k.$$

EXAMPLE 4.1: Let *d* be a square free integer (other than 1) and consider the field $\mathbb{Q}(\sqrt{d})$. This has the two embedding σ_1 and σ_2 characterized by

$$\sigma_1(\sqrt{d}) = \sqrt{d}$$

and

$$\sigma_2(\sqrt{d}) = -\sqrt{d}.$$

We find that $\sigma_2\sigma_2(\sqrt{d}) = \sigma_2(-\sqrt{d}) = -\sigma_2(\sqrt{d}) = \sqrt{d};$

that is, $\sigma_2^2 = \sigma_1$. This confirms that

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$$

as it must be σ_1 ; is the identity element and is the σ_2 nontrivial element.

EXAMPLE - Consider the field

$$\sigma_1(\sqrt{2}) = \sqrt{2},\ \sigma_1(\sqrt{3}) = \sqrt{3}$$
$$\sigma_2(\sqrt{2}) = -\sqrt{2},\ \sigma_2(\sqrt{3}) = \sqrt{3}$$
$$\sigma_3(\sqrt{2}) = \sqrt{2},\ \sigma_3(\sqrt{3}) = -\sqrt{3}$$
$$\sigma_4(\sqrt{2}) = -\sqrt{2},\ \sigma_4(\sqrt{3}) = -\sqrt{3}$$

This field has $\mathbb{Q}(\sqrt{2},\sqrt{3})$ degree 4 over with complex embedding characterized.

One computes easily that each of σ_2, σ_3 and σ_4 have square σ_1 and that the product of any two of them is the third, so that is $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$ isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

REFERENCES

- Avigad, Jeremy (2006). \Methodology and metaphysics in the development of Dedekind's theory of ideals". In: The Architecture of Modern Mathematics. Ed. by Jose Ferreiros and Jeremy Gray. Oxford University Press, pp. 159{186 (cit. on pp. 8, 30).
- G.Greaves, Sieves in Number Theory. Results in Mathematics and Related Areas (3), 43. Springer-Verlag, Berlin, 2001.
- Gabor Ivanyos, Marek Karpinski, Lajos Ronyai, and Nitin Saxena. Trading GRH for algebra: algorithms for factoring polynomials and related structures. CoRR, abs/0811.3165, 2008. 30
- H.Cohen, A course in computational algebraic number theory, Springer-Verlag, Berlin, 1993. MR 94i:11105
- H.P.F. Swinnerton-Dyer. *A Brief Guide to Algebraic Number Theory*. University Press of Cambridge, 2001.
- Harper, M., and Murty, R., Euclidean rings of algebraic integers, *Canadian Journal of Mathematics*, **56**(1), (2004), 71-76.
- J. A. Buchmann and H. W. Lenstra, Jr., Approximating rings of integers in number fields, J. Th_eor. Nombres Bordeaux 6 (1994), no. 2, 221{260. MR 1360644 (96m:11092)
- J.W.S. Cassels, Global fields, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 42-84.
- Kimball Martin. Nonunique factorization and principalization in number fields. Proc. Amer. Math. Soc. 139, No. 9: 3025-3038, 2011.
- Lawrence C. Washington, Introduction to cyclotomic fields, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR 1421575 (97h:11130)
- M.Artin, Algebra, Prentice Hall Inc., Englewood Clients, NJ, 1991. MR 92g:00001
- Michael Atiyah and Ian G. Macdonald. Introduction to Commutative Algebra. Addison-Wesley, 1969.
- Mollin, Richard: Algebraic Number Theory. Chapman and Hall/CRC Press. 1999
- Murty, R., *Problems in Analytic Number Theory*, GTM/RIM 206, Springer-Verlag, 2001
- Ono, Takashi: An Introduction to Algebraic Number Theory. Plenum Publishing Corporation. 1990