MATH 797AP ALGEBRAIC NUMBER THEORY LECTURE NOTES

FARSHID HAJIR
FEBRUARY 26, 2014 – 11 : 20

1. Algebraic Number Fields and Rings

1.1. **Field extensions.** Suppose K is a field containing a subfield F. An element $\alpha \in K$ is called *algebraic over* F if there exists a non-zero polynomial $f \in F[x]$ such that $f(\alpha) = 0$. If α is algebraic over F, the set

$$I_\alpha(F) := \{f \in F[x] \mid f(\alpha) = 0\}$$

is a non-zero ideal of $F[x]$ (this is easy, but do check it). Since $F[x]$ is a PID (it is in fact a Euclidean ring with respect to the degree function), $I_\alpha(F)$ is generated by any least-degree non-zero element of it, in particular by the *monic* least-degree non-zero element of $I_\alpha(F)$, which we denote by $\mathrm{Irr}_\alpha(x; F) \in F[x]$ or, if F is understood, by $\mathrm{Irr}_\alpha(x)$. We call $\mathrm{Irr}_\alpha(x; F)$ the *minimal polynomial of* α over F. If $\alpha \in K$ is not algebraic over F, we say that it is *transcendental* over F.

A complex number $z \in \mathbb{C}$ is called algebraic or transcental depending on whether it is so with respect to the field of rational numbers $\mathbb{Q}$. We let $\mathbb{Q}^{\mathrm{alg}}$ be the set of all algebraic numbers in $\mathbb{C}$; as we will see shortly, it is a subfield of $\mathbb{C}$.

Exercise 1.1. *Show that if α is algebraic over F, then $\mathrm{Irr}_\alpha(x; F)$ is irreducible in $F[x]$.*

Reversing this process, suppose we start with a non-zero irreducible polynomial $f(x) \in F[x]$ of degree n and we seek a field containing F in which f has a root. In other words, now we have the irreducible polynomial f and we are searching for a "quantity" α whose minimal polynomial is f. A brilliant algebraic solution to this problem, advocated by Cauchy, Kronecker, and every algebraist who has followed them, is as follows. In the ring of polynomials, $F[x]$, consider the (principal) ideal $I = (f) = fF[x]$ generated by f. One shows (meaning "you should show") that I is a maximal ideal of $F[x]$, so that the quotient ring $K := F[x]/(f)$ is a field. The composite of natrual maps

This is the version of February 26, 2014.

$F \hookrightarrow F[x] \twoheadrightarrow K$ (which sends $a \mapsto a + I$) is a natural emebdding of F into K, so without too much abuse of language we can think of F as a subfield of K. But now, magically, what we have in K is a root of f, namely $\alpha := x + I$ because $f(\alpha) = f(x + I) = f(x) + I = I$, i.e. $f(\alpha) = 0$ in the ring K.

Definition 1.2. *Suppose K/F is an extension of fields. If $\alpha, \alpha' \in K$ are algebraic over F, we say that α' is a conjugate of α over F (or an F-conjugate of α) if $\mathrm{Irr}_\alpha(x; F) = \mathrm{Irr}_{\alpha'}(x; F)$. If α, α' are algebraic numbers, we say α' is a conjugate of α if this is so over $\mathbb{Q}$, i.e. if their minimial polynomials over $\mathbb{Q}$ coincide.*

Exercise 1.3. *If K/F is a finite extension, conjugacy of elements over F is an equivalence relation on K.*

Exercise 1.4. *Suppose $\alpha \in \mathbb{Q}^{\mathrm{alg}}$ is algebraic over $\mathbb{Q}$. Let*

$$\mathrm{Conj}_\alpha = \{\alpha' \in \mathbb{C} \mid \alpha' \text{ is conjugate to } \alpha\}.$$

Then

$$\mathrm{Irr}_\alpha(x) = \prod_{\alpha' \in \mathrm{Conj}_\alpha} (x - \alpha').$$

1.2. **The rich algebraic structure of field extensions.** Let K/F be an extension of fields. In other words, K is a field and F is a subfield of it; then the field operations immediately make K into a vector space over F. If it has been a while since you have thought about such objects, take a moment now to recall the axioms of a field as well as those of a vector space and verify for yourself the claim we have just made.

Now, the dimension of K as a vector space over F is called the *degree* of the extension and denoted by $[K : F]$. Thus, $[K : F] = \dim_F K$. Note that unless K and F are finite fields, the index of F as an *additive* subgroup of K is infinite so the notation $[K : F]$ should not be confused with the index $[K_+ : F_+]$.

We say that K is a finite extension of F (or K/F is a finite extension) if $[K : F]$ is finite. The seemingly innocent fact that on the one hand, we can think of elements of K as vectors in a vector space and, on the other hand, as elements of a field, creates a lot of algebraic structure (or some kind of "rigidity") on K. For instance, every element $\alpha \in K$ gives rise to an endomorphism $\ell_\alpha : K \to K$ defined by $\ell_\alpha(\beta) = \alpha\beta$, i.e. ℓ_α is nothing but the "left-multiplication by α" operator on the F-vector space K. [In an "ordinary" F-vector space K, you can multiply elements of K only by the scalars (elements of F)]. You can check easily that ℓ_α is a linear map for every $\alpha \in K$. We could say that

the F-vector space K comes equipped with an embedding into its own endomorphism ring, namely:

$$\ell : K \hookrightarrow \mathrm{Hom}_F(K, K).$$

Here $\mathrm{Hom}_F(K, K)$ (we also call it $\mathrm{End}_F(K)$ for short), is just the set of all F-linear maps from K to itself. Recall that this set is naturally endowed with the structure of a ring: we can add two endomorphisms by virtue of addition in K (namely for $T_i \in \mathrm{End}_F(K)$ and $x \in K$, we define $(T_1 + T_2)(x) = T_1(x) + T_2(x)$) and we can "multiply" them by composition: $T_1T_2(x) = T_1(T_2(x))$.

Exercise 1.5. *Verify the claim we made above that $\ell : K \hookrightarrow \mathrm{End}_F(K)$ is one-to-one. Check also that it is an F-linear ring homomorphism. (Of course $\mathrm{End}_F(K)$ is a an F-vector space in a natural way).*

Now let us assume that K/F is a finite extension. Thus, writing $n = [K : F]$ for the degree of K over F, we choose and fix an ordered list of elements $\mathcal{B} = (\alpha_1, \ldots, \alpha_n) \in K^n$ forming a basis for K as an F-vector space. By definition, for each $\alpha \in K$, there exists a unique vector $(c_1(\alpha), \ldots, c_n(\alpha)) \in F^n$ such that $\alpha = \sum_{i=1}^n c_i(\alpha)\alpha_i$. The map $\alpha \mapsto (c_1(\alpha), \ldots, c_n(\alpha))$ of course gives a vector space isomorphism $K \to F^n$, which in turn induces a ring isomorphism $\mu_{\mathcal{B}} : \mathrm{End}_F(K) \to \mathcal{M}_n(F)$. All we are saying here is that once we choose a basis $\mathcal{B}$ for a vector space K, an endomorphism T of K gives rise to a unique $n \times n$ matrix $\mu_{\mathcal{B}}(T)$ representing it. In particular, choosing and fixing a basis for K/F, composing ℓ with $\mu_{\mathcal{B}}$ gives us a map

$$K \to \mathrm{End}_F(K) \to \mathcal{M}_n,$$

which is in fact an *injective ring homomorphism* of K into $\mathcal{M}_n(F)$, the set of $n \times n$ matrices with entries in F. Note that $\mathcal{M}_n(F)$ is a non-commutative ring (for $n > 1$) but the image of K inside it is of course commutative, so in some sense this image is "small." It turns out to be a convenient place to do computations for many applications.

To expand on this remark, recall that $\mathcal{B}$ is chosen and fixed so we allow ourselves to drop it from a lot of the notation. Now, for $\alpha \in K$, let us put $M_\alpha := \mu_{\mathcal{B}}(\ell_\alpha)$. In other words, M_α is just the matrix for left-multiplication by α in the chosen basis.[1]

Example 1.6. *Let $f(x) = x^3 - x - 1$. Since f is cubic, it is either irreducible over $\mathbb{Q}$ or it has a linear factor over $\mathbb{Q}$. By Gauss's Lemma*

[1] I have allowed myself to drop the choice of $\mathcal{B}$ from the notation for my own convenience: please do not forget that M_α depends on the choice of this basis! We'll use the notation $M_\alpha^{\mathcal{B}}$ if we need to keep track of the basis. For a lot of what we will say, of course the choice of basis will not be important.

(see Problem 1), if f has a linear factor over $\mathbb{Q}$, then it has a linear factor in $\mathbb{Z}[x]$. But $f(\pm 1) \neq 0$ so f does not have a linear factor in $\mathbb{Z}[x]$ hence it is irreducible.

Let $K = \mathbb{Q}[x]/(f)$ or $K = \mathbb{Q}(\theta)$ where $\theta = x + (f)$. Then $[K : \mathbb{Q}] = 3$ and $\mathcal{B} = (1, \theta, \theta^2)$ is a basis for $K/\mathbb{Q}$. Let us determine M_θ for this basis. We compute the images of our basis vectors under left multiplication by θ: we have $\ell_\theta(1) = \theta$, $\ell_\theta(\theta) = \theta^2$ and $\ell_\theta(\theta^2) = \theta^3 = \theta + 1$. In other words,

$$M_\theta \begin{pmatrix} 1 \\ \theta \\ \theta^2 \end{pmatrix} = \theta \begin{pmatrix} 1 \\ \theta \\ \theta^2 \end{pmatrix} = \begin{pmatrix} \theta \\ \theta^2 \\ \theta + 1 \end{pmatrix},$$

which gives

$$M_\theta = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

You should calculate the characteristic and minimal polynomials of M_θ; the answer should not surprise you! Keeping in mind the fixed chosen basis for $K/\mathbb{Q}$, now M_θ "is" (a model for) θ; it carries all the information θ does but in a, perhaps, more tangible form. In a sense, we have torn ourselves away from the comfort of the commutativity of the field K for the tangibility of working with matrices and the (bargain basement) price we have paid is that of working in a non-commutative ring.

Now suppose we are asked to compute $M_{\theta+1}$. We could do it directly just as above, but: recalling that M_α is defined to be $(\mu \circ \ell)(\alpha)$ and recalling that μ and ℓ are ring homomorphisms, we note that

$$M_{c\alpha+\beta} = cM_\alpha + M_\beta, \qquad \alpha, \beta \in K, c \in F.$$

Since $M_1 = I_3$ (the identity) is easy to determine (why?) we find

$$M_{\theta+1} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

You can use this to calculate the minimal polynomial of $\theta + 1$. How? Well, it should be the characteristic polynomial of $M_{\theta+1}$, eh? We can double-check this by considering $\mathrm{Irr}_\theta(x-1)$; this is clearly a polynomial that has $\theta+1$ as a root. For practice, calculate also M_{θ^2}, and $M_{\theta^2+\theta+1}$.

Definition 1.7. *Suppose K/F is a finite extension and $\alpha \in K$. Let $\mathcal{B}$ be a fixed basis for K as a vector space over F. We define the (relative)*

norm and (relative) trace of α from K to F with respect to $\mathcal{B}$ to be, respectively,

$$\mathbb{N}_{K/F}(\alpha) = \det(M_\alpha), \qquad \mathrm{tr}_{K/F}(\alpha) = \mathrm{trace}(M_\alpha).$$

We recall that the trace of a matrix is the sum of its diagonal entries. We define $\mathrm{ch}_\alpha(x; K/F)$ be the characteristic polynomial of M_α.

Exercise 1.8. *Suppose $f(x) \in F[x]$ is a degree n irreducible polynomial over F, and let $K = F[x]/(f)$. Let $\theta := x + (f)$ be a root of f in K. Show that $\mathcal{B} = \{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ forms a basis for K as an F-vector space; this is called a power basis for K/F, for obvious reasons.*

Exercise 1.9. *Show that $\mathbb{N}_{K/F}(\alpha)$ and $\mathrm{tr}_{K/F}(\alpha)$ do not depend on the choice of basis $\mathcal{B}$ for K/F. [Basically, just invoke the right facts from linear algebra.]*

Exercise 1.10. *Show that $\mathrm{ch}_\alpha(x; K/F) = \mathrm{Irr}_\alpha(x; F)^{[K:F(\alpha)]}$.*

1.3. **Number fields.** An *algebraic number field* or *number field* is a field K which contains $\mathbb{Q}$ and which has finite dimension as a $\mathbb{Q}$-vector space. This definition is a little more general than what one finds in many textbooks, where an algebraic number field is defined to be a subfield of $\mathbb{C}$ of finite degree over $\mathbb{Q}$. Of course, it is extremely important that any number field has embeddings into $\mathbb{C}$ and is therefore isomorphic, as a field, to a subfield of $\mathbb{C}$ of finite degree over $\mathbb{Q}$; moreover, subfields of $\mathbb{C}$ are more tangible and concrete for a beginning student. But I think there are advantages to considering number fields as more abstract objects right from the outset.

For instance, even though handling elements of algebraic number fields as complex numbers can be very convenient (the number $7 + i\sqrt{3}$ is somehow more familiar than $7+(x^2+3)$!), once we talk about number fields of even mildly large degree (say 5), it is not so easy to write their elements as complex numbers in a way that is immediately useful and accurate for all computations (we can only write down so many digits of an algebraic number α satisfying $\alpha^5 - \alpha - 1 = 0$ for example, and we cannot express it in terms of nested radicals either!). As we have just noted in §1.2, another way to represent algebraic numbers is in terms of their associated matrices (once a basis is chosen for an ambient number field). This representation has the added advantage that now the algebraic number is captured completely in finite terms and in a completely comfortable computing environment (in the space of $n \times n$ matrices over $\mathbb{Z}$). At any rate, for these and many other reasons, it is useful to think of algebraic number fields as finite field extensions of $\mathbb{Q}$ and not just as subfields of $\mathbb{C}$.

1.4. **Integrality.** Recall that in the ordinary genesis of numbers, one defines whole numbers, then the ring of ordinary integers, then its fraction field $\mathbb{Q}$. Since $\mathbb{Q}$ is a field, it is important to consider its subrings. But we have a bit more structure on $\mathbb{Q}$, namely a *topology*. Indeed, $\mathbb{Q}$ is equipped with the usual metric (induced by the ordinary absolute value) so it is natural to consider its discrete subsets. Putting these two notions together, we ask: What are the discrete subrings of $\mathbb{Q}$? A subring $R \subseteq \mathbb{Q}$ must contain 0 and 1, so must contain $\mathbb{Z}$. Clearly, $\mathbb{Z} \subset \mathbb{Q}$ is indeed a discrete subset of $\mathbb{Q}$.

Exercise 1.11. *Prove that $\mathbb{Z}$ is the only discrete subring of $\mathbb{Q}$.*

[Hint: proof by contradiction, shift your non-integer to $(0, 1)$ and feed it repeatedly into the multiplication machine.]

Now, suppose $K/\mathbb{Q}$ is a finite extension. Just as arithmetic in $\mathbb{Q}$ is "really" carried out in some sense in the discrete subring $\mathbb{Z} \subset \mathbb{Q}$, there is a ring $\mathcal{O}_K \subset K$, called the ring of (algebraic) integers in K which is suitable for arithmetic calculations. When you think back to the basic facts of arithmetic (say, for example, the existence of a Euclidean algorithm for $\mathbb{Z}$), you appreciate the tremendous importance of the fact that $\mathbb{Z}$ is a discrete subset of $\mathbb{Q}$. In the same way, we desperately need a discrete analogue of $\mathbb{Z}$ for K, so we seek a "discrete" subring of K whose fraction field is K. It is not immediately how to do this following this line of discussion since we don't even have a topology on K as of yet. We will pursue this line of thinking later, but for now let us take the algebraic approach outlined by Dedekind and others, where the notion of "$\mathbb{Z}$-module of finite type" is a good algebraic reflection of our desire for having "discrete" subring of K.

If you recall the notion of integral closure from an algebra class, then it is easy to define the analogue of $\mathbb{Z}$ for K: it is the *integral closure* of $\mathbb{Z}$ in K. We recall the notion of integral closure in case it is rusty.

Definition 1.12. *If R is a subring of a ring S, and $s \in S$, then s is integral over R if it satisfies a* **monic** *polynomial over R, i.e. if there exists an integer $n \geq 1$ and elements $a_0, a_1, \ldots, a_{n-1}$ such that*

$$s^n + a_{n-1}s^{n-1} + \ldots + a_0 = 0.$$

The set of all elements of S which are integral over R is called the integral closure of R in S. Note that the latter contains R. If the integral closure of R in S is R, we say that R is integrally closed in S. If R is an integral domain, we say that R is integrally closed if its integral closure in its field of fractions is R itself.

Exercise 1.13. *(a) Show that* $1/2$ *is not integral over* $\mathbb{Z}$*. [Note: The topological approach would say* $1/2$ *is not an integer because* $\{(1/2)^n \mid n \geq 1\}$ *has a limit point in* $\mathbb{Q}$*.]*

(b) Show that $\mathbb{Z}$ *is integrally closed in* $\mathbb{Q}$*.*

(c) What is the integral closure of $\mathbb{Z}[\frac{1}{2}]$ *in* $\mathbb{Q}$*? Note:* $\mathbb{Z}[\frac{1}{2}]$ *is the set of rational numbers with* 2*-power denominator.*

Definition 1.14. *Suppose* K *is a field containing* $\mathbb{Q}$*. If* $\alpha \in K$ *is algebraic over* $\mathbb{Q}$*, i.e. if there exists* $f \in \mathbb{Q}[x]$ *such that* $f(\alpha) = 0$*, we say that* α *is an algebraic number. If there exists a* monic $f \in \mathbb{Z}[x]$ *such that* $f(\alpha) =$*, we say that* α *is an* algebraic integer*. We define*

$$\mathcal{O}_K = \{\alpha \in K \mid \alpha \text{ is an algebraic integer}\}.$$

In the exercises, you will prove the following important result.

Theorem 1.15. *An algebraic number* α *is an algebraic integer if and only if* $\mathrm{Irr}_\alpha(x; \mathbb{Q}) \in \mathbb{Z}[x]$*.*

Remark 1.16. *Note that this theorem furnishes an efficient algorithm for checking whether a given algebraic number is integral or not.*

Corollary 1.17. *If* α *is an algebraic integer, then every conjugate* α' *of* α *is an algebraic integer.*

Proof. By exercise 1.4, $\mathrm{Irr}_\alpha(x; \mathbb{Q}) = \mathrm{Irr}_{\alpha'}(x; \mathbb{Q})$ so one is in $\mathbb{Z}[x]$ if and only if the other is. □

If $K/\mathbb{Q}$ is finite, i.e. if K is an algebraic number field, then the set $\mathcal{O}_K$ forms a ring. Indeed, the name "ring" was at first invented by Dedeking to refer just to these *rings of algebraic integers*. In fact, many, if not most, of the basic terms of algebra were invented in the 19th century as mathematicians explored the foundations of algebraic number theory.

We now summarize the most important facts about $\mathcal{O}_K$, the ring of algebraic integers of a number field K. The proofs will come a bit later.

Theorem 1.18. *Suppose* $K/\mathbb{Q}$ *is a field extension of finite degree* n*. Then*

i) $\mathcal{O}_K$ *is a subring of* K *with fraction field* K*;*

ii) $\mathcal{O}_K$ *is a free* $\mathbb{Z}$*-module of rank* n*, i.e. there exist* $\omega_1, \ldots, \omega_n \in \mathcal{O}_K$ *such that for all* $\omega \in \mathcal{O}_K$ *there exists a unique* n*-tuple* $(a_1, \ldots, a_n) \in \mathbb{Z}^n$ *such that* $\omega = \sum_{i=1}^n a_i \omega_i$*.*

iii) For all ring homomorphisms $\sigma : K \to \mathbb{C}$*,* $\sigma(\mathcal{O}_K)$ *is a maximal discrete subring of* $\sigma(K)$*.*

Definition 1.19. *If K is an algebraic number field of degree n, an n-tuple $(\omega_1, \ldots, \omega_n) \in \mathcal{O}_K^n$ enjoying the property described in ii) of the above theorem, i.e. forming a $\mathbb{Z}$-basis for $\mathcal{O}_K$, is called an* ordered integral basis *for K (or for $\mathcal{O}_K$).*

Remark 1.20. *Since $\mathcal{O}_K$ is so canonically attached to K, and as in the definition just given, we often refer to an object as belonging to K when it properly belongs to its ring of integers $\mathcal{O}_K$. For example, we will often speak of a prime ideal of K (K, being a field, doesn't have too many of those!) when what we really mean is a prime ideal of $\mathcal{O}_K$. It is not expected that any confusion will arise from this widely adopted convention.*

1.5. **Facts about the ring of integers.** Here we prove various properties of the ring $\mathcal{O}_K$ listed in the previous section.

Theorem 1.21. *Suppose $\alpha \in K$ where $K/\mathbb{Q}$ is a fintie extension. The following are equivalent:*

i) α is an algebraic integer;

ii) $\mathrm{Irr}_\alpha(x) \in \mathbb{Z}[x]$;

iii) $\mathbb{Z}[\alpha]$ is finitely generated as $\mathbb{Z}$-module, i.e. its additive subgroup is a finitely generated abelian group;

iv) there exists a subring $L \subset K$ which is finitely generated as $\mathbb{Z}$-module and contains α;

v) there exists a finitely generated $\mathbb{Z}$-module L contained in K and stable under multiplication by α i.e. such that $\alpha L \subseteq L$.

Proof. That i) implies ii) is a homework problem [HW 1, Problem 2] and already mentioned as Theorem 1.15. Now ii) $\Rightarrow$ iii) is simple: by definition, the additive group of $\mathbb{Z}[\alpha]$ is generated by the powers of α, but if $\mathrm{Irr}_\alpha(x) \in \mathbb{Z}[x]$ has degree n, then $\alpha^k \in [1, \alpha, \alpha^2, \ldots, \alpha^{n-1}]_{\mathbb{Z}}$, for $k = n$, and then this is so for all $k > n$ by induction. Thus, $\mathbb{Z}[\alpha]$ is a $\mathbb{Z}$-module of finite type. The implications iii) $\Rightarrow$ iv) and iv) $\Rightarrow$ v) are immediate, leaving us to prove that v) $\Rightarrow$ i). Suppose L is an additive subgroup of K generated by $\lambda_1, \ldots, \lambda_d$ (not all 0) as $\mathbb{Z}$-module. Since $\alpha L \in L$, there exists a matrix $M \in M_d(\mathbb{Z})$ such that

$$\alpha \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_d \end{pmatrix} = M \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_d \end{pmatrix}.$$

In other words, $\alpha I_d - M$ kills the vector $(\lambda_1, \ldots, \lambda_d)^t$, which is by assumption non-zero. Hence α is an eigenvalue of M, i.e. a root of the characteristic polynomial $\det(xI_d - M)$, which (since $M \in \mathcal{M}_d(\mathbb{Z})$) is clearly a monic degree d polynomial in $\mathbb{Z}[x]$, proving i). $\square$

Corollary 1.22. *The sum, difference, and product of two algebraic integers is an algebraic integer. If K is a number field, then $\mathcal{O}_K$ is a subring of K whose field of fractions is K.*

Proof. The second claim follows immediately from the first. Suppose α, β are algebraic integers. By Theorem 1.21, $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated $\mathbb{Z}$-modules; say the first is generated by $\alpha_1, \ldots, \alpha_m$ and the second by $\beta_1, \ldots, \beta_n$. Then $\mathbb{Z}[\alpha, \beta]$ is generated by the mn elements $\alpha_i \beta_j$, and is, in particular, finitely generated. Since $\alpha \pm \beta, \alpha\beta \in \mathbb{Z}[\alpha, \beta]$, we are done by appealing to Theorem 1.21 once again. Finally, to show that the field of fractions of $\mathcal{O}_K$ is K, we merely invoke one of the homework problems: if $\alpha \in K$, then there exists $m \in \mathbb{Z}$ such that $m\alpha \in \mathcal{O}_K$. □

Exercise 1.23. *To illustrate the above proof, compute a matrix representing $\alpha = \sqrt{3} + \sqrt{5}$ and use it to show that this real number is an algebraic integer. [In the field $\mathbb{Q}(\sqrt{3}, \sqrt{5})$, consider the $\mathbb{Z}$-module $L = [1, \sqrt{3}, \sqrt{5}, \sqrt{15}]_{\mathbb{Z}}$. Now compute the matrix for multiplication by $\sqrt{3}+\sqrt{5}$ as well as its characteristic polynomial: why does this (monic, $\mathbb{Z}$-integral) polynomial kill α? Recalling Exercise 1.4, can we also compute $Irr_\alpha(x)$ via a product over conjugates? What are the conjugates of α over $\mathbb{Q}$?]*

Exercise 1.24. *Suppose $\alpha \in \mathbb{Q}^{\mathrm{alg}}$. Show that α is an algebraic integer if and only if $\mathbb{Z}[\alpha]$ is a discrete subring of $\mathbb{Q}(\alpha)$.*

1.6. **The matrix approach vs. the conjugate approach, in which each side of the debate comes to admire the other side's strengths and bemoans its own drawbacks, following which catharsis both sides rally to cheer each other up and agree to coexist peacefully.** So far, we have championed the "matrix model" for understanding and working with algebraic numbers. It is now time to pay homage to the "embed everything in $\mathbb{C}$" approach. What one must deal with is that if $n := [K : \mathbb{Q}] > 1$, there are in fact several ways to embed K into $\mathbb{C}$ and it turns out that the best thing to do is to wrap all of these embeddings together into one fabulously useful Euclidean embedding $K \hookrightarrow \mathbb{R}^n$. The image of this map is a dense subset of $\mathbb{R}^n$ (just as $\mathbb{Q}$ is dense in $\mathbb{R}$), and the image of $\mathcal{O}_K$ is a (discrete) *lattice* of rank n in $\mathbb{R}^n$! This means that we can "see" some of the arithmetic geometrically, which is often very useful.

If K is a number field of degree n, then K has n distinct embeddings into $\mathbb{C}$. Here is a concrete description of them. Using the theorem of the primitive element (a future homework problem, perhaps), we can "model" K by a polynomial $f \in \mathbb{Q}[x]$. Namely, we can find $\theta \in K$

such that $K = \mathbb{Q}(\theta)$. Letting $f(x) = \mathrm{Irr}_\theta(x;\mathbb{Q}) \in \mathbb{Q}[x]$, we have $K \approx \mathbb{Q}[x]/(f)$. Multiplying θ by an appropriate integer, if necessary, we may and will assume (HW 1) that $f(x) \in \mathbb{Z}[x]$. Now we factor $f(x)$ into linear factors over $\mathbb{C}$, viz.

$$f(x) = \prod_{i=1}^{n}(x - \theta^{(i)}).$$

We call the elements of $\mathrm{Roots}_f := \{\theta^{(i)} \mid 1 \le i \le n\}$ the conjugates of θ in $\mathbb{Q}^{\mathrm{alg}}$. For each $i = 1, 2, \ldots, n$, the assignment $\sigma_i(\theta) = \theta^{(i)}$ extends to a unique ring homomorphism $\sigma_i : K \hookrightarrow \mathbb{C}$, namely $\sigma_i(g(\theta)) := g(\theta^{(i)})$ for $g \in \mathbb{Q}[x]$.

Recall that we have defined maps $\mathrm{tr}_{K/\mathbb{Q}} : K \to \mathbb{Q}$, $\mathbb{N}_{K/\mathbb{Q}} : K \to \mathbb{Q}$, and $\mathrm{ch}_\bullet(x; K/F) : K \to \mathbb{Q}[x]$ in Definition 1.7. The following proposition explains how one can compute these maps using conjugates instead of matrices.

Proposition 1.25. *Suppose K is a number field of degree n, with n distinct embeddings $\sigma_1, \ldots, \sigma_n$ into $\mathbb{C}$. Let $\alpha \in K$ have degree d over $\mathbb{Q}$ i.e. $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$. Then,*

$$\mathrm{tr}_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n}\sigma_i(\alpha) = \frac{n}{d}\mathrm{tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha), \qquad \mathbb{N}_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n}\sigma_i(\alpha) = \mathbb{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)^{n/d}.$$

These numbers are, respectively, $-a_{n-1}$ and $(-1)^n a_0$ where $\mathrm{ch}_\alpha(x; K/\mathbb{Q}) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$.

Proposition 1.26 (Transitivity of norm and trace)**.** *If $L/K/F$ is a tower of number fields, then $\mathrm{tr}_{L/F} = \mathrm{tr}_{K/F} \circ \mathrm{tr}_{L/K}$ and $\mathbb{N}_{L/F} = \mathbb{N}_{K/F} \circ \mathbb{N}_{L/K}$.*

Quite often, it will turn out convenient to order the n embeddings of $K \approx \mathbb{Q}[x]/(f)$ into $\mathbb{C}$ (or, what is the same, the n roots of f in $\mathbb{C}$) in the following way. We assume that r_1 of the roots of f are real, giving $2r_2$ complex conjugate pairs of roots, where $r_1 + 2r_2 = n$. We relabel the roots so that $\theta^{(1)}, \ldots, \theta^{(r_1)}$ are the r_1 real roots, $\theta^{(r_1+1)}, \ldots, \theta^{(r_1+r_2)}$ is a collection of r_2 non-complex-conjugate roots[2] and let $\theta^{(r_1+r_2+j)} = \overline{\theta^{(r_1+j)}}$ for $j = 1, \ldots, r_2$. Now, the assignment

$$\theta \mapsto (\theta^{(1)}, \ldots, \theta^{(r_1)}, \Re(\theta^{(r_1+1)}), \mathrm{Im}(\theta^{(r_1+1)}), \ldots, \Re(\theta^{(r_1+r_2)}), \mathrm{Im}(\theta^{(r_1+r_2)})$$

extends to a unique additive homomorphism

$$\sigma : K \hookrightarrow \mathbb{R}^n$$

[2]We will not need this comment for the course, but this choice of r_2 non-complex-conjugate non-real roots of f is called a "CM-type" for K.

which is an embedding because its kernel clearly vanishes. In other words,

$$\sigma = (\sigma_1, \ldots, \sigma_{r_1}, \Re\sigma_{r_1+1}, \mathrm{Im}\sigma_{r_1+1}, \ldots, \Re\sigma_{r_1+r_2}, \mathrm{Im}\sigma_{r_1+r_2}).$$

Now, $\sigma(\mathcal{O}_K) \subset \sigma(K) \subset \mathbb{R}^n$ is an n-dimensional Euclidean lattice Λ_σ: if $\mathcal{O}_K = [\omega_1, \ldots, \omega_n]_\mathbb{Z}$, then $\Lambda_\sigma = [\sigma(\omega_1), \ldots, \sigma(\omega_n)]_\mathbb{Z}$, so we just have to show that the $\sigma(\omega_i)$ are linearly independent over $\mathbb{R}$. This follows from the following lemma.

Lemma 1.27. *The square of the determinant of the matrix whose ith row vector is $\sigma(\omega_i)$ does not vanish.*