ARITHMETIC STATISTICS COURSE NOTES

ROBERT J. LEMKE OLIVER

2. Rings of integers and discriminants

We now turn to considering what will prove to be some of the most fundamental objects to this course, namely *rings of integers*. We begin with several definitions and lemmas.

2.1. **Algebraic integers.**

Definition. A number $\alpha \in \mathbb{C}$ is called an *algebraic integer* if it is the root of a monic polynomial $f \in \mathbb{Z}[x]$.

We've given this definition relative to roots of any monic integer polynomial because that's the definition that's easiest to check, but in fact, we could have defined it relative to irreducible polynomials only (as are usually considered when dealing with field extensions).

Lemma 2.1. *A number α is an algebraic integer if and only if it is the root of an irreducible monic polynomial $f \in \mathbb{Z}[x]$.*

Proof. One direction is immediate: if α is the root of an irreducible monic polynomial, then it's an algebraic integer by definition.

Conversely, suppose that α is the root of some monic integer polynomial, $f \in \mathbb{Z}[x]$. If f is not irreducible, then it must factor as $f = f_1 f_2$. We thus find $f(\alpha) = f_1(\alpha) f_2(\alpha)$, but $f(\alpha) = 0$, so either $f_1(\alpha) = 0$ or $f_2(\alpha) = 0$ since $\mathbb{C}$ is a field; suppose $f_1(\alpha) = 0$. If f_1 is irreducible, we're done, and if not, we can repeat this process, eventually ending at an irreducible polynomial of which α is a root. □

We next show that the set of all algebraic integers forms a ring under the conventional notions of addition and multiplication. This is provided by the following lemma.

Lemma 2.2. *Suppose α and β are algebraic integers. Then both $\alpha + \beta$ and $\alpha\beta$ are algebraic integers as well.*

Proof sketch. We begin with some preliminary observations. By definition, both α and β are roots of monic integer polynomials, say

$$f_\alpha(x) = x^n + a_1 x^{n-1} + \cdots + a_n, \quad f_\beta(x) = x^m + b_1 x^{m-1} + \cdots + b_m.$$

We will find it useful to aslso factor f_α and f_β over $\mathbb{C}$. By the fundamental theorem of algebra, they each factor completely into linear polynomials, say

$$f_\alpha(x) = \prod_{i=1}^{n} (x - \alpha_i), \quad f_\beta(x) = \prod_{j=1}^{m} (x - \beta_j).$$

Date: January 31, 2022.

Necessarily, $\alpha = \alpha_i$ for some i, and $\beta = \beta_j$ for some j.[1] Observe finally that the coefficients of f_α and f_β may therefore be expressed in terms of the roots, e.g.

$$a_1 = -(\alpha_1 + \cdots + \alpha_n), \quad a_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n = \sum_{i_1<i_2} \alpha_{i_1}\alpha_{i_2},$$

and in general

$$a_k = (-1)^k \sum_{i_1<i_2<\cdots<i_k} \alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_k},$$

with analogous expressions for the b_j.

We now show that $\alpha+\beta$ is an algebraic integer. Consider the polynomial

$$f_{\alpha+\beta}(x) := \prod_{i=1}^{n}\prod_{j=1}^{m}(x-\alpha_i-\beta_j).$$

We claim that, using the expressions for a_i and b_j in terms of the α_i and β_j, it is possible to show that this polynomial has integer coefficients.[2] By construction, it is a monic polynomial for which $\alpha+\beta$ is a root, so $\alpha+\beta$ is an algebraic integer. Similarly, $\alpha\beta$ is a root of the polynomial

$$f_{\alpha\beta}(x) := \prod_{i=1}^{n}\prod_{j=1}^{m}(x-\alpha_i\beta_j).$$

□

This brings us to arguably the most important definition of this course:

Definition. If K is a number field (i.e., a finite degree extension of $\mathbb{Q}$), the *ring of integers* of K, usually denoted $\mathcal{O}_K$, is the set of algebraic integers contained in K.

The name "ring of integers" is justified by the observation that Lemma 2.2, together with the closure properties of K itself, imply that $\mathcal{O}_K$ is a ring.

Here are some simple motivating examples:

- $K = \mathbb{Q}$. In this case, $\mathcal{O}_K = \mathbb{Z}$. (What are the irreducible polynomials that have rationals as roots?)
- $K = \mathbb{Q}(i)$. In this case, $\mathcal{O}_K = \mathbb{Z}[i]$, often referred to as the Gaussian integers.
- $K = \mathbb{Q}(\sqrt{-3})$. In this case, $\mathcal{O}_K \supset \mathbb{Z}[\sqrt{-3}]$, but $\alpha = \frac{1+\sqrt{-3}}{2}$ is a root of the polynomial x^2+x+1, so is an algebraic integer, and $\alpha \notin \mathbb{Z}[\sqrt{-3}]$. It turns out that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for this α.
- $K = \mathbb{Q}(\sqrt{5})$. In this case, $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

We will consider higher degree field extensions later, but for now, we find it convenient to note the following characterization of the ring of integers of quadratic fields.

Lemma 2.3. *If $K = \mathbb{Q}(\sqrt{d})$ for some squarefree $d \neq 1$, either positive or negative, then $\mathcal{O}_K = \mathbb{Z}[\alpha]$, where*

$$\alpha = \begin{cases} \frac{1+\sqrt{d}}{2}, & \textit{if } d \equiv 1 \pmod 4 \\ \sqrt{d}, & \textit{if } d \equiv 2,3 \pmod 4. \end{cases}$$

[1] Without loss of generality, you may assume $\alpha = \alpha_1$ and $\beta = \beta_1$, but in fact, the proof we will write down is "index agnostic," and this won't substantially simplify things.

[2] You should, exactly once in your lifetime, think through why this is true. Useful keywords beyond those already presented if you want to look things up include "symmetric functions."

Proof. Exercise. □

2.2. **Visualizing rings of integers.** In the case of $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$ (or, in fact, any $\mathbb{Q}(\sqrt{d})$ with negative d), there is a ready-made way to visualize the ring of integers $\mathcal{O}_K$. In particular, such fields are subfields of the complex numbers, and there is a standard visualization of $\mathbb{C}$ as $\mathbb{R}^2$. We find the following for $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$.

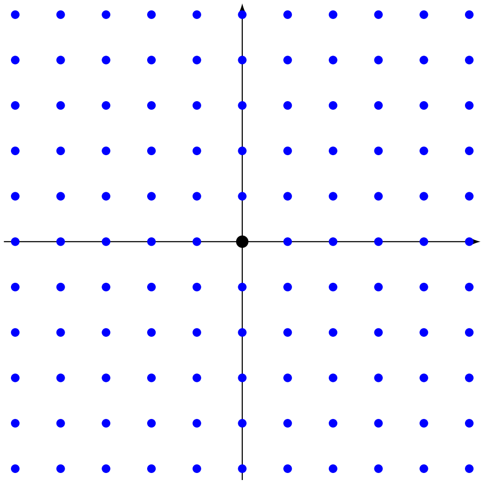

FIGURE 1. The ring of integers $\mathbb{Z}[i]$ for $\mathbb{Q}(i)$.

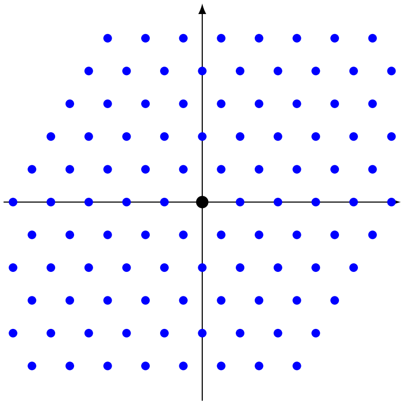

FIGURE 2. The ring of integers $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ for $\mathbb{Q}(\sqrt{-3})$.

In particular, we observe that each of these rings of integers is a lattice in $\mathbb{R}^2$. On the other hand, $\mathbb{Q}(\sqrt{5})$ most naturally embeds into $\mathbb{R}$, not $\mathbb{R}^2$. It turns out (not entirely obviously) that the ring of integers $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ is dense in $\mathbb{R}$; see Figure 3.

Our first goal is to provide a way of visualizing $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ as a lattice, analogous to Figures 1 and 2. For this, we need the notion of *embeddings*.

Definition. A real embedding of a number field K is an injective homomorphism $\sigma\colon K \hookrightarrow \mathbb{R}$. A complex embedding of a number field K is an injective homomorphism $\sigma\colon K \hookrightarrow \mathbb{C}$ that doesn't factor through an embedding to $\mathbb{R}$ (equivalently, whose image $\sigma(K)$ is not contained in $\mathbb{R}$). An embedding of K is implicitly either a real or complex embedding.

FIGURE 3. A (bad!) visualization of the ring of integers $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ of $\mathbb{Q}(\sqrt{5})$ on the number line.

We summarize several useful facts in the following lemma.

Lemma 2.4. *Let K be a number field of degree n. Then:*

1. *If $\alpha \in K$ is a root of $f \in \mathbb{Q}[x]$, then so is $\sigma(\alpha)$.*
2. *There are exactly n embeddings of K.*
3. *Complex embeddings come in pairs, differing by complex conjugation.*
4. *If r_1 denotes the number of real embeddings of K and r_2 denotes the number of pairs of complex embeddings, then $n = r_1 + 2r_2$.*
5. *If $\widetilde{K}$ denotes the normal closure[3] of K, then $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ acts faithfully and transitively on the set of embeddings of K.*

Proof. 1) Since σ is an injective field homomorphism, it fixes $\mathbb{Q}$. Thus, for any $f \in \mathbb{Q}[x]$ and any $\alpha \in K$, $\sigma(f(\alpha)) = f(\sigma(\alpha))$, so $\sigma(\alpha)$ is a root of f if and only if α is.

2) Since K has degree n, there is some α for which $K = \mathbb{Q}(\alpha)$ and whose minimal polynomial $f_\alpha(x)$ has degree n. By part 1), $\sigma(\alpha)$ must be one of the n conjugates of α, and this choice completely determines σ since σ must fix $\mathbb{Q}$. Each of these n choices defines an embedding, and thus there are exactly n embeddings of K.

3) Let τ denote complex conjugation. If σ is a complex embedding, then $\tau \circ \sigma$ is also an embedding of K, necessarily not equal to σ since σ is complex.

4) Follows from 2) and 3).

5) By 1) and 2), if $K = \mathbb{Q}(\alpha)$, then embeddings of K are in correspondence with a choice $\sigma(\alpha) = \alpha_i$, where $\alpha_1, \ldots, \alpha_n$ are the conjugates of α. Moreover, $\widetilde{K} = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, so all α_i are defined in $\widetilde{K}$. An element $\phi \in \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ is a field automorphism of $\widetilde{K}$, which must send each α_i to some α_j. That is, it acts on the set $\{\alpha_1, \ldots, \alpha_n\}$. It therefore also acts in the obvious way on the set of embeddings by exploiting the correspondence between embeddings and conjugates.

A "transitive" action of a group G on a set $\{1, \ldots, n\}$ is one for which, for every pair (i, j), there is an element $g \in G$ for which $g(i) = j$. There is a field automorphism $\phi \in \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ for which $\phi(\alpha) = \alpha_i$ for any i, from which follows that the action of $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ on the set of conjugates of α is transitive. By the way we defined the action on the set of embeddings, it follows that the action of $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ on the set of embeddings is also transitive.

An action is "faithful" if only the identity element fixes everything. The action of $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ on the conjugates $\alpha_1, \ldots, \alpha_n$ is faithful: if $\phi(\alpha_i) = \alpha_i$ for each i, then since $\widetilde{K} = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, ϕ must be the identity automorphism. Since we have defined the action of $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ on

[3] i.e., splitting field

embeddings via its action on conjugates, it follows that the action of $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ on the set of embeddings must be faithful as well. □

Remark. There's a lot of formal manipulation going on in the statement and proof of the fifth claim. Here's the real point. We can abstractly construct number fields as quotients $\mathbb{Q}[x]/(f(x))$ where $f(x)$ is an irreducible polynomial, but in this formalism we haven't "picked a root." For example, if $f(x) = x^2 - 2$, then we have formally constructed $\mathbb{Q}(\sqrt{2}) \simeq \mathbb{Q}[x]/(x^2 - 2)$ without having to specify which squareroot of 2 we mean. We can let embeddings "choose" a squareroot for us. The substance of the fifth point is entirely that instead of the (very useful!) notion that the Galois group permutes roots of irreducible polynomials, it instead permutes the embeddings. In modern number theory, it's considered gauche to fix a root when thinking about number fields. You'll never actually be misled if you want to fix a root, but it's both psychologically and mathematically important to remember you could have made a different choice, and that embeddings create the universes in which you made that alternate choice.