

₁ ALGEBRAIC NUMBER THEORY,
₂ A COMPUTATIONAL APPROACH

₃ William Stein

₄ May 1, 2019

Chapter 1

Basic Commutative Algebra

The commutative algebra in this chapter provides a foundation for understanding the more refined number-theoretic structures associated to number fields.

First we prove the structure theorem for finitely generated abelian groups. Then we establish the standard properties of Noetherian rings and modules, including a proof of the Hilbert basis theorem. We also observe that finitely generated abelian groups are Noetherian \mathbb{Z} -modules. After establishing properties of Noetherian rings, we consider rings of algebraic integers and discuss some of their properties.

1.1 Finitely Generated Abelian Groups

Finitely generated abelian groups arise all over algebraic number theory. For example, they will appear in this book as class groups, unit groups, and the underlying additive groups of rings of integers, and as Mordell-Weil groups of elliptic curves.

In this section, we prove the structure theorem for finitely generated abelian groups, since it will be crucial for much of what we will do later.

Let $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ denote the ring of (rational) integers, and for each positive integer n , let $\mathbb{Z}/n\mathbb{Z}$ denote the ring of integers modulo n , which is a cyclic abelian group of order n under addition.

Definition 1.1.1 (Finitely Generated). A group G is *finitely generated* if there exists $g_1, \dots, g_n \in G$ such that every element of G can be expressed as a finite product (or sum, if we write G additively) of positive or negative powers of the g_i .

31 For example, the group \mathbb{Z} is finitely generated, since it is generated by 1.

Theorem 1.1.2 (Structure Theorem for Finitely Generated Abelian Groups).
 Let G be a finitely generated abelian group. Then there is an isomorphism

$$G \approx (\mathbb{Z}/n_1\mathbb{Z}) \oplus (\mathbb{Z}/n_2\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/n_s\mathbb{Z}) \oplus \mathbb{Z}^r,$$

32 where $r, s \geq 0$, $n_i > 1$ for all i , and $n_1 \mid n_2 \mid \cdots \mid n_s$. Furthermore, the n_i
 33 and r are uniquely determined by G .

34 **Exercise 1.1.3.** Quick! Guess how many abelian groups there are of order
 35 less than 12. Use Theorem 1.1.2 to classify all abelian groups of order less
 36 than 12. How many do you think there are? How many are there?

37 We will prove the theorem as follows. We first remark that any subgroup
 38 of a finitely generated free abelian group is finitely generated. Then we see
 39 how to represent finitely generated abelian groups as quotients of finite rank
 40 free abelian groups, and how to reinterpret such a presentation in terms of
 41 matrices over the integers. Next we describe how to use row and column
 42 operations over the integers to show that every matrix over the integers is
 43 equivalent to one in a canonical diagonal form, called the Smith normal form.
 44 We obtain a proof of the theorem by reinterpreting the in terms of groups.
 45 Finally, we observe that the representation in the theorem is necessarily
 46 unique.

47 **Proposition 1.1.4.** If H is a subgroup of a finitely generated abelian group
 48 G , then H is finitely generated.

49 The key reason that this is true is that G is a finitely generated module
 50 over the principal ideal domain \mathbb{Z} . We defer the proof of Proposition 1.1.4 to
 51 Section 1.2, where we will give a complete proof of a beautiful generalization
 52 in the context of Noetherian rings (the Hilbert basis theorem).

53 **Corollary 1.1.5.** Suppose G is a finitely generated abelian group. Then
 54 there are finitely generated free abelian groups F_1 and F_2 and there is a
 55 homomorphism $\psi : F_2 \rightarrow F_1$ such that $G \approx F_1/\psi(F_2)$.

56 *Proof.* Let x_1, \dots, x_m be generators for G . Let $F_1 = \mathbb{Z}^m$ and let $\varphi : F_1 \rightarrow G$
 57 be the homomorphism that sends the i th generator $(0, 0, \dots, 1, \dots, 0)$ of \mathbb{Z}^m
 58 to x_i . Then φ is surjective, and by Proposition 1.1.4 the kernel $\ker(\varphi)$ of
 59 φ is a finitely generated abelian group. Suppose there are n generators for
 60 $\ker(\varphi)$, let $F_2 = \mathbb{Z}^n$ and fix a surjective homomorphism $\psi : F_2 \rightarrow \ker(\varphi)$.
 61 Then $F_1/\psi(F_2)$ is isomorphic to G . \square

An *sequence* of homomorphisms of abelian groups

$$H \xrightarrow{f} G \xrightarrow{g} K$$

is exact if $\text{im}(f) = \ker(g)$. For longer sequences, exactness means every three consecutive terms with two arrows are exact. Given a finitely generated abelian group G , Corollary 1.1.5 provides an exact sequence

$$F_2 \xrightarrow{\psi} F_1 \rightarrow G \rightarrow 0.$$

Suppose G is a nonzero finitely generated abelian group. By the corollary, there are free abelian groups F_1 and F_2 and there is a homomorphism $\psi : F_2 \rightarrow F_1$ such that $G \approx F_1/\psi(F_2)$. Upon choosing a basis for F_1 and F_2 , we obtain isomorphisms $F_1 \approx \mathbb{Z}^n$ and $F_2 \approx \mathbb{Z}^m$ for integers n and m . Just as in linear algebra, we view $\psi : F_2 \rightarrow F_1$ as being given by left multiplication by the $n \times m$ matrix A whose columns are the images of the generators of F_2 in \mathbb{Z}^n . We visualize this as follows:

$$\mathbb{Z}^m \xrightarrow{A} \mathbb{Z}^n \rightarrow G \rightarrow 0$$

62 The *cokernel* of the homomorphism defined by A is the quotient of \mathbb{Z}^n
 63 by the image of A (i.e., the \mathbb{Z} -span of the columns of A), and this cokernel
 64 is isomorphic to G .

65 The following proposition implies that we may choose a bases for F_1 and
 66 F_2 such that the matrix of A only has nonzero entries along the diagonal,
 67 so that the structure of the cokernel of A is trivial to understand.

68 **Proposition 1.1.6** (Smith normal form). *Suppose A is an $n \times m$ integer*
 69 *matrix. Then there exist invertible integer matrices P and Q such that*
 70 *$A' = PAQ$ only has nonzero entries along the diagonal, and these entries*
 71 *are $n_1, n_2, \dots, n_s, 0, \dots, 0$, where $s \geq 0$, $n_i \geq 1$ for all i , and $n_1 \mid n_2 \mid \dots \mid n_s$.*

72

INSERT EXAMPLE

73 **Remark 1.1.7.** Note that the matrices P and Q are invertible as integer
 74 matrices, so $\det(P)$ and $\det(Q)$ are ± 1 . In particular $\det A' = \pm \det A$.

75 **Definition 1.1.8.** The matrix A' in Proposition 1.1.6 is called the *Smith*
 76 *normal form* of A .

We will see in the proof of Theorem 1.1.2 that A' is uniquely determined by A . An example of a matrix in Smith normal form is

$$A = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

77 *Proof of Proposition 1.1.6.* The matrix P will be a product of matrices that
 78 define elementary row operations and Q will be a product corresponding to
 79 elementary column operations. The elementary row and column operations
 80 over \mathbb{Z} are as follows:

81 **Add multiple:** Add an integer multiple of one row to another (or a multi-
 82 ple of one column to another).

83 **Swap:** Interchange two rows or two columns.

84 **Rescale:** Multiply a row by -1 .

85 Each of these operations is given by left or right multiplying by an invertible
 86 matrix E with integer entries, where E is the result of applying the given
 87 operation to the identity matrix, and E is invertible because each operation
 88 can be reversed using another row or column operation over the integers.

89 To see that the proposition must be true, assume $A \neq 0$ and perform
 90 the following steps (compare [Art91, pg. 459]):

- 91 1. By permuting rows and columns, move a nonzero entry of A with
 92 smallest absolute value to the upper left corner of A . Now “attempt”
 93 (as explained in detail below) to make all other entries in the first row
 94 and column 0 by adding multiples of the top row or first column to
 95 other rows or columns, as follows:

96 Suppose a_{i1} is a nonzero entry in the first column, with
 97 $i > 1$. Using the division algorithm, write $a_{i1} = a_{11}q + r$,
 98 with $0 \leq r < a_{11}$. Now add $-q$ times the first row to the
 99 i th row. If $r > 0$, then go to step 1 (so that an entry with
 100 absolute value at most r is the upper left corner).

101 If at any point this operation produces a nonzero entry in the matrix
 102 with absolute value smaller than $|a_{11}|$, start the process over by per-
 103 muting rows and columns to move that entry to the upper left corner
 104 of A . Since the integers $|a_{11}|$ are a decreasing sequence of positive
 105 integers, we will not have to move an entry to the upper left corner
 106 infinitely often, so when this step is done the upper left entry of the
 107 matrix is nonzero, and all entries in the first row and column are 0.

- 108 2. We may now assume that a_{11} is the only nonzero entry in the first
 109 row and column. If some entry a_{ij} of A is not divisible by a_{11} , add
 110 the column of A containing a_{ij} to the first column, thus producing an
 111 entry in the first column that is nonzero. When we perform step 2,

the remainder r will be greater than 0. Permuting rows and columns results in a smaller $|a_{11}|$. Since $|a_{11}|$ can only shrink finitely many times, eventually we will get to a point where every a_{ij} is divisible by a_{11} . If a_{11} is negative, multiple the first row by -1 .

After performing the above operations, the first row and column of A are zero except for a_{11} which is positive and divides all other entries of A . We repeat the above steps for the matrix B obtained from A by deleting the first row and column. The upper left entry of the resulting matrix will be divisible by a_{11} , since every entry of B is. Repeating the argument inductively proves the proposition. \square

Example 1.1.9. The matrix $\begin{pmatrix} -2 & 2 \\ -3 & 4 \end{pmatrix}$ has Smith normal form $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$, and the

matrix $\begin{pmatrix} 1 & 4 & 9 \\ 16 & 25 & 36 \\ 49 & 64 & 81 \end{pmatrix}$ has Smith normal form $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 72 \end{pmatrix}$. As a double check, note that the determinants of a matrix and its Smith normal form match, up to sign. This is because

$$\det(PAQ) = \det(P) \det(A) \det(Q) = \pm \det(A).$$

We compute each of the above Smith forms using **Sage**, along with the corresponding transformation matrices. To do this we use the **Sage** command **matrix**, which takes as input the base ring, the number of rows, and the entries. The output of **matrix** is a matrix object which has the method **smith_form**.

First the 2×2 matrix.

```
A = matrix(ZZ, 2, [-2,2, -3,4])
S, P, Q = A.smith_form(); S
```

```
[1 0]
[0 2]
```

```
P*A*Q
```

```
[1 0]
[0 2]
```

```
P
```

```
[0 1]
[1 0]
```

```
Q
```

```
[1 -4]
[1 -3]
```

128 Next the 3×3 matrix.

```
A = matrix(ZZ, 3, [1,4,9, 16,25,36, 49,64,81])
S, P, Q = A.smith_form(); S
```

```
[ 1  0  0]
[ 0  3  0]
[ 0  0 72]
```

```
P*A*Q
```

```
[ 1  0  0]
[ 0  3  0]
[ 0  0 72]
```

```
P
```

```
[ 0  0  1]
[ 0  1 -1]
[ 1 -20 -17]
```

```
Q
```

```
[ 47  74  93]
[-79 -125 -156]
[ 34  54  67]
```

130

131 For one more example, we compute the Smith form of a 3×3 matrix of
 132 rank 2:

```
m = matrix(ZZ, 3, [2..10]); m
```

```
[ 2  3  4]
[ 5  6  7]
[ 8  9 10]
```

```
m.smith_form()[0]
```

```
[1 0 0]
[0 3 0]
[0 0 0]
```

134 *Proof of Theorem 1.1.2.* Suppose G is a finitely generated abelian group,
 135 which we may assume is nonzero. As in the paragraph before Proposi-
 136 tion 1.1.6, we use Corollary 1.1.5 to write G as the cokernel of an $n \times$
 137 m integer matrix A . By Proposition 1.1.6 there are isomorphisms $Q :$
 138 $\mathbb{Z}^m \rightarrow \mathbb{Z}^m$ and $P : \mathbb{Z}^n \rightarrow \mathbb{Z}^n$ such that $A' = PAQ$ has diagonal entries
 139 $n_1, n_2, \dots, n_s, 0, \dots, 0$, where $n_1 > 1$ and $n_1 \mid n_2 \mid \dots \mid n_s$. Then G is
 140 isomorphic to the cokernel of the diagonal matrix A' , so

$$G \cong (\mathbb{Z}/n_1\mathbb{Z}) \oplus (\mathbb{Z}/n_2\mathbb{Z}) \oplus \dots \oplus (\mathbb{Z}/n_s\mathbb{Z}) \oplus \mathbb{Z}^r, \quad (1.1)$$

141 as claimed. The n_i are determined by G , because n_i is the smallest positive
 142 integer n such that nG requires at most $s + r - i$ generators. We see from
 143 the representation (1.1) of G as a product that n_i has this property and that
 144 no smaller positive integer does. \square

145 **Exercise 1.1.10.** Recall Smith normal form defined in Proposition 1.1.6.
 146 With only minor modifications, then the proposition and proof will work
 147 over any principle ideal domain. Find and apply these modifications then

148 find the Smith normal form of the matrix $\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1+i & 2 \\ 0 & 1 & 5 \end{pmatrix}$.

149 [Hint: You can use Sage to verify your answer. However, you will need
 150 to make explicitly construct the Gaussian integers in order to input the
 151 matrix. You can do this by the following code.]

```
K.<i> = QuadraticField(-1)
R = K.maximal_order()
M = matrix(R, 3, [1,2,3,0,1+i,2,0,1,5]); show(M)
#show(M.smith_form()[0]) #uncomment for the answer
```

153 **Exercise 1.1.11.** Let $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$.

- 154 1. Find the Smith normal form of A .
- 155 2. Prove that the cokernel of the map $\mathbb{Z}^3 \rightarrow \mathbb{Z}^3$ given by multiplication
- 156 by A is isomorphic to $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}$.

157 1.2 Noetherian Rings and Modules

158 A module M over a commutative ring R with unit element is much like
 159 a vector space, but with more subtle structure. In this book, most of the
 160 modules we encounter will be noetherian, which is a generalization of the
 161 “finite dimensional” property of vector spaces. This section is about prop-
 162 erties of noetherian modules (and rings), which are crucial to much of this
 163 book. We thus give complete proofs of these properties, so you will have a
 164 solid foundation on which to learn algebraic number theory.

165 We first define noetherian rings and modules, then introduce several
 166 equivalent characterizations of them. We prove that when the base ring is
 167 noetherian, a module is finitely generated if and only if it is noetherian.
 168 Next we define short exact sequences, and prove that the middle module
 169 in a sequence is noetherian if and only if the first and last modules are
 170 noetherian. Finally, we prove the Hilbert basis theorem, which asserts that
 171 adjoining finitely many elements to a noetherian ring results in a noetherian
 172 ring.

173 Let R be a commutative ring with unity. An R -module is an additive
 174 abelian group M equipped with a map $R \times M \rightarrow M$ such that for all $r, r' \in R$
 175 and all $m, m' \in M$ we have $(rr')m = r(r'm)$, $(r + r')m = rm + r'm$,
 176 $r(m + m') = rm + rm'$, and $1m = m$. A *submodule* of M is a subgroup of
 177 M that is preserved by the action of R . For example, R is a module over
 178 itself, and any ideal I in R is an R -submodule of R .

179 *Example 1.2.1.* Abelian groups are the same as \mathbb{Z} -modules, and vector spaces
 180 over a field K are the same as K -modules.

181 An R -module M is finitely generated if there are elements $m_1, \dots, m_n \in$
 182 M such that every element of M is an R -linear combination of the m_i . The
 183 noetherian property is stronger than just being finitely generated:

184 **Definition 1.2.2** (Noetherian). An R -module M is *noetherian* if every sub-
 185 module of M is finitely generated. A ring R is *noetherian* if R is noetherian
 186 as a module over itself, i.e., if every ideal of R is finitely generated.

Any submodule M' of a noetherian module M is also noetherian. Indeed, if every submodule of M is finitely generated then so is every submodule of M' , since submodules of M' are also submodules of M .

Example 1.2.3. Let $R = M = \mathbb{Q}[x_1, x_2, \dots]$ be a polynomial ring over \mathbb{Q} in infinitely many indeterminants x_i . Then M is finitely generated as an R -module (!), since it is generated by 1. Consider the submodule $I = (x_1, x_2, \dots)$ of polynomials with 0 constant term, and suppose it is generated by polynomials f_1, \dots, f_n . Let x_i be an indeterminant that does not appear in any f_j , and suppose there are $h_k \in R$ such that $\sum_{k=1}^n h_k f_k = x_i$. Setting $x_i = 1$ and all other $x_j = 0$ on both sides of this equation and using that the f_k all vanish (they have 0 constant term), yields $0 = 1$, a contradiction. We conclude that the ideal I is not finitely generated, hence M is not a noetherian R -module, despite being finitely generated.

Definition 1.2.4 (Ascending chain condition). An R -module M satisfies the *ascending chain condition* if every sequence $M_1 \subset M_2 \subset M_3 \subset \dots$ of submodules of M eventually stabilizes, i.e., there is some n such that $M_n = M_{n+1} = M_{n+2} = \dots$.

We will use the notion of maximal element below. If \mathcal{X} is a set of subsets of a set S , ordered by inclusion, then a *maximal element* $A \in \mathcal{X}$ is a set such that no superset of A is contained in \mathcal{X} . Note that \mathcal{X} may contain many different maximal elements.

Proposition 1.2.5. *If M is an R -module, then the following are equivalent:*

1. M is noetherian,
2. M satisfies the ascending chain condition, and
3. Every nonempty set of submodules of M contains at least one maximal element.

Proof.

(1 \Rightarrow 2) : Suppose $M_1 \subset M_2 \subset \dots$ is a sequence of submodules of M . Then $M_\infty = \cup_{n=1}^\infty M_n$ is a submodule of M . Since M is noetherian and M_∞ is a submodule of M , there is a finite set a_1, \dots, a_m of generators for M_∞ . Each a_i must be contained in some M_j , so there is an n such that $a_1, \dots, a_m \in M_n$. But then $M_k = M_n$ for all $k \geq n$, which proves that the chain of M_i stabilizes, so the ascending chain condition holds for M .

221 (2 \Rightarrow 3) : Suppose 3 were false, so there exists a nonempty set S of submod-
 222 ules of M that does not contain a maximal element. We will use S
 223 to construct an infinite ascending chain of submodules of M that does
 224 not stabilize. Note that S is infinite, otherwise it would contain a
 225 maximal element. Let M_1 be any element of S . Then there is an M_2
 226 in S that strictly contains M_1 , otherwise S would contain the maximal
 227 element M_1 . Continuing inductively in this way we find an M_3 in S
 228 that properly contains M_2 , etc., and we produce an infinite ascend-
 229 ing chain of submodules of M , which contradicts the ascending chain
 230 condition.

231 (3 \Rightarrow 1) : Suppose 1 is false, so there is a submodule M' of M that is not
 232 finitely generated. We will show that the set S of all finitely generated
 233 submodules of M' does not have a maximal element, which will be a
 234 contradiction. Suppose S does have a maximal element L . Since L is
 235 finitely generated and $L \subset M'$, and M' is not finitely generated, there
 236 is an $a \in M'$ such that $a \notin L$. Then $L' = L + Ra$ is an element of S that
 237 strictly contains the presumed maximal element L , a contradiction.

238 □

Definition 1.2.6. A *homomorphism* of R -modules $\varphi : M \rightarrow N$ is an abelian group homomorphism such that for any $r \in R$ and $m \in M$ we have $\varphi(rm) = r\varphi(m)$. A sequence

$$L \xrightarrow{f} M \xrightarrow{g} N,$$

where f and g are homomorphisms of R -modules, is *exact* if $\text{im}(f) = \ker(g)$. A *short exact sequence* of R -modules is a sequence

$$0 \rightarrow L \xrightarrow{f} M \xrightarrow{g} N \rightarrow 0$$

239 that is exact at each point, i.e., f is injective, g is surjective, and $\text{im}(f) =$
 240 $\ker(g)$.

Example 1.2.7. The sequence

$$0 \rightarrow \mathbb{Z} \xrightarrow{2} \mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0$$

241 is an exact sequence, where the first map sends 1 to 2, and the second is the
 242 natural quotient map.

Lemma 1.2.8. *If*

$$0 \rightarrow L \xrightarrow{f} M \xrightarrow{g} N \rightarrow 0$$

243 *is a short exact sequence of R -modules, then M is noetherian if and only if*
 244 *both L and N are noetherian.*

245 *Proof.* First suppose that M is noetherian. Then L is a submodule of M ,
 246 so L is noetherian. Let N' be a submodule of N ; then the inverse image of
 247 N' in M is a submodule of M , so it is finitely generated, hence its image N'
 248 is also finitely generated. Thus N is noetherian as well.

249 Next assume nothing about M , but suppose that both L and N are
 250 noetherian. Suppose M' is a submodule of M ; then $M_0 = f(L) \cap M'$ is
 251 isomorphic to a submodule of the noetherian module L , so M_0 is generated
 252 by finitely many elements a_1, \dots, a_n . The quotient M'/M_0 is isomorphic
 253 (via g) to a submodule of the noetherian module N , so M'/M_0 is generated
 254 by finitely many elements b_1, \dots, b_m . For each $i \leq m$, let c_i be a lift of b_i to
 255 M' , modulo M_0 . Then the elements $a_1, \dots, a_n, c_1, \dots, c_m$ generate M' , for
 256 if $x \in M'$, then there is some element $y \in M_0$ such that $x - y$ is an R -linear
 257 combination of the c_i , and y is an R -linear combination of the a_i . \square

258 **Proposition 1.2.9.** *Suppose R is a noetherian ring. Then an R -module M*
 259 *is noetherian if and only if it is finitely generated.*

260 *Proof.* If M is noetherian then every submodule of M is finitely generated
 261 so M itself is finitely generated. Conversely, suppose M is finitely generated,
 262 say by elements a_1, \dots, a_n . Then there is a surjective homomorphism from
 263 $R^n = R \oplus \dots \oplus R$ to M that sends $(0, \dots, 0, 1, 0, \dots, 0)$ (1 in the i th factor)
 264 to a_i . Using Lemma 1.2.8 and exact sequences of R -modules such as $0 \rightarrow$
 265 $R \rightarrow R \oplus R \rightarrow R \rightarrow 0$, we see inductively that R^n is noetherian. Again by
 266 Lemma 1.2.8, homomorphic images of noetherian modules are noetherian,
 267 so M is noetherian. \square

268 **Lemma 1.2.10.** *Suppose $\varphi : R \rightarrow S$ is a surjective homomorphism of rings*
 269 *and R is noetherian. Then S is noetherian.*

Proof. The kernel of φ is an ideal I in R , and we have an exact sequence

$$0 \rightarrow I \rightarrow R \rightarrow S \rightarrow 0$$

270 with R noetherian. This is an exact sequence of R -modules, where S has
 271 the R -module structure induced from φ (if $r \in R$ and $s \in S$, then we define
 272 $rs = \varphi(r)s$). By Lemma 1.2.8, it follows that S is a noetherian R -modules.

Suppose J is an ideal of S . Since J is an R -submodule of S , if we view J as an R -module, then J is finitely generated. Since R acts on J through S , the R -generators of J are also S -generators of J , so J is finitely generated as an ideal. Thus S is noetherian. \square

Theorem 1.2.11 (Hilbert Basis Theorem). *If R is a noetherian ring and S is finitely generated as a ring over R , then S is noetherian. In particular, for any n the polynomial ring $R[x_1, \dots, x_n]$ and any of its quotients are noetherian.*

Proof. Assume first that we have already shown that for any n the polynomial ring $R[x_1, \dots, x_n]$ is noetherian. Suppose S is finitely generated as a ring over R , so there are generators s_1, \dots, s_n for S . Then the map $x_i \mapsto s_i$ extends uniquely to a surjective homomorphism $\pi : R[x_1, \dots, x_n] \twoheadrightarrow S$, and Lemma 1.2.10 implies that S is noetherian.

The rings $R[x_1, \dots, x_n]$ and $(R[x_1, \dots, x_{n-1}])[x_n]$ are isomorphic, so it suffices to prove that if R is noetherian then $R[x]$ is also noetherian. (Our proof follows [Art91, §12.5].) Thus suppose I is an ideal of $R[x]$ and that R is noetherian. We will show that I is finitely generated.

Let A be the set of leading coefficients of polynomials in I . (The leading coefficient of a polynomial is the coefficient of the highest degree monomial, or 0 if the polynomial is 0; thus $3x^7 + 5x^2 - 4$ has leading coefficient 3.) We will first show that A is an ideal of R . Suppose $a, b \in A$ are nonzero with $a + b \neq 0$. Then there are polynomials f and g in I with leading coefficients a and b . If $\deg(f) \leq \deg(g)$, then $a + b$ is the leading coefficient of $x^{\deg(g)-\deg(f)}f + g$, so $a + b \in A$; the argument when $\deg(f) > \deg(g)$ is analogous. Suppose $r \in R$ and $a \in A$ with $ra \neq 0$. Then ra is the leading coefficient of rf , so $ra \in A$. Thus A is an ideal in R .

Since R is noetherian and A is an ideal of R , there exist nonzero $a_1, \dots, a_n \in A$ that generate A as an ideal. Since A is the set of leading coefficients of elements of I , and the a_j are in A , we can choose for each $j \leq n$ an element $f_j \in I$ with leading coefficient a_j . By multiplying the f_j by some power of x , we may assume that the f_j all have the same degree $d \geq 1$.

Let $S_{<d}$ be the set of elements of I that have degree strictly less than d . This set is closed under addition and under multiplication by elements of R , so $S_{<d}$ is a module over R . The module $S_{<d}$ is the submodule of the R -module of polynomials of degree less than n , which is noetherian by Proposition 1.2.9 because it is generated by $1, x, \dots, x^{n-1}$. Thus $S_{<d}$ is finitely generated, and we may choose generators h_1, \dots, h_m for $S_{<d}$.

We finish by proving using induction on the degree that every $g \in I$ is an $R[x]$ -linear combination of $f_1, \dots, f_n, h_1, \dots, h_m$. If $g \in I$ has degree 0, then

312 $g \in S_{<d}$, since $d \geq 1$, so g is a linear combination of h_1, \dots, h_m . Next suppose
 313 $g \in I$ has degree e , and that we have proven the statement for all elements
 314 of I of degree $< e$. If $e \leq d$, then $g \in S_{<d}$, so g is in the $R[x]$ -ideal generated
 315 by h_1, \dots, h_m . Next suppose that $e \geq d$. Then the leading coefficient b
 316 of g lies in the ideal A of leading coefficients of elements of I , so there exist
 317 $r_i \in R$ such that $b = r_1 a_1 + \dots + r_n a_n$. Since f_i has leading coefficient a_i , the
 318 difference $g - x^{e-d} r_i f_i$ has degree less than the degree e of g . By induction
 319 $g - x^{e-d} r_i f_i$ is an $R[x]$ linear combination of $f_1, \dots, f_n, h_1, \dots, h_m$, so g is
 320 also an $R[x]$ linear combination of $f_1, \dots, f_n, h_1, \dots, h_m$. Since each f_i and
 321 h_j lies in I , it follows that I is generated by $f_1, \dots, f_n, h_1, \dots, h_m$, so I is
 322 finitely generated, as required. \square

323 1.2.1 The Ring \mathbb{Z} is Noetherian

324 The ring \mathbb{Z} is noetherian since every ideal of \mathbb{Z} is generated by one element.

325 **Proposition 1.2.12.** *Every ideal of the ring \mathbb{Z} is principal.*

326 *Proof.* Suppose I is a nonzero ideal in \mathbb{Z} . Let d be the least positive element
 327 of I . Suppose that $a \in I$ is any nonzero element of I . Using the division
 328 algorithm, we write $a = dq + r$, where q is an integer and $0 \leq r < d$. We have
 329 $r = a - dq \in I$ and $r < d$, so our assumption that d is minimal implies that
 330 $r = 0$, hence $a = dq$ is in the ideal generated by d . Thus I is the principal
 331 ideal generated by d . \square

332 *Example 1.2.13.* Let $I = (12, 18)$ be the ideal of \mathbb{Z} generated by 12 and 18.
 333 If $n = 12a + 18b \in I$, with $a, b \in \mathbb{Z}$, then $6 \mid n$, since $6 \mid 12$ and $6 \mid 18$. Also,
 334 $6 = 18 - 12 \in I$, so $I = (6)$.


335 The ring \mathbb{Z} in Sage is ZZ, which is Noetherian.

```
ZZ.is_noetherian()
```

336  True

337 We create the ideal I in Sage as follows, and note that it is principal:

```
I = ideal(12,18); I
```

 Principal ideal (6) of Integer Ring

338

I.is_principal()

 True

339 We could also create I as follows:

```
340      ZZ.ideal(12,18)
```

```
      Principal ideal (6) of Integer Ring
```

341 Propositions 1.2.9 and 1.2.12 together imply that any finitely generated
 342 abelian group is noetherian. This means that subgroups of finitely generated
 343 abelian groups are finitely generated, which provides the missing step in our
 344 proof of the structure theorem for finitely generated abelian groups.

345 **Exercise 1.2.14.** There is another way to show every principle ideal domain
 346 (for example \mathbb{Z}) is noetherian (contrast to the proof in Section 1.2.1). Let
 347 R be a PID and (a) an arbitrary ideal. Use the facts that $(b) \supseteq (a)$ if and
 348 only if $b \mid a$ and R is a UFD to show that ascending chain of ideals starting
 349 with (a) must stabilize.

350 1.3 Rings of Algebraic Integers

351 In this section we introduce the central objects of this book, which are the
 352 rings of algebraic integers. These are noetherian rings with an enormous
 353 amount of structure. We also introduce a function field analogue of these
 354 rings.

355 An *algebraic number* is a root of some nonzero polynomial $f(x) \in \mathbb{Q}[x]$.
 356 For example, $\sqrt{2}$ and $\sqrt{5}$ are both algebraic numbers, being roots of $x^2 - 2$
 357 and $x^2 - 5$, respectively. But is $\sqrt{2} + \sqrt{5}$ necessarily the root of some
 358 polynomial in $\mathbb{Q}[x]$? This isn't quite so obvious.

359 **Proposition 1.3.1.** *An element α of a field extension of \mathbb{Q} is an algebraic*
 360 *number if and only if the ring $\mathbb{Q}[\alpha]$ generated by α is finite dimensional as*
 361 *a \mathbb{Q} vector space.*

362 *Proof.* Suppose α is an algebraic number, so there is a nonzero polynomial
 363 $f(x) \in \mathbb{Q}[x]$, so that $f(\alpha) = 0$. The equation $f(\alpha) = 0$ implies that $\alpha^{\deg(f)}$
 364 can be written in terms of smaller powers of α , so $\mathbb{Q}[\alpha]$ is spanned by the
 365 finitely many numbers $1, \alpha, \dots, \alpha^{\deg(f)-1}$, hence finite dimensional. Con-
 366 versely, suppose $\mathbb{Q}[\alpha]$ is finite dimensional. Then for some $n \geq 1$, we have
 367 that α^n is in the \mathbb{Q} -vector space spanned by $1, \alpha, \dots, \alpha^{n-1}$. Thus α satisfies
 368 a polynomial $f(x) \in \mathbb{Q}[x]$ of degree n . \square

369 **Proposition 1.3.2.** *Suppose K is a field and $\alpha, \beta \in K$ are two algebraic*
 370 *numbers. Then $\alpha\beta$ and $\alpha + \beta$ are also algebraic numbers.*

371 *Proof.* Let $n = \dim_{\mathbb{Q}} \mathbb{Q}[\alpha]$ and $n = \dim_{\mathbb{Q}} \mathbb{Q}[\beta]$. The subring $\mathbb{Q}[\alpha, \beta] \subset K$ is
 372 a \mathbb{Q} -vector space that is spanned by the numbers $\alpha^i \beta^j$, where $0 \leq i < n$ and
 373 $0 \leq j < m$. Thus $\mathbb{Q}[\alpha, \beta]$ is finite dimensional, and since $\alpha + \beta$ and $\alpha\beta$ are
 374 both in $\mathbb{Q}[\alpha, \beta]$, we conclude by Proposition 1.3.1 that both are algebraic
 375 numbers. \square

376 Suppose C is a field extension of \mathbb{Q} such that every polynomial $f(x) \in$
 377 $\mathbb{Q}[x]$ factors completely in C . The algebraic closure $\overline{\mathbb{Q}}$ of \mathbb{Q} inside C is the
 378 field generated by all roots in C of polynomials in $\mathbb{Q}[x]$. The fundamental
 379 theorem of algebra tells us that $C = \mathbb{C}$ is one choice of field C as above.
 380 There are other fields C , e.g., constructed using p -adic numbers. One can
 381 show that any two choices of $\overline{\mathbb{Q}}$ are isomorphic; however, there will be *many*
 382 isomorphisms between them.

383 **Definition 1.3.3** (Algebraic Integer). An element $\alpha \in \overline{\mathbb{Q}}$ is an *algebraic*
 384 *integer* if it is a root of some monic polynomial with coefficients in \mathbb{Z} .

385 For example, $\sqrt{2}$ is an algebraic integer, since it is a root of the monic
 386 integral polynomial $x^2 - 2$. As we will see below, $1/2$ is not an algebraic
 387 integer.

388 The following two propositions are analogous to Propositions 1.3.1–1.3.2
 389 above, with the proofs replacing basic facts about vector spaces with facts
 390 we proved above about noetherian rings and modules.

391 **Proposition 1.3.4.** *An element $\alpha \in \overline{\mathbb{Q}}$ is an algebraic integer if and only*
 392 *if $\mathbb{Z}[\alpha]$ is finitely generated as a \mathbb{Z} -module.*

393 *Proof.* Suppose α is integral and let $f \in \mathbb{Z}[x]$ be a monic integral poly-
 394 nomial such that $f(\alpha) = 0$. Then, as a \mathbb{Z} -module, $\mathbb{Z}[\alpha]$ is generated by
 395 $1, \alpha, \alpha^2, \dots, \alpha^{d-1}$, where d is the degree of f . Conversely, suppose $\alpha \in \overline{\mathbb{Q}}$
 396 is such that $\mathbb{Z}[\alpha]$ is finitely generated as a module over \mathbb{Z} , say by elements
 397 $f_1(\alpha), \dots, f_n(\alpha)$. Let d be any integer bigger than the degrees of all f_i .
 398 Then there exist integers a_i such that $\alpha^d = \sum_{i=1}^n a_i f_i(\alpha)$, hence α satis-
 399 fies the monic polynomial $x^d - \sum_{i=1}^n a_i f_i(x) \in \mathbb{Z}[x]$, so α is an algebraic
 400 integer. \square

401 The proof of the following proposition uses repeatedly that any submod-
 402 ule of a finitely generated \mathbb{Z} -module is finitely generated, which uses that \mathbb{Z}
 403 is noetherian and that finitely generated modules over a noetherian ring are
 404 noetherian.

405 **Proposition 1.3.5.** *Suppose K is a field and $\alpha, \beta \in K$ are two algebraic*
 406 *integers. Then $\alpha\beta$ and $\alpha + \beta$ are also algebraic integers.*

407 *Proof.* Let m, n be the degrees of monic integral polynomials that have α, β
 408 as roots, respectively. Then we can write α^m in terms of smaller powers of
 409 α and likewise for β^n , so the elements $\alpha^i \beta^j$ for $0 \leq i < m$ and $0 \leq j < n$
 410 span the \mathbb{Z} -module $\mathbb{Z}[\alpha, \beta]$. Since $\mathbb{Z}[\alpha + \beta]$ is a submodule of the finitely-
 411 generated \mathbb{Z} -module $\mathbb{Z}[\alpha, \beta]$, it is finitely generated, so $\alpha + \beta$ is integral.
 412 Likewise, $\mathbb{Z}[\alpha\beta]$ is a submodule of $\mathbb{Z}[\alpha, \beta]$, so it is also finitely generated,
 413 and $\alpha\beta$ is integral. \square

414 1.3.1 Minimal Polynomials

415 **Definition 1.3.6** (Minimal Polynomial). The *minimal polynomial* of $\alpha \in \overline{\mathbb{Q}}$
 416 is the monic polynomial $f \in \mathbb{Q}[x]$ of least positive degree such that $f(\alpha) = 0$.

417 It is a consequence of Lemma 1.3.9 below that “the” minimal polynomial
 418 of α is unique. The minimal polynomial of $1/2$ is $x - 1/2$, and the minimal
 419 polynomial of $\sqrt[3]{2}$ is $x^3 - 2$.

420 *Example 1.3.7.* We compute the minimal polynomial of a number expressed
 421 in terms of $\sqrt[4]{2}$:

```

422 k.<a> = NumberField(x^4 - 2)
      a^4

      2

      (a^2 + 3).minpoly()

      x^2 - 6*x + 7
```

423 **Exercise 1.3.8.** Find the minimal polynomial of $\sqrt{2} + \sqrt{3}$ by hand. Check
 424 your result with **Sage**.

425 **Lemma 1.3.9.** Suppose $\alpha \in \overline{\mathbb{Q}}$. Then the minimal polynomial of α divides
 426 any polynomial h such that $h(\alpha) = 0$.

Proof. Let f be a choice of minimal polynomial of α , as in Definition 1.3.6,
 and let h be a polynomial with $h(\alpha) = 0$. Use the division algorithm to
 write $h = qf + r$, where $0 \leq \deg(r) < \deg(f)$. We have

$$r(\alpha) = h(\alpha) - q(\alpha)f(\alpha) = 0,$$

427 so α is a root of r . However, f is a polynomial of least positive degree with
 428 root α , so $r = 0$. \square

429 **Exercise 1.3.10.** Show that the minimal polynomial of an algebraic number
 430 $\alpha \in \overline{\mathbb{Q}}$ is unique.

431 **Lemma 1.3.11.** Suppose $\alpha \in \overline{\mathbb{Q}}$. Then α is an algebraic integer if and only
 432 if the minimal polynomial f of α has coefficients in \mathbb{Z} .

433 *Proof.* First suppose that the minimal polynomial f of α has coefficients in
 434 \mathbb{Z} . Since $f \in \mathbb{Z}[x]$ is monic (by definition) and $f(\alpha) = 0$, we see immediately
 435 that α is an algebraic integer.

436 Now suppose that α is an algebraic integer. Then there is some nonzero
 437 monic $g \in \mathbb{Z}[x]$ such that $g(\alpha) = 0$. By Lemma 1.3.9, we have $g = fh$,
 438 for some $h \in \mathbb{Q}[x]$, and h is monic because f and g are. If $f \notin \mathbb{Z}[x]$, then
 439 some prime p divides the denominator of some coefficient of f . Let p^i be
 440 the largest power of p that divides some denominator of some coefficient f ,
 441 and likewise let p^j be the largest power of p that divides some denominator
 442 of a coefficient of h . Then $p^{i+j}g = (p^i f)(p^j h)$, and if we reduce both sides
 443 modulo p , then the left hand side is 0 but the right hand side is a product
 444 of two nonzero polynomials in $\mathbb{F}_p[x]$, hence nonzero, a contradiction. \square

445 **Exercise 1.3.12.** Which of the following numbers are algebraic integers?

- 446 (a) The number $(1 + \sqrt{5})/2$.
 447 (b) The number $(2 + \sqrt{5})/2$.
 448 (c) The value of the infinite sum $\sum_{n=1}^{\infty} 1/n^2$.
 449 (d) The number $\alpha/3$, where α is a root of $x^4 + 54x + 243$.

450 *Example 1.3.13.* We compute some minimal polynomials in **Sage**. The min-
 451 imal polynomial of $1/2$:

```
(1/2).minpoly()
```

```
| x - 1/2
```

We construct a root a of $x^2 - 2$ and compute its minimal polynomial:

```
452 k.<a> = NumberField(x^2 - 2)
a^2 - 2
```

```
| 0
```

```
a.minpoly()
```

```
| x^2 - 2
```

453 Finally we compute the minimal polynomial of $\alpha = \sqrt{2}/2 + 3$, which is not
 454 integral, hence Proposition 1.3.4 implies that α is not an algebraic integer:

```
(a/2 + 3).minpoly()
```

455

```
| x^2 - 6*x + 17/2
```

The only elements of \mathbb{Q} that are algebraic integers are the usual integers \mathbb{Z} , since $\mathbb{Z}[1/d]$ is not finitely generated as a \mathbb{Z} -module. Watch out since there are elements of \mathbb{Q} that seem to *appear* to have denominators when written down, but are still algebraic integers. This is an artifact of how we write them down, e.g., if we wrote our integers as a multiple of $\alpha = 2$, then we would write 1 as $\alpha/2$. For example,

$$\alpha = \frac{1 + \sqrt{5}}{2}$$

456 is an algebraic integer, since it is a root of the monic integral polynomial
 457 $x^2 - x - 1$. We verify this using **Sage** below, though of course this is easy
 458 to do by hand (you should try much more complicated examples in **Sage**).

```
k.<a> = QuadraticField(5)
a^2
```

```
| 5
```

```
alpha = (1 + a)/2
alpha.minpoly()
```

459

```
| x^2 - x - 1
```

```
alpha.is_integral()
```

```
| True
```

460 Since $\sqrt{5}$ can be expressed in terms of radicals, we can also compute this
 461 minimal polynomial using the symbolic functionality in Sage.

```
alpha = (1+sqrt(5))/2
alpha.minpoly()
```

```
| x^2 - x - 1
```

462 Here is a more complicated example using a similar approach:

```
alpha = sqrt(2) + 3^(1/4)
alpha.minpoly()
```

```
| x^8 - 8*x^6 + 18*x^4 - 104*x^2 + 1
```

463 *Example 1.3.14.* We illustrate an example of a sum and product of two
 464 algebraic integers being an algebraic integer. We first make the relative
 465 number field obtained by adjoining a root of $x^3 - 5$ to the field $\mathbb{Q}(\sqrt{2})$:

```
k.<a, b> = NumberField([x^2 - 2, x^3 - 5])
k
```

466

```
| Number Field in a with defining polynomial x^2 + -2 over its base field
```

467 Here a and b are roots of $x^2 - 2$ and $x^3 - 5$, respectively.

```
a^2
```

```
| 2
```

468

```
b^3
```

```
| 5
```

469 We compute the minimal polynomial of the sum and product of $\sqrt[3]{5}$ and
 470 $\sqrt{2}$. The command `absolute_minpoly` gives the minimal polynomial of the
 471 element over the rational numbers \mathbb{Q} .

```
(a+b).absolute_minpoly()
```

```
| x^6 - 6*x^4 - 10*x^3 + 12*x^2 - 60*x + 17
```

472

```
(a*b).absolute_minpoly()
```

```
| x^6 - 200
```

The minimal polynomial of the product is $\sqrt[3]{5}\sqrt{2}$ is trivial to compute by hand. In light of the Cayley-Hamilton theorem, we can compute the minimal polynomial of $\alpha = \sqrt[3]{5} + \sqrt{2}$ by hand by computing the determinant of the matrix given by left multiplication by α on the basis

$$1, \sqrt{2}, \sqrt[3]{5}, \sqrt[3]{5}\sqrt{2}, \sqrt[3]{5}^2, \sqrt[3]{5}^2\sqrt{2}.$$

473 This is a general method which works well for computers. However it can
474 also be done using simple algebra.

475 *Exercise 1.3.15.* Compute the minimal polynomial of $\alpha = \sqrt[3]{5} + \sqrt{2}$ by hand
476 without finding the determinate of a 6×6 matrix.

477 [*Hint:* Let $a^2 = 2$, $b^3 = 5$, and $x = a + b$. Then $(x - a)^3 = b^3 = 5$. Now
478 simplify and use the fact that $a^2 = 2$.]

479 The following is an alternative, more symbolic way to compute the min-
480 imal polynomials above, though it is not provably correct. We compute α
481 to 100 bits precision (via the `n` command), then use the LLL algorithm (via
482 the `algdep` command) to heuristically find a linear relation between the first
483 6 powers of α (see Section 1.5 below for more about LLL).

```

a = 5^(1/3); b = sqrt(2)
c = a+b; c

| 5^(1/3) + sqrt(2)

(a+b).n(100).algdep(6)

484 | x^6 - 6*x^4 - 10*x^3 + 12*x^2 - 60*x + 17

(a*b).n(100).algdep(6)

| x^6 - 200
```

485 **Exercise 1.3.16.** Let $\alpha = \sqrt{2} + \frac{1+\sqrt{5}}{2}$.

486 (a) Is α an algebraic integer?

487 (b) Explicitly write down the minimal polynomial of α as an element of
488 $\mathbb{Q}[x]$.

1.3.2 Number fields, rings of integers, and orders

Definition 1.3.17 (Number field). A *number field* is a field K that contains the rational numbers \mathbb{Q} such that the degree $[K : \mathbb{Q}] = \dim_{\mathbb{Q}}(K)$ is finite.

If K is a number field, then by the primitive element theorem there is an $\alpha \in K$ so that $K = \mathbb{Q}(\alpha)$. Let $f(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α . Fix a choice of algebraic closure $\overline{\mathbb{Q}}$ of \mathbb{Q} . Associated to each of the $\deg(f)$ roots $\alpha' \in \overline{\mathbb{Q}}$ of f , we obtain a field embedding $K \hookrightarrow \overline{\mathbb{Q}}$ that sends α to α' . Thus any number field can be embedded in $[K : \mathbb{Q}] = \deg(f)$ distinct ways in $\overline{\mathbb{Q}}$.

Definition 1.3.18 (Ring of Integers). The *ring of integers* of a number field K is the ring

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

One of the most basic facts about \mathcal{O}_K is that it is indeed a ring. This fact is important enough to be stated as a separate theorem.

Theorem 1.3.19. *Let K be a number field. The ring of integers \mathcal{O}_K is a ring.*

Proof. This follows directly from Proposition 1.3.5. □

Example 1.3.20. The field \mathbb{Q} of rational numbers is a number field of degree 1, and the ring of integers of \mathbb{Q} is \mathbb{Z} . The field $K = \mathbb{Q}(i)$ of Gaussian integers has degree 2 and $\mathcal{O}_K = \mathbb{Z}[i]$.

Example 1.3.21. The golden ratio $\varphi = (1 + \sqrt{5})/2$ is in the quadratic number field $K = \mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\varphi)$; notice that φ satisfies $x^2 - x - 1$, so $\varphi \in \mathcal{O}_K$. To see that $\mathcal{O}_K = \mathbb{Z}[\varphi]$ directly, we proceed as follows. By Proposition 1.3.4, the algebraic integers K are exactly the elements $a + b\sqrt{5} \in K$, with $a, b \in \mathbb{Q}$ that have integral minimal polynomial. The matrix of $a + b\sqrt{5}$ with respect to the basis $1, \sqrt{5}$ for K is $m = \begin{pmatrix} a & 5b \\ b & a \end{pmatrix}$. The characteristic polynomial of m is $f = (x - a)^2 - 5b^2 = x^2 - 2ax + a^2 - 5b^2$, which is in $\mathbb{Z}[x]$ if and only if $2a \in \mathbb{Z}$ and $a^2 - 5b^2 \in \mathbb{Z}$. Thus $a = a'/2$ with $a' \in \mathbb{Z}$, and $(a'/2)^2 - 5b^2 \in \mathbb{Z}$, so $5b^2 \in \frac{1}{4}\mathbb{Z}$, so $b \in \frac{1}{2}\mathbb{Z}$ as well. If a has a denominator of 2, then b must also have a denominator of 2 to ensure that the difference $a^2 - 5b^2$ is an integer. This proves that $\mathcal{O}_K = \mathbb{Z}[\varphi]$.

Example 1.3.22. The ring of integers of $K = \mathbb{Q}(\sqrt[3]{9})$ is $\mathbb{Z}[\sqrt[3]{3}]$, where $\sqrt[3]{3} = \frac{1}{3}(\sqrt[3]{9})^2 \notin \mathbb{Z}[\sqrt[3]{9}]$. As we will see, in general the problem of computing \mathcal{O}_K given K may be very hard, since it requires factoring a certain potentially large integer.

521 **Exercise 1.3.23.** From basic definitions, find the rings of integers of the
 522 fields $\mathbb{Q}(\sqrt{11})$ and $\mathbb{Q}(\sqrt{-6})$.

523 **Definition 1.3.24** (Order). An *order* in \mathcal{O}_K is any subring R of \mathcal{O}_K such
 524 that the quotient \mathcal{O}_K/R of abelian groups is finite. (By definition R must
 525 contain 1 because it is a ring.)

526 **Exercise 1.3.25.** Let R be a subring of \mathcal{O}_K . Show that R is an order of
 527 \mathcal{O}_K if and only if R contains a spanning set for K as a vector space over \mathbb{Q} .

528 As noted above, $\mathbb{Z}[i]$ is the ring of integers of $\mathbb{Q}(i)$. For every nonzero
 529 integer n , the subring $\mathbb{Z} + ni\mathbb{Z}$ of $\mathbb{Z}[i]$ is an order. The subring \mathbb{Z} of $\mathbb{Z}[i]$ is not
 530 an order, because \mathbb{Z} does not have finite index in $\mathbb{Z}[i]$. Also the subgroup
 531 $2\mathbb{Z} + i\mathbb{Z}$ of $\mathbb{Z}[i]$ is not an order because it is not a ring.

532 **Exercise 1.3.26.** Let K be a quadratic extension of \mathbb{Q} and R be any order
 533 in \mathcal{O}_K . Show that \mathcal{O}_K/R is cyclic as an abelian group and that there is a
 534 bijection between orders of \mathcal{O}_K containing R and divisors of $[\mathcal{O}_K : R]$.

535 *Remark 1.3.27.* Exercise 1.3.26 is used in elliptic curve cryptography to
 536 measure the number of isogenies; for example, see [KKM11, §11.2].

537 We define the number field $\mathbb{Q}(i)$ and compute its ring of integers.

```

538 K.<i> = NumberField(x^2 + 1)
      OK = K.ring_of_integers(); OK

      Order with module basis 1, i in Number Field in i with
      defining polynomial x^2 + 1

```

539 Next we compute the order $\mathbb{Z} + 3i\mathbb{Z}$.

```

      O3 = K.order(3*i); O3

      Order with module basis 1, 3*i in Number Field in i with
      defining polynomial x^2 + 1

540 O3.gens()

      [1, 3*i]

```

541 We test whether certain elements are in the order.

```
5 + 9*i in O3
```

```
| True
```

542

```
1 + 2*i in O3
```

```
| False
```

543 We will frequently consider orders because they are often much easier
 544 to write down explicitly than \mathcal{O}_K . For example, if $K = \mathbb{Q}(\alpha)$ and α is an
 545 algebraic integer, then $\mathbb{Z}[\alpha]$ is an order in \mathcal{O}_K , but frequently $\mathbb{Z}[\alpha] \neq \mathcal{O}_K$.
 546 *Example 1.3.28.* In this example $[\mathcal{O}_K : \mathbb{Z}[a]] = 2197$. First we define the
 547 number field $K = \mathbb{Q}(a)$ where a is a root of $x^3 - 15x^2 - 94x - 3674$, then
 548 we compute the order $\mathbb{Z}[a]$ generated by a .

```
K.<a> = NumberField(x^3 - 15*x^2 - 94*x - 3674)
Oa = K.order(a); Oa
```

```
549 | Order with module basis 1, a, a^2 in Number Field in a with defining
    | polynomial x^3 - 15*x^2 - 94*x - 3674
```

```
Oa.basis()
```

```
| [1, a, a^2]
```

550 Next we compute a \mathbb{Z} -basis for the maximal order \mathcal{O}_K of K , and compute
 551 that the index of $\mathbb{Z}[a]$ in \mathcal{O}_K is $2197 = 13^3$.

```
OK = K.maximal_order()
OK.basis()
```

```
552 | [25/169*a^2 + 10/169*a + 1/169, 5/13*a^2 + 1/13*a, a^2]
```

```
Oa.index_in(OK)
```

```
| 2197
```

553 **Lemma 1.3.29.** *Let \mathcal{O}_K be the ring of integers of a number field. Then*
 554 *$\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$ and $\mathbb{Q}\mathcal{O}_K = K$.*

555 *Proof.* Suppose $\alpha \in \mathcal{O}_K \cap \mathbb{Q}$ with $\alpha = a/b \in \mathbb{Q}$ in lowest terms and $b > 0$.
 556 Since α is integral, $\mathbb{Z}[a/b]$ is finitely generated as a module, so $b = 1$.

557 To prove that $\mathbb{Q}\mathcal{O}_K = K$, suppose $\alpha \in K$, and let $f(x) \in \mathbb{Q}[x]$ be the
 558 minimal monic polynomial of α . For any positive integer d , the minimal

monic polynomial of $d\alpha$ is $d^{\deg(f)}f(x/d)$, i.e., the polynomial obtained from $f(x)$ by multiplying the coefficient of $x^{\deg(f)}$ by 1, multiplying the coefficient of $x^{\deg(f)-1}$ by d , multiplying the coefficient of $x^{\deg(f)-2}$ by d^2 , etc. If d is the least common multiple of the denominators of the coefficients of f , then the minimal monic polynomial of $d\alpha$ has integer coefficients, so $d\alpha$ is integral and $d\alpha \in \mathcal{O}_K$. This proves that $\mathbb{Q}\mathcal{O}_K = K$. \square

Exercise 1.3.30. Which of the following rings are orders in the given number field, i.e. orders in the ring of integers of the given number field.

- (a) The ring $R = \mathbb{Z}[i]$ in the number field $\mathbb{Q}(i)$.
- (b) The ring $R = \mathbb{Z}[i/2]$ in the number field $\mathbb{Q}(i)$.
- (c) The ring $R = \mathbb{Z}[17i]$ in the number field $\mathbb{Q}(i)$.
- (d) The ring $R = \mathbb{Z}[i]$ in the number field $\mathbb{Q}(\sqrt[4]{-1})$.

Exercise 1.3.31. Find the ring of integers of $\mathbb{Q}(a)$, where $a^5 + 7a + 1 = 0$ using a computer.

1.3.3 Function fields

Let k be any field. We can also make the same definitions, but with \mathbb{Q} replaced by the field $k(t)$ of rational functions in an indeterminate t , and \mathbb{Z} replaced by $k[t]$. The analogue of a number field is called a *function field*; it is a finite algebraic extension field K of $k(t)$. Elements of K have a unique minimal polynomial as above, and the ring of integers of K consists of those elements whose monic minimal polynomial has coefficients in the polynomial ring $k[t]$.

Geometrically, if $F(x, t) = 0$ is an affine equation that defines (via projective closure) a nonsingular projective curve C , then $K = k(t)[x]/(F(x, t))$ is a function field. We view the field K as the field of all rational functions on the projective closure of the curve C . The ring of integers \mathcal{O}_K is the subring of rational functions that have no poles on the affine curve $F(x, t) = 0$, though they may have poles at infinity, i.e., at the extra points we introduce when passing to the projective closure C . The algebraic arguments we gave above prove that \mathcal{O}_K is a ring. This is also geometrically intuitive, since the sum and product of two functions with no poles also have no poles.

Exercise 1.3.32. Let $k = \mathbb{F}_p$ be the finite field with p elements where p is some prime. Find all automorphisms of $k(t)$. Note that an automorphism is

completely characterized by its value on t . How many such automorphisms are there?

[*Hint:* For some people, it is easier to think about the equivalent question: What rational functions $f \in k(t)$ is the map $k(t) \rightarrow k(t)$ given by $t \mapsto f(t)$ an automorphism?]

1.4 Norms and Traces

In this section we develop some basic properties of norms, traces, and discriminants, and give more properties of rings of integers in the general context of Dedekind domains.

Before discussing norms and traces we introduce some notation for field extensions. If $K \subset L$ are number fields, we let $[L : K]$ denote the dimension of L viewed as a K -vector space. If K is a number field and $a \in \overline{\mathbb{Q}}$, let $K(a)$ be the extension of K generated by a , which is the smallest number field that contains both K and a . If $a \in \overline{\mathbb{Q}}$ then a has a minimal polynomial $f(x) \in \mathbb{Q}[x]$, and the *Galois conjugates* of a are the roots of f . These are called the Galois conjugates because they are the orbit of a under the action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Example 1.4.1. The element $\sqrt{2}$ has minimal polynomial $x^2 - 2$ and the Galois conjugates of $\sqrt{2}$ are $\sqrt{2}$ and $-\sqrt{2}$. The cube root $\sqrt[3]{2}$ has minimal polynomial $x^3 - 2$ and three Galois conjugates $\sqrt[3]{2}, \zeta_3 \sqrt[3]{2}, \zeta_3^2 \sqrt[3]{2}$, where ζ_3 is a cube root of unity.

We create the extension $\mathbb{Q}(\zeta_3)(\sqrt[3]{2})$ in Sage.

```
L.< cuberoot2 > = CyclotomicField(3).extension(x^3 - 2)
cuberoot2^3
```

614

```
| 2
```

Then we list the Galois conjugates of $\sqrt[3]{2}$.

```
cuberoot2.galois_conjugates(L)

| [cuberoot2, (-zeta3 - 1)*cuberoot2, zeta3*cuberoot2]
```

616

Note that $\zeta_3^2 = -\zeta_3 - 1$:

```
zeta3 = L.base_field().0
zeta3^2
```

618

```
| -zeta3 - 1
```

619 Suppose $K \subset L$ is an inclusion of number fields and let $a \in L$. Then
 620 left multiplication by a defines a K -linear transformation $\ell_a : L \rightarrow L$. (The
 621 transformation ℓ_a is K -linear because L is commutative.)

Definition 1.4.2 (Norm and Trace). The *norm* and *trace* of a from L to K are

$$\text{Norm}_{L/K}(a) = \det(\ell_a) \quad \text{and} \quad \text{Trace}_{L/K}(a) = \text{Trace}(\ell_a).$$

We know from linear algebra that determinants are multiplicative and traces are additive, so for $a, b \in L$ we have

$$\text{Norm}_{L/K}(ab) = \text{Norm}_{L/K}(a) \cdot \text{Norm}_{L/K}(b)$$

and

$$\text{Trace}_{L/K}(a + b) = \text{Trace}_{L/K}(a) + \text{Trace}_{L/K}(b).$$

622 Note that if $f \in \mathbb{Q}[x]$ is the characteristic polynomial of ℓ_a , then the
 623 constant term of f is $(-1)^{\deg(f)} \det(\ell_a)$, and the coefficient of $x^{\deg(f)-1}$ is
 624 $-\text{Trace}(\ell_a)$.

Proposition 1.4.3. Let $a \in L$ and let $\sigma_1, \dots, \sigma_d$, where $d = [L : K]$, be the distinct field embeddings $L \hookrightarrow \overline{\mathbb{Q}}$ that fix every element of K . Then

$$\text{Norm}_{L/K}(a) = \prod_{i=1}^d \sigma_i(a) \quad \text{and} \quad \text{Trace}_{L/K}(a) = \sum_{i=1}^d \sigma_i(a).$$

625 *Proof.* We prove the proposition by computing the characteristic polynomial
 626 of a . Let $f \in K[x]$ be the minimal polynomial of a over K , and note that f
 627 has distinct roots and is irreducible, since it is the polynomial in $K[x]$ of
 628 least degree that is satisfied by a and K has characteristic 0. Since f is
 629 irreducible, we have $K(a) \cong K[x]/(f)$, so $[K(a) : K] = \deg(f)$. Also a
 630 satisfies a polynomial if and only if ℓ_a does, so the characteristic polynomial
 631 of ℓ_a acting on $K(a)$ is f . Let b_1, \dots, b_n be a basis for L over $K(a)$ and
 632 note that $1, \dots, a^m$ is a basis for $K(a)/K$, where $m = \deg(f) - 1$. Then
 633 $a^i b_j$ is a basis for L over K , and left multiplication by a acts the same way
 634 on the span of $b_j, ab_j, \dots, a^m b_j$ as on the span of $b_k, ab_k, \dots, a^m b_k$, for any
 635 pair $j, k \leq n$. Thus the matrix of ℓ_a on L is a block direct sum of copies
 636 of the matrix of ℓ_a acting on $K(a)$, so the characteristic polynomial of ℓ_a
 637 on L is $f^{[L:K(a)]}$. The proposition follows because the roots of $f^{[L:K(a)]}$ are
 638 exactly the images $\sigma_i(a)$, with multiplicity $[L : K(a)]$, since each embedding
 639 of $K(a)$ into $\overline{\mathbb{Q}}$ extends in exactly $[L : K(a)]$ ways to L . \square

640 **Warning 1.4.4.** It is important in Proposition 1.4.3 that the product and
 641 sum be over *all* the images $\sigma_i(a)$, not over just the distinct images. For
 642 example, if $a = 1 \in L$, then $\text{Trace}_{L/K}(a) = [L : K]$, whereas the sum of the
 643 distinct conjugates of a is 1.

644 *Remark 1.4.5.* Let $K \subset L$ be an extension of number fields. If $\alpha \in \mathcal{O}_L$, then
 645 the formula of Proposition 1.4.3 implies that the norm and trace down to K
 646 of α is an element of \mathcal{O}_K , because the sum and product of algebraic integers
 647 is an algebraic integer.

648 The following corollary asserts that the norm and trace behave well in
 649 towers.

Corollary 1.4.6. *Suppose $K \subset L \subset M$ is a tower of number fields, and let $a \in M$. Then*

$$\text{Norm}_{M/K}(a) = \text{Norm}_{L/K}(\text{Norm}_{M/L}(a)) \quad \text{and} \quad \text{Trace}_{M/K}(a) = \text{Trace}_{L/K}(\text{Trace}_{M/L}(a)).$$

650 *Proof.* The proof uses that every embedding $L \hookrightarrow \overline{\mathbb{Q}}$ extends in exactly
 651 $[M : L]$ way to an embedding $M \hookrightarrow \overline{\mathbb{Q}}$. This is clear if we view M as
 652 $L[x]/(h(x))$ for some irreducible polynomial $h(x) \in L[x]$ of degree $[M : L]$,
 653 and note that the extensions of $L \hookrightarrow \overline{\mathbb{Q}}$ to M correspond to the roots of h ,
 654 of which there are $\deg(h)$, since $\overline{\mathbb{Q}}$ is algebraically closed.

655 For the first equation, both sides are the product of $\sigma_i(a)$, where σ_i
 656 runs through the embeddings of M into $\overline{\mathbb{Q}}$ that fix K . To see this, suppose
 657 $\sigma : L \rightarrow \overline{\mathbb{Q}}$ fixes K . If σ' is an extension of σ to M , and τ_1, \dots, τ_d are
 658 the embeddings of M into $\overline{\mathbb{Q}}$ that fix L , then $\sigma'\tau_1, \dots, \sigma'\tau_d$ are exactly the
 659 extensions of σ to M . For the second statement, both sides are the sum of
 660 the $\sigma_i(a)$. \square

661 **Proposition 1.4.7.** *Let K be a number field. The ring of integers \mathcal{O}_K is a*
 662 *lattice in K , i.e., $\mathbb{Q}\mathcal{O}_K = K$ and \mathcal{O}_K is an abelian group of rank $[K : \mathbb{Q}]$.*

Proof. We saw in Lemma 1.3.29 that $\mathbb{Q}\mathcal{O}_K = K$. Thus there exists a basis
 a_1, \dots, a_n for K , where each a_i is in \mathcal{O}_K . Suppose that as $x = \sum_{i=1}^n c_i a_i \in$
 \mathcal{O}_K varies over all elements of \mathcal{O}_K the denominators of the coefficients c_i
 are not all uniformly bounded. Then subtracting off integer multiples of the
 a_i , we see that as $x = \sum_{i=1}^n c_i a_i \in \mathcal{O}_K$ varies over elements of \mathcal{O}_K with c_i
 between 0 and 1, the denominators of the c_i are also arbitrarily large. This
 implies that there are infinitely many elements of \mathcal{O}_K in the bounded subset

$$S = \{c_1 a_1 + \dots + c_n a_n : c_i \in \mathbb{Q}, 0 \leq c_i \leq 1\} \subset K.$$

Thus for any $\varepsilon > 0$, there are elements $a, b \in \mathcal{O}_K$ such that the coefficients of $a - b$ are all less than ε (otherwise the elements of \mathcal{O}_K would all be a “distance” of least ε from each other, so only finitely many of them would fit in S).

As mentioned above, the norms of elements of \mathcal{O}_K are integers. Since the norm of an element is the determinant of left multiplication by that element, the norm is a homogenous polynomial of degree n in the indeterminate coefficients c_i , which is 0 only on the element 0, so the constant term of this polynomial is 0. If the c_i get arbitrarily small for elements of \mathcal{O}_K , then the values of the norm polynomial get arbitrarily small, which would imply that there are elements of \mathcal{O}_K with positive norm too small to be in \mathbb{Z} , a contradiction. So the set S contains only finitely many elements of \mathcal{O}_K . Thus the denominators of the c_i are bounded, so for some d , we have that \mathcal{O}_K has finite index in $A = \frac{1}{d}\mathbb{Z}a_1 + \cdots + \frac{1}{d}\mathbb{Z}a_n$. Since A is isomorphic to \mathbb{Z}^n , it follows from the structure theorem for finitely generated abelian groups that \mathcal{O}_K is isomorphic as a \mathbb{Z} -module to \mathbb{Z}^n , as claimed. \square

Corollary 1.4.8. *The ring of integers \mathcal{O}_K of a number field is noetherian.*

Proof. By Proposition 1.4.7, the ring \mathcal{O}_K is finitely generated as a module over \mathbb{Z} , so it is certainly finitely generated as a ring over \mathbb{Z} . By Theorem 1.2.11, \mathcal{O}_K is noetherian. \square

1.5 Recognizing Algebraic Numbers using LLL

Suppose we somehow compute a decimal approximation α to some rational number $\beta \in \mathbb{Q}$ and from this wish to recover β . For concreteness, say

$$\beta = \frac{22}{389} = 0.05655526992287917737789203084832904884318766066838046 \dots$$

and we compute

$$\alpha = 0.056555.$$

Now suppose given only α that you would like to recover β . A standard technique is to use continued fractions, which yields a sequence of good rational approximations for α ; by truncating right before a surprisingly big partial quotient (the 23 in the continued fraction v), we obtain β :

```

v = continued_fraction(0.056555); v

```

```

[0, 17, 1, 2, 6, 1, 23, 1, 1, 1, 1, 1, 2]

```

```

convergents([0, 17, 1, 2, 6, 1])

```

```

[0, 1/17, 1/18, 3/53, 19/336, 22/389]

```

Generalizing this, suppose next that somehow you numerically approximate an algebraic number, e.g., by evaluating a special function and get a decimal approximation $\alpha \in \mathbb{C}$ to an algebraic number $\beta \in \overline{\mathbb{Q}}$. For concreteness, suppose $\beta = \frac{1}{3} + \sqrt[4]{3}$:

```

N(1/3 + 3^(1/4), digits=50)

```

```

1.64940734628582579415255223513033238849340192353916

```

Now suppose you very much want to find the (rescaled) minimal polynomial $f(x) \in \mathbb{Z}[x]$ of β just given this numerical approximation α . This is of great value even without proof, since often in practice once you know a potential minimal polynomial you can verify that it is in fact right. Exactly this situation arises in the explicit construction of class fields (a more advanced topic in number theory) and in the construction of Heegner points on elliptic curves. As we will see, the LLL algorithm provides a polynomial time way to solve this problem, assuming α has been computed to sufficient precision.

1.5.1 LLL Reduced Basis

Given a basis b_1, \dots, b_n for \mathbb{R}^n , the *Gramm-Schmidt orthogonalization* process produces an orthogonal basis b_1^*, \dots, b_n^* for \mathbb{R}^n as follows. Define inductively

$$b_i^* = b_i - \sum_{j < i} \mu_{i,j} b_j^*$$

where

$$\mu_{i,j} = \frac{b_i \cdot b_j^*}{b_j^* \cdot b_j^*}.$$

Example 1.5.1. We compute the Gramm-Schmidt orthogonal basis of the rows of a matrix. Note that no square roots are introduced in the process; there would be square roots if we constructed an orthonormal basis.

```
A = matrix(ZZ, 2, [1,2, 3,4]); A
```

706

```
[1 2]
[3 4]
```

```
Bstar, mu = A.gramm_schmidt()
```

707 The rows of the matrix B^* are obtained from the rows of A by the Gramm-
 708 Schmidt procedure.

```
Bstar
```

```
[ 1 2]
[ 4/5 -2/5]
```

709

```
mu
```

```
[ 0 0]
[11/5 0]
```

710 A lattice $L \subset \mathbb{R}^n$ is a subgroup that is free of rank n such that $\mathbb{R}L = \mathbb{R}^n$.

Definition 1.5.2 (LLL-reduced basis). The basis b_1, \dots, b_n for a lattice $L \subset \mathbb{R}^n$ is *LLL reduced* if for all i, j ,

$$|\mu_{i,j}| \leq \frac{1}{2}$$

and for each $i \geq 2$,

$$|b_i^*|^2 \geq \left(\frac{3}{4} - \mu_{i,i-1}^2 \right) |b_{i-1}^*|^2$$

For example, the basis $b_1 = (1, 2)$, $b_2 = (3, 4)$ for a lattice L is *not* LLL reduced because $b_1^* = b_1$ and

$$\mu_{2,1} = \frac{b_2 \cdot b_1^*}{b_1^* \cdot b_1^*} = \frac{11}{5} > \frac{1}{2}.$$

However, the basis $b_1 = (1, 0)$, $b_2 = (0, 2)$ for L is LLL reduced, since

$$\mu_{2,1} = \frac{b_2 \cdot b_1^*}{b_1^* \cdot b_1^*} = 0,$$

and

$$2^2 \geq (3/4) \cdot 1^2.$$

```
A = matrix(ZZ, 2, [1,2, 3,4])
A.LLL()
```

711

```

[1 0]
[0 2]
```

712 **1.5.2 What LLL really means**

713 The following theorem is not too difficult to prove.

714 Let b_1, \dots, b_n be an LLL reduced basis for a lattice $L \subset \mathbb{R}^n$. Let $d(L)$
 715 denote the absolute value of the determinant of any matrix whose rows are
 716 basis for L . Then the vectors b_i are “nearly orthogonal” and “short” in the
 717 sense of the following theorem:

718 **Theorem 1.5.3.** *We have*719 1. $d(L) \leq \prod_{i=1}^n |b_i| \leq 2^{n(n-1)/4} d(L)$.2. For $1 \leq j \leq i \leq n$, we have

$$|b_j| \leq 2^{(i-1)/2} |b_i^*|.$$

3. The vector b_1 is very short in the sense that

$$|b_1| \leq 2^{(n-1)/4} d(L)^{1/n}$$

and for every nonzero $x \in L$ we have

$$|b_1| \leq 2^{(n-1)/2} |x|.$$

4. More generally, for any linearly independent $x_1, \dots, x_t \in L$, we have

$$|b_j| \leq 2^{(n-1)/2} \max(|x_1|, \dots, |x_t|)$$

720 for $1 \leq j \leq t$.

721 Perhaps the most amazing thing about the idea of an LLL reduced basis
 722 is that there is an algorithm (in fact many) that given a basis for a lattice L
 723 produce an LLL reduced basis for L , and do so *quickly*, i.e., in polynomial
 724 time in the number of digits of the input. The current optimal implementa-
 725 tion (and practically optimal algorithms) for computing LLL reduced basis
 726 are due to Damien Stehle, and are included standard in Magma in **Sage**.
 727 Stehle’s code is amazing – it can LLL reduce a random lattice in \mathbb{R}^n for
 728 $n < 1000$ in a matter of minutes!

```

A = random_matrix(ZZ, 200)
t = cputime()
B = A.LLL()
729 cputime(t)      # random output

```

```

| 3.0494159999999999

```

730 There is even a very fast variant of Stehle's implementation that computes
731 a basis for L that is very likely LLL reduced but may in rare cases fail to
732 be LLL reduced.

```

t = cputime()
B = A.LLL(algorithm="fpLLL:fast") # not tested
733 cputime(t)      # random output

```

```

| 0.968426999999999837

```

734 1.5.3 Applying LLL

735 The LLL definition and algorithm has many application in number theory,
736 e.g., to cracking lattice-based cryptosystems, to enumerating all short vec-
737 tors in a lattice, to finding relations between decimal approximations to
738 complex numbers, to very fast univariate polynomial factorization in $\mathbb{Z}[x]$
739 and more generally in $K[x]$ where K is a number fields, and to computation
740 of kernels and images of integer matrices. LLL can also be used to solve
741 the problem of recognizing algebraic numbers mentioned at the beginning
742 of Section 1.5.

743 Suppose as above that α is a decimal approximation to some algebraic
744 number β , and to for simplicity assume that $\alpha \in \mathbb{R}$ (the general case of
745 $\alpha \in \mathbb{C}$ is described in [Coh93]). We finish by explaining how to use LLL to
746 find a polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha)$ and its coefficients are small,
747 hence has a shot at being the minimal polynomial of β .

748 Given a real number decimal approximation α , an integer d (the degree),
749 and an integer K (a function of the precision to which α is known), the
750 following steps produce a polynomial $f(x) \in \mathbb{Z}[x]$ of degree at most d such
751 that $f(\alpha)$ is small.

- 752 1. Form the lattice in \mathbb{R}^{d+2} with basis the rows of the matrix A whose
753 first $(d+1) \times (d+1)$ part is the identity matrix, and whose last column
754 has entries

$$K, \lfloor K\alpha \rfloor, \lfloor K\alpha^2 \rfloor, \dots, \lfloor K\alpha^d \rfloor. \quad (1.2)$$

755 (Note this matrix is $(d+1) \times (d+2)$ so the lattice is not of full rank
 756 in \mathbb{R}^{d+2} , which isn't a problem, since the LLL definition also makes
 757 sense for fewer vectors.)

758 2. Compute an LLL reduced basis for the \mathbb{Z} -span of the rows of A , and
 759 let B be the corresponding matrix. Let $b_1 = (a_0, a_1, \dots, a_{d+1})$ be the
 760 first row of B and notice that B is obtained from A by left multipli-
 761 cation by an invertible integer matrix. Thus a_0, \dots, a_d are the linear
 762 combination of the (1.2) that equals a_{d+1} . Moreover, since B is LLL
 763 reduced we expect that a_{d+1} is relatively small.

764 3. Output $f(x) = a_0 + a_1x + \dots + a_dx^d$. We have that $f(\alpha) \sim a_{d+1}/K$,
 765 which is small. Thus $f(x)$ may be a very good candidate for the
 766 minimal polynomial of β (the algebraic number we are approximating),
 767 assuming d was chosen minimally and α was computed to sufficient
 768 precision.

769 The following is a complete implementation of the above algorithm in
 770 Sage:

```

def myalgdep(a, d, K=10^6):
    aa = [floor(K*a^i) for i in range(d+1)]
    A = identity_matrix(ZZ, d+1)
    B = matrix(ZZ, d+1, 1, aa)
771 A = A.augment(B)
    L = A.LLL()
    v = L[0][:-1].list()
    return ZZ['x'](v)

```

772 Here is an example of using it:

```

R.<x> = RDF[]
f = 2*x^3 - 3*x^2 + 10*x - 4
a = f.roots()[0][0]; a
773 myalgdep(a, 3, 10^6)          # not tested

```

2*x^3 - 3*x^2 + 10*x - 4

Index

774	R -module, 8	802	homomorphism, 10
775	\mathbb{Z} is a PID proposition, 13	803	lattice, 30
776	\mathcal{O}_K is a lattice proposition, 27	804	Lemma
777	\mathcal{O}_K is noetherian corollary, 28		\mathcal{O}_K span and $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$, 23
778	\mathcal{O}_K span and $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$ lemma, 23		exactness and noetherian, 11
779	$\overline{\mathbb{Z}}$ is a ring proposition, 15	806	minimal polynomial of algebraic
		807	integer, 17
780	algebraic integer, 15	808	surjection and noetherian, 11
781	algebraic number, 14	809	
782	ascending chain condition, 9	810	LLL reduced, 30
783	characterization of integrality propo-	811	maximal element, 9
784	sition, 15	812	minimal polynomial, 16
785	characterization of noetherian propo-	813	minimal polynomial of algebraic in-
786	sition, 9	814	teger lemma, 17
787	cokernel, 3		
788	Corollary	815	noetherian, 8
789	\mathcal{O}_K is noetherian, 28	816	noetherian equals finitely generated
790	group as quotient of free groups, 2		proposition, 11
791	2	818	norm, 26
792	norm, trace compatible with towers,	819	norm and trace proposition, 26
793	27	820	norm, trace compatible with towers
		821	corollary, 27
794	exact, 10	822	number field, 21
795	exactness and noetherian lemma, 11		
		823	order, 22
796	finitely generated, 1		
		824	Proposition
797	Galois conjugates, 25		\mathbb{Z} is a PID, 13
798	Gramm-Schmidt orthogonalization, 29		\mathcal{O}_K is a lattice, 27
799	group as quotient of free groups corol-	825	$\overline{\mathbb{Z}}$ is a ring, 15
800	lary, 2	826	characterization of integrality, 15
		827	characterization of noetherian, 9
801	Hilbert Basis theorem, 12	828	
		829	

- 830 noetherian equals finitely gener-
- 831 ated, 11
- 832 norm and trace, 26
- 833 Smith normal form, 3
- 834 subgroup of free group, 2

- 835 ring of integers, 21

- 836 sequence, 3
- 837 short exact sequence, 10
- 838 Smith normal form, 2, 3
- 839 Smith normal form proposition, 3
- 840 structure of abelian groups theorem,
- 841 2
- 842 subgroup of free group proposition, 2
- 843 submodule, 8
- 844 surjection and noetherian lemma, 11

- 845 Theorem
- 846 Hilbert Basis, 12
- 847 structure of abelian groups, 2
- 848 trace, 26

Bibliography

- [Art91] M. Artin, *Algebra*, Prentice Hall Inc., Englewood Cliffs, NJ, 1991.
MR 92g:00001
- [Coh93] H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, Berlin, 1993. MR 94i:11105
- [KKM11] Ann Hibner Koblitz, Neal Koblitz, and Alfred Menezes, *Elliptic curve cryptography: The serpentine course of a paradigm shift*, Journal of Number Theory **131** (2011), no. 5, 781 – 814, Elliptic Curve Cryptography.