10 Rings

10.1 The ring axioms

Definition 10.1. *Let R be a set with two binary operations, addition $+ : R \times R \to R$ and multiplication $\cdot : R \times R \to R$. We say R is a* **(commutative) ring (with 1)** *if for all $a, b, c \in R$,*

(a) R is an abelian group under addition, i.e.,
  (i) $a + (b + c) = (a + b) + c$
  (ii) $a + b = b + a$
  (iii) there exists $0 \in R$ such that $a + 0 = a$ for all $a \in R$
  (iv) for each a, there exists $-a \in R$ such that $a + (-a) = 0$

(b) the usual multipilication rules hold, i.e.,
  (v) $a(bc) = (ab)c$
  (vi) $ab = ba$
  (vii) there exists $1 \in R$ such that $1 \cdot a = a$ for all $a \in R$
  (viii) $0 \cdot a = 0$
  (ix) $a(b + c) = ab + ac$.

If we additionally have $0 \neq 1$ and, we can divide by any non-zero element, i.e.,
  (x) for each $a \neq 0 \in R$, there exists a^{-1} such that $aa^{-1} = 1$,
then we say R is a **field**.

Note that if all the properties and (a) and (b) hold except for (vi)[1], we say R is a *noncommutative ring*. We will primarily be interested in commutative rings for the rest of the semester, though noncommutative rings are also common and useful in number theory: examples include $M_2(\mathbb{Z})$, $M_2(\mathbb{Q})$, $M_2(\mathbb{R})$, $M_2(\mathbb{C})$, where $M_2(R)$ denotes the set of 2×2 matrices with coefficients in R, Hamilton's quaternions $\mathbb{H}$, and the Hurwitz integers from Chapter 8.

Another remark on terminology: not all authors require rings to contain 1. We however, will always mean a commutative ring with 1 by the term ring.

10.2 Rings and fields

Rings and fields should be properly treated in a course on algebra, so we will not go through all the formalities of checking all the axioms hold for our examples. What is important, is to get a feel for what sort of things are rings and fields. The basic idea is that a ring is a "number system" like $\mathbb{Z}$, where one can add, subtract and multiply, and all the usual laws hold. A field is a "number system" like $\mathbb{Q}$, where one can add, subtract, multiply and divide, and all the usual laws hold. The definition we gave says that a field is a ring where every non-zero element is invertible. In particular, any field is a ring. Now let's look at some comcrete examples.

Example. *$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are all rings. All but $\mathbb{Z}$ are fields (only ± 1 are invertible in $\mathbb{Z}$).*

Example. *$\mathbb{Z}/n\mathbb{Z}$ is a ring. If n is prime, it is also a field. ($\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime).*

[1] Technically, one should also modify (vii), (viii), (ix) so they are true from the left and right, e.g., $1 \cdot a = a$ becomes $1 \cdot a = a \cdot 1 = a$

Example. $\mathbb{N}$ *is not a ring. Nor is* $\mathbb{N} \cup \{0\}$*. The first does not contain* 0*, and the second does not contain negatives, i.e., they are not closed under subtraction.*

Example. $S = \{z \in \mathbb{C} : |z| \leq 1\}$ *is not a ring. It contains* $0, 1$*, all its negatives and is closed under multiplication, but it is not closed under addition: e.g.,* $1 + 1 \notin S$*.*

Example. $\mathbb{Z}[\sqrt{n}]$ *is a ring for any* $n \in \mathbb{Z}$*. (If* n *is a square, then* $\mathbb{Z}[\sqrt{n}] = \mathbb{Z}$*. So is* $\mathbb{Z}[\zeta_3]$*. These are not fields.*

Exercise 10.1. *Why are* $\mathbb{Z}/4\mathbb{Z}$ *and* $\mathbb{Z}/6\mathbb{Z}$ *not fields? What about* $\mathbb{Z}[i]$*?*

Example. *Let* $n \in \mathbb{Z}$ *and* $\mathbb{Q}(\sqrt{n}) = \{a + b\sqrt{n} : a, b \in \mathbb{Q}\}$*. (Again* $\mathbb{Q}(\sqrt{n}) = \mathbb{Q}$ *if* n *is a square.) Then* $\mathbb{Q}(\sqrt{n})$ *is a field.*

From the $\mathbb{Z}[\sqrt{n}]$ and $\mathbb{Q}(\sqrt{n})$ examples, we see we may form new rings and fields, by adding elements to old one—this is called *adjoining* elements.

Definition 10.2. *Let* $R, F \subseteq \mathbb{C}$ *where* R *is a ring and* F *is a field. Let* $\alpha \in \mathbb{C}$*. Then* $R[\alpha]$ *is defined to be the smallest ring in* $\mathbb{C}$ *containing both* R *and* α*. Similarly* $F(\alpha)$ *is defined to be the smallest field in* $\mathbb{C}$ *containing both* F *and* α*.*

Note: we can sequentially adjoin more than element to a ring or field. We denote this simply by putting more than one element in the brackets or parentheses. For example if $R = \mathbb{Z}[\sqrt{2}]$, we can consider $R' = R[\sqrt{3}]$. It is cumbersome to write $R' = \mathbb{Z}[\sqrt{2}][\sqrt{3}]$, so we just write $R' = \mathbb{Z}[\sqrt{2}, \sqrt{3}]$.

Example. $\mathbb{Z}[\sqrt{-3}, \frac{-1+\sqrt{-3}}{2}] = \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}] = \mathbb{Z}[\zeta_3]$*. We encountered this in Chapter 7, since* $\mathbb{Z}[\sqrt{-3}]$ *did not have unique factorization, we adjoined* $\zeta_3 = \frac{-1+\sqrt{3}}{2}$*. But we can write this new ring simply as* $\mathbb{Z}[\zeta_3]$*, as opposed to* $\mathbb{Z}[\sqrt{-3}, \frac{-1+\sqrt{-3}}{2}]$*, since* $\sqrt{-3} = 2\zeta_3 + 1 \in \mathbb{Z}[\zeta_3]$*.*

Example. $\mathbb{Z}[\sqrt{2}, \sqrt{3}] = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Z}\right\}$*. To see why, observe that* $\sqrt{2}\sqrt{3} = \sqrt{6}$ *must be in the ring. Since* $\mathbb{Z}[\sqrt{2}, \sqrt{3}]$ *is closed under multiplication and addition, we must have every element of the form* $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ *for* a, b, c, d *is in the ring, i.e., any ring containg* $\mathbb{Z}$*,* $\sqrt{2}$ *and* $\sqrt{3}$ *must contain the set on the right. Hence it suffices to show the set on the right is a ring. This will follow (see below) if we know it is closed under addition, subtraction and multipliation. Clearly adding or subtracting two elements of this form gives another element of this form, so it is closed under addition and subtraction. It is closed under multiplication since*

$$(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6})(e + f\sqrt{2} + g\sqrt{3} + h\sqrt{6}) =$$
$$(ae + 2bf + 3cg + 6hd) + (af + be + 3ch + 3dg)\sqrt{2} + (ag + ce + 2bh + 2df)\sqrt{3} + (ah + de + bg + cf)\sqrt{6}.$$

Similarly one can check $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\right\}$*.*

Here we used the following basic fact.

Definition 10.3. *Let* $R \subset R'$*. If* R *and* R' *are rings (with respect to the same operations), we say* R *is a* **subring** *of* R'*. If* R *and* R' *are fields (with respect to the same operations), we say* R *is a* **subfield** *of* R'*.*

Lemma 10.4. *Let R' be a ring and $R \subseteq R'$ be non-empty. Then R is a subring of R' if and only if R is closed under addition, subtraction and multiplication. Similarly if R' is a field, R is a subfield of R' if and only if R is closed under addition, subtraction, multiplication and division by non-zero elements.*

The proof is like our proof of the corresponding test for subgroups in Chapter 3, which was similar to the corresponding test for subspaces you probably saw in Linear Algebra.

Exercise 10.2. *In the same way we determined $\mathbb{Z}[\sqrt{2},\sqrt{3}] = \left\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} : a,b,c,d \in \mathbb{Z}\right\}$, determine what the rings $\mathbb{Z}[\sqrt{-2},i]$ and $\mathbb{Z}[\sqrt[3]{2}]$ are, in terms of $\mathbb{Z}$-linear combinations of algebraic numbers. Similarly determine what $\mathbb{Q}(\sqrt{-2},i)$ and $\mathbb{Q}(\sqrt[3]{2})$ are in terms of $\mathbb{Q}$-linear combinations of algebraic numbers. Prove at least one of your four answers, like we did in the example above. For the other three, you may just state the answer.*

Now that we have some examples under our belt, let's define some basic concepts we've been working with this semester in the case of specific examples, along with some other fundamental terms.

Definition 10.5. *Let R be a ring. We say $u \in R$ is a* **unit** *if u is invertible in R. We say $\alpha \in R$ is* **irreducible** *if any factorization $\alpha = \beta\gamma$ in R implies β or γ is a unit. If $\alpha = \beta\gamma$ we say β* **divides** *(or is a* **divisor** *of) α and write $\beta|\alpha$. If $\alpha = u\beta$ where u is a unit, we say α and β are* **associates**, *and write $\alpha \sim \beta$.*

Suppose $\alpha \in R$ satisfies the prime divisor property*, i.e., $\alpha|\beta\gamma$ implies $\alpha|\beta$ or $\alpha|\gamma$. Then we say α is* **prime** *in R if α is not a unit.*

An equivalent definition of α being irreducible is that the only divisors of α are the units and the associates of α.

We will not use the notion of prime elements often for rings that do not have unique factorization, but it may be worthwhile to make a couple of comments. For any ring R, one can check every prime π of R is irreducible. Further, if R satisfies the prime divisor property (which is equivalent to unique factorization into irreducibles, up to units) an element $\pi \in R$ is prime if and only if it is a non-unit irreducible. In fact R has unique factorization if and only if every non-unit irreducible is prime.

Example. *Let $n \in \mathbb{N}$. Then u is a unit of $\mathbb{Z}[\sqrt{n}]$ if and only if $N(u) = \pm 1$. However, the norm map on $\mathbb{Z}[\sqrt{-n}]$ is never negative, so u is a unit $\mathbb{Z}[\sqrt{-n}]$ if and only if $N(u) = 1$. We've seen the proofs in Chapters 6 and 7, so this matches with our earlier definition of unit.*

In the case of $\mathbb{Z}[\sqrt{n}]$ and n squarefree, the units are going to be $\pm\epsilon^m$ where ϵ is a fundamental unit *of $\mathbb{Z}[\sqrt{n}]$, i.e., $x+y\sqrt{n}$ where x,y is a smallest positive solution to $x^2-ny^2 = \pm 1$ and $m \in \mathbb{Z}$. There may or may not be a non-trivial solution to $x^2-ny^2 = -1$—if there is, such a solution will correspond to the fundamental unit ϵ—if not, ϵ will be the fundamental $+$-unit from Chapter 5. It is an interesting question to know when is the fundamental $+$-unit the fundamental unit, i.e., when $x^2-ny^2 = -1$ has a non-trivial solution, but we will not pursue this this semester. Instead, we will focus the imaginary quadratic rings like $\mathbb{Z}[\sqrt{-n}]$ and $\mathbb{Z}[\zeta_3]$, which have more structure (making them simpler to work with) and are in many ways more interesting.*

Exercise 10.3. *Let R be a ring, and U be the subset of units. Show that U is a group under multiplication. What are the units of $R = \mathbb{Z}/n\mathbb{Z}$? What about $R = \mathbb{Z}[\sqrt{-n}]$ for $n \in \mathbb{N}$?*

Exercise 10.4. *Let R be a ring. Let u be a unit of R. Show u' is also a unit of R if and only if $u' \sim u$.*

Example. *Let F be a field. Then* every *non-zero element is invertible, i.e., every non-zero element is a unit. Consequently, every non-zero element of F is irreducible, since any factorization must be into units. There are no primes.*

Hence none of the notions in Defintion 10.5 are interesting in the case of fields. Similarly, the question of unique factorization is moot. For example, if $F = \mathbb{Q}$ then we have factorizations like $2 = \frac{2}{3} \cdot 3$, but all 3 of these numbers are units, so this is considered a trivial factorization in F.

This suggests the following. If R does not have unique factorization, e.g., $R = \mathbb{Z}[\sqrt{-3}]$, then maybe we want to try adjoining elements to regain unique factorizations. If we adjoin inverses for each non-zero element of R, we will get the field $F = \mathbb{Q}(\sqrt{-3})$, which trivially has unique factorization (in a very unhelpful way). So if we add enough things to R, we can recover unique factorization, but we don't want to add so much that we get a field, which will make the unique factorization useless. Knowing what is the right amount to add, which in our example is $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$, is a very delicate question, and it may not always be possible. In any case, the first step to knowing what to add is learning about algebraic integers in the next section.

10.3 Algebraic integers

Definition 10.6. *Let $\alpha \in \mathbb{C}$. We say α is an* **algebraic number of degree** *$m > 0$ if*

$$\alpha^m + c_{m-1}\alpha^{m-1} + \cdots + c_1\alpha + c_0 = 0$$

for some $c_0, c_1, \ldots, c_m \in \mathbb{Q}$ with $m > 0$ minimal. If each $c_i \in \mathbb{Z}$, we say α is an **algebraic integer**. *The polynomial $p(x) = x^m + c_{m-1}x^{m-1} + \cdots + c_1x + c_0$ is called the* **minimum polynomial** *of α.*

In other words, α is an algebraic number if it is a root of a monic polynomial with coefficients in $\mathbb{Q}$, and it is an algebraic integer if it is a root of a monic polynomial with coefficients in $\mathbb{Z}$. (Recall a monic polynomial is one whose leading coefficient is 1.)

Exercise 10.5. *Show the definition of algebraic number and algebraic integer given in class coincide with that in the text. Namely show that (i) α is an an algebraic number of degree m if and only if*

$$a_m\alpha^m a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0 = 0$$

for some $a_i \in \mathbb{Z}$ with m minimal; and (ii) α is an algebraic integer if and only if we may take $a_m = 1$.

In other words, the algebraic numbers are just roots of polynomials over $\mathbb{Z}$, and the algebraic integers are the roots of monic polynomials over $\mathbb{Z}$. These may seem like strange conditions, but the next example suggests our definition is reasonable.

Example. *$m = 1$. The algebraic numbers of degree 1 are the solutions to*

$$\alpha + c = 0 \iff \alpha = -c$$

for $c \in \mathbb{Q}$, i.e., they are precisely the rational numbers. The algebraic integers of degree 1 are those $\alpha = -c$ with $c \in \mathbb{Z}$, i.e., just $\mathbb{Z}$. Thus the notion of algebraic numbers and algebraic integers are some sort higher degree generalization of $\mathbb{Q}$ and $\mathbb{Z}$.

Example. $m = 2$. *The algebraic numbers of degree* 2 *are the non-rational solutions to*

$$\alpha^2 + b\alpha + c = 0 \iff \alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

where $b, c \in \mathbb{Q}$. *The algebraic integers of degree* 2 *are just the numbers of the same form but with* $b, c \in \mathbb{Z}$. *Note if* $b = c = 1$, *we get* $\alpha = \zeta_3$, *so* ζ_3 *is an algebraic integer.*

Example. *An* n*-th root of any* $a \in \mathbb{Z}$ *is an algebraic integer. It satisfies* $p(x) = x^n - a = 0$. *Caution: the roots of* $p(x)$ *are not necessarily of degree* n. *For instance* $p(x) = x^4 - 1 = (x^2 - 1)(x^2 + 1)$ *has roots* $\pm 1, \pm i$, *the* 4*-th roots of unity. Clearly* ± 1 *are of degree* 1 *and* $\pm i$ *are of degree* 2. *However, the* 4*-th roots of* 2, *i.e., the roots of* $p(x) = x^4 - 2$ *namely* $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$ *are all of degree* 4. *The difference is that* 1 *is both a square and a* 4*-th power, but* 2 *is neither.*

Note that unlike the degree 1 case, the algebraic integers (numbers) of degree ≤ 2 do not form a ring (field). For instance $\sqrt{2}$ and $\sqrt{3}$ are algebraic integers of degree 2, but $\sqrt{2} + \sqrt{3}$ is not. It will be algebraic of degree 4 however. In fact, one has the following.

Proposition 10.7. *The algebraic integers form a subring of* $\mathbb{C}$. *The algebraic numbers form a subfield of* $\mathbb{C}$.

The proof is somewhat technical and not so enlightening, so we omit the proof. In any case, we will never work with all algebraic integers or algebraic numbers at the same time. The point is, these sets are too large to be useful, particularly from the point of view of unique factorization. (Another hint that they might not be a good thing to work with is that there is no standard notation for them.) For instance, how does 2 factor into the ring of all algebraic integers? It clearly factors as $(\sqrt{2})^2$, which further factors as $(\sqrt[4]{2})^4$. We can repeat this process indefinitely, so there is no minimal factorization. (Also none of these factors are units, because their reciprocals are not algebraic integers, so there are infinitely many "non-trivial" factorizations of 2.) Instead, one works with more manageable-sized subrings of the algebraic integers, such as $\mathbb{Z}[i], \mathbb{Z}[\zeta_3]$ or $\mathbb{Z}[\sqrt{2}, \sqrt{3}]$.

The importance of the distinction between algebraic integers and algebraic non-integers is perhaps still not clear. To understand this, we will first need some analogues of notions familiar from linear algebra.

Definition 10.8. *Let* R *be a subring of* $\mathbb{C}$. *We say* $\{\alpha_i\}$ *is a* $\mathbb{Z}$**-basis** *for* R *if each* $\alpha_i \in R$ *and every* $x \in R$ *can be written uniquely in the form* $x = c_1\alpha_{i_1} + c_2\alpha_{i_2} + \cdots c_m\alpha_{i_m}$ *where* $c_i \in \mathbb{Z}$. *Every* $\mathbb{Z}$*-basis for* R *has the same number of elements; this number is called the* **degree** *of* R *(over* $\mathbb{Z}$*), and denoted* $[R : \mathbb{Z}]$.

Note that any non-zero subring R of $\mathbb{C}$ contains $\mathbb{Z}$: it contains 1, and therefore $2 = 1 + 1$, $3 = 1 + 1 + 1$, and so on, as well as their negatives. Technically, the zero ring $R = \{0\}$ is also a subring of $\mathbb{C}$, and it has the empty set as its $\mathbb{Z}$-basis, i.e., it is degree 0 over $\mathbb{Z}$. We will not prove the fact that every $\mathbb{Z}$-basis of R has the same number of elements—but the idea is the same as for vector spaces over fields. If you want to see a proof, look up some basic *module theory* (a module is like a vector space, but defined over a ring instead of a field).

Proposition 10.9. *Let* $\alpha \in \mathbb{C}$ *be algebraic. Then* $[\mathbb{Z}[\alpha] : \mathbb{Z}] < \infty$ *if and only if* α *is an algebraic integer. Further, if* α *is an algebraic integer of degree* m, *then* $[\mathbb{Z}[\alpha] : \mathbb{Z}] = m$ *and* $\left\{1, \alpha, \cdots, \ , \alpha^{m-1}\right\}$ *is a* $\mathbb{Z}$*-basis of* $\mathbb{Z}[\alpha]$.

Proof. ($\Leftarrow$) Suppose α is an algebraic integer of degree m, so it satisfies

$$\alpha^m = c_{m-1}\alpha^{m-1} + \cdots + c_1\alpha + c_0$$

for some $c_i \in \mathbb{Z}$.

We claim $\left\{1, \alpha, \ldots, \alpha^{m-1}\right\}$ is a basis for $\mathbb{Z}[\alpha]$. Since $\mathbb{Z}[\alpha]$ is closed under multiplication, all the powers of α must be contained in $\mathbb{Z}[\alpha]$, i.e., each $\alpha^i \in \mathbb{Z}[\alpha]$. We want to show that

$$\mathbb{Z}[\alpha] = \left\{a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} | a_i \in Z\right\}.$$

It is clear the right hand side is contained in the left, so it suffices to show the right hand side is a subring of $\mathbb{C}$. It is clearly closed under addition and subtraction. When one multiplies two elements of the form on the right, one gets a $\mathbb{Z}$-linear combination of $1, \alpha, \cdots \alpha^{2m-2}$, but we can rewrite each α^j for $j \leq m$ in terms of smaller powers of α from the relation above. We can keep doing this this until our product is expressible entirely as a $\mathbb{Z}$-linear combination of $1, \alpha, \ldots, \alpha^{m-1}$, showing the right hand set is closed under multiplication, hence the smallest ring containing $\mathbb{Z}$ and α.

This almost proves the claim, but we didn't show that $\left\{1, \alpha, \ldots, \alpha^{m-1}\right\}$ is a $\mathbb{Z}$-basis, because we didn't check that it is $\mathbb{Z}$-*linearly independent*, i.e., that $a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} = 0$ has only the trivial solution. (This implies the uniqueness criterion in the definition of $\mathbb{Z}$-basis just like in the vector space case.) But this is true because no α^i is a $\mathbb{Z}$-linear combination of smaller powers of α if $i < m$ (otherwise α would have smaller degree).

($\Rightarrow$) For clarity, we sketch the idea with a specific example—the general case follows in the same way. Suppose $\alpha = \frac{1}{\sqrt{2}}$. Then it satisfies the integer polynomial $2x^2 - 1 = 0$ or the monic polynomial $x^2 - \frac{1}{2} = 0$, so this is an algebraic non-integer. Again $\mathbb{Z}[\alpha]$ must contain all powers of α, namely $\frac{1}{\sqrt{2}}, \frac{1}{2}, \frac{1}{2\sqrt{2}}, \ldots, \frac{1}{2^m}, \frac{1}{2^m\sqrt{2}}, \ldots$. One can check that these form a $\mathbb{Z}$-basis for $\mathbb{Z}[\alpha]$. Since the denominators are increasing, none of these powers of α can be written as a $\mathbb{Z}$-linear combination of the smaller powers. For example, $\frac{1}{2} \neq a + \frac{b}{\sqrt{2}}$, $\frac{1}{2\sqrt{2}} \neq a + \frac{b}{\sqrt{2}} + \frac{c}{2}$ for any $a, b, c \in \mathbb{Z}$. Hence no finite subset of these powers can form a $\mathbb{Z}$-basis for $\mathbb{Z}[\alpha]$. Therefore $\mathbb{Z}[\alpha]$ does not have a finite $\mathbb{Z}$-basis. □

Note one can use the above proposition to prove the previous one. See Stewart and Tall's *Algebraic Number Theory*.

10.4 Quadratic fields and their integers

Let F be a subfield of $\mathbb{C}$. As with (non-zero) subrings of $\mathbb{C}$, since it contains 1 it must contain $\mathbb{Z}$; therefore it must contain $\mathbb{Q}$. Just like $\mathbb{C}$ is a 2-dimensional vector space over $\mathbb{R}$, we may view F as a vector space over $\mathbb{Q}$—one can add any two vectors, and one can scale any vector by a rational number. This just addition and multiplication in F. For example $\mathbb{Q}(\sqrt{2}) = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}$ is a 2-dimensional vector space over $\mathbb{Q}$ with basis $\left\{1, \sqrt{2}\right\}$.

Definition 10.10. *Let F be a subfield of $\mathbb{C}$. The* **degree** *of F over $\mathbb{Q}$, denoted by $[F : \mathbb{Q}]$, is the dimension of F over $\mathbb{Q}$ as a vector space. If $[F : \mathbb{Q}]$ is finite, we say F is a* **number field**. *We say F is a* **quadratic field** *if $[F : \mathbb{Q}] = 2$.*

Number fields, and their corresponding rings of integers (see below), are the fundamental objects of study in algebraic number theory. It is not to hard to see that every number field consists entirely of algebraic numbers. We will start off by investigating the simplest case (apart from $\mathbb{Q}$), the quadratic fields.

Proposition 10.11. *If F is a quadratic field, then $F = \mathbb{Q}(\sqrt{d})$ for some $d \in Z$ (non-square). In fact, we may take d to be* squarefree*, i.e., d is not divisible by any square.*

We will not need this, so we will omit the proof, but it is good to know. It should also be reassuring, since the text defines a quadratic field to be one of the form $\mathbb{Q}(\sqrt{d})$. The reason we may take d to be squarefree is because if $d = n^2 d'$, $\mathbb{Q}(\sqrt{n^2 d'}) = \mathbb{Q}(\sqrt{d'})$, so we may factor out any squares dividing d. In general, the characterization of higher degree fields (cubic, quartic, etc), is not so simple. You should be sure of the converse however.

Exercise 10.6. *Let $d \in \mathbb{Z}$ be a non-square. Show that $F = \mathbb{Q}(\sqrt{d})$ has degree 2 over $\mathbb{Q}$.*

Definition 10.12. *Let F be a number field. Its* **ring of integers***, denoted by $\mathcal{O}_F$, is defined to be the set of algebraic integers which lie in F.*

Note that $\mathcal{O}_F$ is indeed a ring since it is the intersection of two subrings of $\mathbb{C}$: F and the ring of all algebraic integers. While we omitted the proof of the fact that all algebraic integers form a ring, it is easy to check that $\mathcal{O}_F$ is a ring for F quadratic from the determination of $\mathcal{O}_F$ below.

Now one needs to be careful of terminology with a more general notion of integer floating around. We typically refer to $\mathcal{O}_F$ as the integers of F, or just integers if it is clear what field we are working in. Then to distinguish the usual integers $\mathbb{Z}$ from the integers $\mathcal{O}_F$, we call elements of $\mathbb{Z}$ *rational integers*. Indeed, they are the integer ring of $\mathbb{Q}$, i.e., $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

Exercise 10.7. *Check that $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.*

Proposition 10.13. *Let $d \in \mathbb{Z}$ be squarefree, $F = \mathbb{Q}(\sqrt{d})$ and $\mathcal{O}_F$ be its ring of integers. Then*

$$\mathcal{O}_F = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & d \equiv 1 \bmod 4, \\ \mathbb{Z}[\sqrt{d}] & d \equiv 2, 3 \bmod 4. \end{cases}$$

Note d squarefree implies $d \not\equiv 0 \bmod 4$.

Proof. ($\supseteq$) It is easy to see that $\mathcal{O}_F$ always $\mathbb{Z}[\sqrt{d}]$, since $\sqrt{d}$ is an algebraic integer: it is a root of $x^2 - d$. Further, to see when the element $\alpha = \frac{1+\sqrt{d}}{2} \in \mathcal{O}_F$, observe

$$N(\alpha) = \alpha\overline{\alpha} = \frac{1+\sqrt{d}}{2}\frac{1-\sqrt{d}}{2} = \alpha(1-\alpha),$$

i.e., the minimum polynomial for α is $p(x) = x^2 - x + N(\alpha)$, which has integer coefficients since $N(\alpha) = \frac{1-d}{4}$. precisely when $d \equiv 1 \bmod 4$. In other words $\frac{1+\sqrt{d}}{2} \in \mathcal{O}_F$ if and only if $d \equiv 1 \bmod 4$.

This shows $\mathcal{O}_F$ is at least as big is as claimed—we still have to show nothing else is contained in $\mathcal{O}_F$.

($\subseteq$) Suppose $\alpha \in \mathbb{Q}(\sqrt{d})$ is an integer. It is easy to see that α must be of degree 2 (e.g., quadratic formula or exercise below). We saw earlier this means α is of the form $\alpha = \frac{-b' \pm \sqrt{b'^2 - 4c'}}{2}$. for $b', c' \in \mathbb{Z}$. In particular, any $\alpha \in F$ must be of the form $\alpha = \frac{a+b\sqrt{d}}{2}$ for some $a, b \in \mathbb{Z}$ (and $b \neq 0$). We want to find the minimum polynomial $p(x)$ for α in terms of a and b.

Write $p(x) = x^2 + mx + n$. This means

$$p(\alpha) = \frac{a^2 + db^2 + 2ma + 4n + 2(a+m)b\sqrt{d}}{4} = 0.$$

Looking at the $\sqrt{d}$ coefficient (which is called the irrational part if $d > 0$ and the complex part if $d < 0$), we see $m = -a$. Then the rational part (called the real part if $d < 0$) is $\frac{db^2-a^2}{4} + n = 0$. Hence $n = -\frac{db^2-a^2}{4} \in \mathbb{Z}$ if and only if $db^2 \equiv a^2 \bmod 4$.

If $d \not\equiv 1 \bmod 4$, the only possibility is that a, b are both even, i.e., $\alpha \in \mathbb{Z}[\sqrt{d}]$. This proves the $d \equiv 2, 3 \bmod 4$ cases.

If $d \equiv 1 \bmod 4$, the above means $a \equiv b \bmod 4$, i.e., $\alpha = \frac{a-b}{2} + b\frac{1+\sqrt{d}}{2}$. Note $\frac{a-b}{2} \in \mathbb{Z}$ when $a \equiv b \bmod 4$, so in fact $\alpha \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. □

Example. *Let $F = \mathbb{Q}(\sqrt{-3})$. Then $\mathcal{O}_F$ is not $\mathbb{Z}[\sqrt{-3}]$ but $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$. Since $\frac{1+\sqrt{-3}}{2} = 1 + \zeta_3$, we see $\mathcal{O}_F = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}] = \mathbb{Z}[\zeta_3]$.*

This provides some motivation for why we tried looking at $\mathbb{Z}[\zeta_3]$ after realizing unique factorization fails in $\mathbb{Z}[\sqrt{-3}]$. The ring $\mathbb{Z}[\sqrt{-3}]$ does not contain all algebraic integers of the form $x + y\sqrt{-3}$ for $x, y \in \mathbb{Q}$, but $\mathbb{Z}[\zeta_3]$ does.

Exercise 10.8. *Let d be squarefree, and $\alpha = a + b\sqrt{d}$ where $a, b \in \mathbb{Q}$, i.e., $\alpha \in \mathbb{Q}(\sqrt{d})$. As usual $\overline{\alpha} = a - b\sqrt{d}$, and the norm is $N(\alpha) = \alpha\overline{\alpha}$. Define the* trace *of α to be $\mathrm{tr}(\alpha) = \alpha + \overline{\alpha}$. Suppose $\alpha \notin \mathbb{Q}$. Show the minimum polynomial for α is $p(x) = x^2 - \mathrm{tr}(\alpha)x + N(\alpha)$.*

This formula may remind you of the formula characterisic polynomial for a 2×2 non-scalar matrix, where one replaces norm by determinant.

In particular this means every $\alpha \in \mathbb{Q}(\sqrt{d})$ is in fact an algebraic number of degree 2. Moreover, it means the integers of $\mathbb{Q}(\sqrt{d})$ are precisely the elements whose trace and norm is an integer. This is a more intuitive way of looking at what it means to be an algebraic integer of degree 2.

Exercise 10.9. *Check the trace (as defined above) is a group homomorphism from $(\mathbb{Q}(\sqrt{d}), +)$ to $(\mathbb{Q}, +)$. In other words check (i) $\mathrm{tr}(\alpha) \in \mathbb{Q}$ for $\alpha \in \mathbb{Q}(\sqrt{d})$, and (ii) $\mathrm{tr}(\alpha + \beta) = \mathrm{tr}(\alpha) + \mathrm{tr}(\beta)$ for $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$.*

Let's summarize some basic ideas of algebraic number theory now with a couple of examples that illustrate the main issues arising.

1. Goal of number theory: study integer solutions to polynomial equations, e.g., what numbers are of the form $n = x^2 + 3y^2$ or $n = x^2 + 5y^2$.

2. Main principle of algebraic number theory: work in a larger ring/field than $\mathbb{Z}/\mathbb{Q}$ so that your polynomial equation factors; e.g., if we work in $\mathbb{Z}[\sqrt{-3}]/\mathbb{Q}(\sqrt{-3}))$ and $\mathbb{Z}[\sqrt{-5}]/\mathbb{Q}(\sqrt{-5})$, we can factor $x^2 + 3y^2 = (x + y\sqrt{-3})(x - y\sqrt{-3})$ and $x^2 + 5y^2 = (x + y\sqrt{5})(x - y\sqrt{5})$.

3. Main difficulty: to make use of the factorizations $x^2 + 3y^2 = (x + y\sqrt{-3})(x - y\sqrt{-3})$ and $x^2 + 5y^2 = (x + y\sqrt{5})(x - y\sqrt{5})$, we want to use unique factorization into primes/irreducibles (or equivalently, the prime divisor property), but neither $\mathbb{Z}[\sqrt{-3}]$ nor $\mathbb{Z}[\sqrt{-5}]$ have unique factorization.

4. First idea: maybe one can add more elements of $\mathbb{Q}(\sqrt{-3})$ to recover unique factorization in $\mathbb{Z}[\sqrt{-3}]$; indeed, $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}[\zeta_3]$ has unique factorization. The big problem with this idea is that it only works in a few cases.

5. Second idea: The above does not work for $\mathbb{Z}[\sqrt{-5}]$, since $\mathbb{Z}[\sqrt{-5}] = \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ does not have unique factorization. Perhaps we can recover unique factorization in $\mathbb{Z}[\sqrt{-5}]$ by working with the algebraic integers of a larger field than $\mathbb{Q}(\sqrt{-5})$. Indeed, every element of $\mathbb{Z}[\sqrt{-5}]$ has a unique factorization into elements of $\mathbb{Z}[\sqrt{-5}, i] = \mathcal{O}_{\mathbb{Q}(\sqrt{-5},i)}$. There are a two main issues with this idea: (i) how does one find the appropriate larger field to work in? (ii) the ring of integers of this larger field may be considerably more complicated than the ring we wanted to work in.

6. Third idea: Look at the problem from a different perspective. Historically we have learned through experimentation that the simplest way to study factorization questions in a ring is through Dedekind's theory of ideals. We will revisit the second idea later in the year, which can be useful, but we will spend the rest of the semester considering Dedekind's ideal theory.

10.5 Norms and units of quadratic fields

We've already covered pretty much everything in here, but I recommend you read over it to review the ideas. Also, there's a solution to one of the exercises in there.

10.6 Discussion

Probably worth reading.