APPENDIX **D**

Groups, Rings, and Fields

At various points in this book, examples and results are given that pertain to the most important types of algebraic structures: groups, rings, and fields, as well as more specialized structures such as integral domains, ordered fields, etc. This appendix provides the definitions of some of the most important algebraic structures, plus a few examples and basic facts (related to topics discussed in the text, for the most part). It is intended as a reference for readers who are a bit rusty on these concepts. However, if you have never studied these structures (usually covered in courses called "abstract algebra" or "modern algebra"), you will probably need more than this appendix in order to understand the parts of the book that discuss them.

The one type of algebraic structure that is discussed in the text but not defined in this appendix is vector spaces. This decision has been made with the hope that most readers will have encountered vector spaces in relatively low-level courses in subjects such as matrix algebra or even calculus, if not in a linear algebra course.

Throughout this appendix, the symbols $*$, $\cdot$ and $+$ denote **binary operations** on a set A, functions from $A \times A$ to A. With these symbols, we always use "infix" notation rather than the usual function notation. That is, the result of applying the operation $*$ to the ordered pair (x, y) is written $x * y$, rather than the strange-looking $*(x, y)$. (The same thing is done with ordering relations—see Appendix B.) We may also abbreviate $x * y$ or $x \cdot y$ further to xy, as we do with ordinary multiplication.

Groups

Definition. A **group** is a set A together with a binary operation $*$ on A satisfying these conditions:

1. The **associative law** holds: $(x * y) * z = x * (y * z)$, for every x, y, and z in A.
2. There is a (two-sided) **identity** element, that is, an element e in A such that $x * e = e * x = x$, for every x in A.
3. Each element of the group has a (two-sided) **inverse**: for every x in A, there is a y in A such that $x * y = y * x = e$, where e is some identity element.

The words "together with" in this definition are a typical bit of jargon. Technically, a group is an ordered pair $(A, *)$ such that $*$ is a binary operation on A and the three listed conditions hold. So a group is a type of first-order structure in the sense of Chapter 5. More precisely, a group is a model of the theory consisting of conditions (1), (2), and (3), in the first-order language with a single binary function symbol.

Note that the set A is not a group by itself. In practice, mathematicians are often sloppy about this usage. For example, a reference to "the group of integers" would be understood to be about the group $(\mathbb{Z}, +)$, since $(\mathbb{Z}, \cdot)$ is not a group. Also, when we refer to an element of a group G, where $G = (A, *)$, we really mean an element of A.

Proposition D.1. *In any group, the identity element is unique, and the inverse of each element is unique.*

In most abstract algebra texts, this proposition is the first thing proved about groups. Because we have uniqueness, we can refer to *the* identity, and *the* inverse of any element, in a given group. Uniqueness also justifies the use of special symbols for the identity and inverses. There are two common conventions for this. In **multiplicative notation** for a group, the binary operation is written as $x \cdot y$ or simply xy, the identity is denoted 1, and the inverse of an element x is denoted x^{-1}. In **additive notation** for a group, the binary operation is written as $x + y$, the identity is denoted 0, and the inverse of x is denoted $-x$.

Furthermore, when multiplicative notation (or even the symbol $*$) is used for a group, it is common to use exponents: x^2 for $x \cdot x$, x^3 for $x \cdot x \cdot x$, and also x^{-2} for $x^{-1} \cdot x^{-1}$, etc. On the other hand, when additive notation is used, one writes $2x$ for $x + x$, $3x$ for $x + x + x$, $-2x$ for $(-x) + (-x)$, etc. Note that these integer exponents and coefficients do not denote elements of the group!

Example 1. The sets $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{Z}$, with ordinary addition as the binary operation, are all groups. So are the sets $\mathbb{R} - \{0\}$, $\mathbb{Q} - \{0\}$, $\mathbb{R}^+$ (the positive reals) and $\mathbb{Q}^+$ under multiplication. We have to exclude 0 in these last four groups since 0 has no multiplicative inverse.

There is a great variety of groups and special types of groups. Here is the most important category of them:

Definition. A group is called **abelian** if it satisfies the **commutative law**: $x * y = y * x$, for all elements x and y.

It would seem logical to refer to such groups as commutative groups, and this usage, although uncommon, would generally be understood. The term "abelian" honors the Norwegian mathematician Niels Abel, one of the pioneers of group theory. By the way, it's customary to use additive notation for a group only when the group is known to be abelian.

Example 2. The five groups mentioned in the previous example are all abelian. To come up with non-abelian groups, it's necessary to get away from familiar number systems. For example, let S be any set. Then the set of all bijections on S (one to one functions from S *onto* S), also known as **permutations** on S, forms a group with composition as the group operation. (Associativity of composition is very easy to show, and the usual identity function and inverse functions serve as the identity and inverses in this group.) This group is nonabelian as long as S has at least three members. For instance, suppose $S = \mathbb{R}$, $f(x) = x + 1$ and $g(x) = 2x$. Then f and g are permutations on S, but $f \circ g \neq g \circ f$. Thus the group of permutations on $\mathbb{R}$ is not abelian.

Example 3. Along with permutation groups, the simplest nonabelian groups are groups of matrices. Let n be any positive integer. Then any two $n \times n$ matrices (with real coefficients, say) can be multiplied, and this operation is known to be associative. Furthermore, there is an $n \times n$ identity matrix, with 1's down the main diagonal (top left to bottom right) and 0's everywhere else. Not every $n \times n$ matrix has an inverse, but the set of *invertible* $n \times n$ matrices forms a group under multiplication. If $n > 1$, this group is not abelian. To test this, choose two 2×2 matrices A and B at random. In all likelihood, you will find that $AB \neq BA$.

Abelian groups are much more well-behaved and easy to understand than nonabelian groups. Another important distinction among groups is the distinction between finite and infinite groups. All of the groups mentioned so far in this appendix are infinite, except for the group of permutations on a finite set S. Finite groups are not necessarily easier to work with than infinite groups; in fact, the classification of finite nonabelian groups has been one of the thorniest problems of modern algebra. However, finite abelian groups are rather simple, as we will see shortly. The number of elements in a finite group is called its **order**.

Example 4. The most straightforward way to construct finite abelian groups is by using "clock arithmetic," or **modular arithmetic** as it is more precisely called. Imagine an ordinary dial clock, except that 0 rather than 12 appears at the top. (Logically, it makes at least as much sense to say the day begins at zero o'clock as twelve o'clock.) If the time now is nine, we know that the time five hours from now will be two o'clock, not fourteen o'clock. In other words, in clock addition we add numbers in the usual way, but then we subtract twelve if necessary to make sure the answer we get is a number that appears on the clock.

A standard clock has twelve numbers, but this idea can be generalized to clocks with any number of numbers. So, for each natural number n, let $A_n = \{0, 1, \ldots, n-1\}$. The group of **integers modulo** n, denoted $\mathbb{Z}_n$, is the set A_n together with the operation of "clock addition" described above. For instance, in $\mathbb{Z}_7$, $2 + 2 = 4$, $4 + 3 = 0$, and

$6 + 4 = 3$. It is not hard to show that $\mathbb{Z}_n$ is an abelian group of order n. The identity of $\mathbb{Z}_n$ is 0. The inverse of 0 is 0, while the inverse of any other element x is $n - x$.

To state the main classification theorem for finite abelian groups, we need to define several important notions that are also discussed in Chapter 5, in the context of general algebraic structures:

Definitions. Let $G_i = (A_i, *_i)$ be a group, for $i = 1, 2$. A **homomorphism** from G_1 to G_2 is a function ϕ from A_1 to A_2 such that $\phi(x *_1 y) = \phi(x) *_2 \phi(y)$, for all x and y in A_1. A one-to-one onto homomorphism is called an **isomorphism**. Finally, two groups are called **isomorphic** if there is an isomorphism from one of them to the other.

A homomorphism is a "structure-preserving" function between groups or other algebraic structures. So an isomorphism is a one-to-one correspondence between two groups (more precisely, between their universes) that is structure-preserving. If two groups are isomorphic, they may be viewed as being "the same group, except possibly for how their elements are named." Isomorphic groups have exactly the same *mathematical* properties.

Definition. Let $G = (A, *)$ be a group and $B \subseteq A$. We say that B defines a **subgroup** of G if B contains e and is closed under $*$ and the inverse operation. Again, the subgroup isn't technically B but rather B together with the restriction of $*$ to $B \times B$, but it's common to be imprecise about this.

Example 5. For each fixed integer n, let $n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\}$ (not to be confused with $\mathbb{Z}_n$). Then it is easy to show that $n\mathbb{Z}$ defines a subgroup of $(\mathbb{Z}, +)$. In fact, these are the only subgroups of $(\mathbb{Z}, +)$. In contrast, it is not easy to describe all the subgroups of $(\mathbb{R}, +)$.

Exercise 1. Prove that all groups of the form $n\mathbb{Z}$, with $n \neq 0$, are isomorphic to each other.

Definition. Let $G = (A, *)$ be a group and $S \subseteq A$. Then there are three ways of defining what is meant by the subgroup of G **generated**

by S. It's the intersection of all subgroups of G that contain S, and also the smallest subgroup of G that contains S. More concretely, it's also the set of all elements of A that can be the interpretation of some term of the language of group theory (with symbols for $*$, the identity, and the inverse operation), with free variables assigned to elements of S. The equivalence of these definitions is implied by Corollaries 5.16 and 5.17 in Section 5.4.

Definitions. A group is said to be **finitely generated** (respectively, **cyclic**) if it is generated by some finite (respectively, one-element) set of its elements. The same terminology is applied to subgroups.

Proposition D.2. *Every cyclic group is isomorphic to the group of integers or to one of the groups $\mathbb{Z}_n$.*

Thus, cyclic groups are rather simple. In particular, $\mathbb{Z}$ is the unique infinite cyclic group, "up to isomorphism." Furthermore, we will soon see that cyclic groups are the main "building blocks" for a rather large category of groups.

Definition. Let $G_i = (A_i, *_i)$ be a group, for $i = 1, 2$. Their **direct product** $G_1 \times G_2$ is the group $(A_1 \times A_2, *)$, where $(u, v) * (x, y)$ is defined to be $(u *_1 x, v *_2 y)$. Similarly, we can define the direct product of three or more groups, or even an infinite collection of groups.

For example, if $G_1 = (\mathbb{Z}, +)$ and $G_2 = (\mathbb{R} - \{0\}, \cdot)$, then in $G_1 \times G_2$ we would have $(-4, 0.3) * (7, -5) = (3, -1.5)$.

Theorem D.3 (Classification of finitely generated abelian groups). *Every finitely generated abelian group is isomorphic to a direct product of a finite number of cyclic groups, with n being a power of a prime in each finite factor $\mathbb{Z}_n$. This representation is unique, except for the order of the factor groups.*

As a special case, every finite abelian group is isomorphic to a direct product of finite cyclic groups, with the same restriction on n and the same uniqueness condition as in the theorem.

Example 6. Suppose G is an abelian group of order 6. Then, since 2×3 is the only factorization of 6 into *powers* of primes, G must be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3$. The groups $\mathbb{Z}_3 \times \mathbb{Z}_2$ and $\mathbb{Z}_6$ are also isomorphic to G. By the way, the group of permutations on a set of three elements is a nonabelian group of order 6, and it is structurally the only nonabelian group of order 6. So there are exactly two groups of order 6, up to isomorphism.

Now suppose G is an abelian group of order 4. Then, according to the classification theorem, G could be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_4$. These two groups are not isomorphic, since $u + u$ is the identity for every u in $\mathbb{Z}_2 \times \mathbb{Z}_2$, but in $\mathbb{Z}_4$ we have $1 + 1 = 2 \neq 0$. (This is the typical sort of reasoning that shows groups are not isomorphic.) Thus, structurally, there are exactly two abelian groups of order 4. It is also simple to show that there are no nonabelian groups of this order.

Similarly, an abelian group of order 60 must be isomorphic to exactly one of $\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_4$ or $\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. For instance, $\mathbb{Z}_{60}$ looks like the former of these, while $\mathbb{Z}_{30} \times \mathbb{Z}_2$ is isomorphic to the latter.

The classification theorem for finitely generated abelian groups provides a very precise, clear way of describing these groups. When applied to finite abelian groups, it is very reminiscent of the fundamental theorem of arithmetic, except that here the "factoring" is based on powers of primes, not simply on primes.

Here are a few other concepts of group theory that are mentioned in the text: Let $G = (A, \cdot)$ be a group and $x \in A$. If there is a positive integer n such that $x^n = 1$, then the smallest such n is called the **order** of x. In this case, the cyclic subgroup of G generated by x consists of $\{1, x, x^2, \ldots, x^{n-1}\}$ and is isomorphic to $\mathbb{Z}_n$, so the order of x equals the order of the subgroup it generates. If there is no such n, x is said to have infinite order (and x generates a subgroup isomorphic to $\mathbb{Z}$).

A group in which every element has finite order is called a **torsion** group. Every finite group is torsion, as is every finite direct product of torsion groups. A group in which every element except the identity has infinite order is said to be **torsion-free**. The groups $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$

under addition are torsion-free, as is every direct product of torsion-free groups.

Finally, a group G is called **divisible** if "every element has an nth root, for every positive integer n." Symbolically, this can be written

$$\forall n \in \mathbb{Z}^+ \forall x \in G \exists y \in G(y^n = x).$$

But it's important to realize that this symbolic statement is not within the first-order language of a group, because n is not a variable for a group element, and group theory does not have exponential terms y^n. So an infinite axiom schema is required to express divisibility. A similar situation holds for the obvious attempts to axiomatize torsion groups and torsion-free groups. These limitations are discussed further in Section 5.7.

The term "divisible group" is more apt when the group operation is written additively, for then y^n becomes ny, and "has an nth root" becomes "is divisible by n." The additive groups $\mathbb{Q}$ and $\mathbb{R}$ are divisible, as is the multiplicative group $\mathbb{R}^+$. The additive group $\mathbb{Z}$ and the multiplicative group $\mathbb{Q}^+$ are not.

Rings and fields

Groups are the most important type of algebraic structure with a single binary operation. For the remainder of this appendix, we consider algebraic structures with two binary operations:

Definition. A **ring** is a set together with two binary operations on it (more formally, an ordered triple $(A, +, \cdot)$) satisfying these conditions:

1. The structure $(A, +)$ is an abelian group.
2. The operation $\cdot$ is associative.
3. The **distributive laws** hold: $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ and $(y + z) \cdot x = (y \cdot x) + (z \cdot x)$, for all x, y, and z in A.

Since a group has only one operation, the question of whether to use multiplicative or additive notation for a group is often a matter of taste. But a ring has two operations, and so it is almost universal to call

them addition and multiplication, as in this definition. Note that the distributive laws are the only properties that connect the two operations. Also, note that the definition of a ring requires much more of addition (all four conditions needed to be an abelian group) than it does of multiplication. For this reason, most of the particular types of rings that are considered are based on putting more conditions on multiplication. Here are the definitions of some of these types of rings:

Definitions. A **commutative ring** is a ring in which multiplication is commutative: $xy = yx$ for all x and y in A.

A **ring with unity** is a ring with a nonzero multiplicative identity: an element 1 such that $1 \neq 0$ and $x \cdot 1 = 1 \cdot x = x$, for all x in A. As with groups, this identity element is easily shown to be unique.

A **division ring** is a ring with unity in which every nonzero element has a multiplicative inverse or **reciprocal**: in symbols, $\forall x \neq 0\, \exists y(xy = yx = 1)$. Whenever an element x in a ring with unity has a reciprocal, that reciprocal is unique and we denote it x^{-1}.

A **field** is a commutative division ring.

Definitions. If x and y are nonzero elements of a ring such that $xy = 0$, then x and y are (each) called **zero-divisors**. An **integral domain** is a commutative ring with unity, with no zero-divisors.

Example 7. Most familiar number systems which have addition and multiplication operations are rings. Examples include $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, and $\mathbb{Z}$. The first three of these are fields, which also implies that they are integral domains. On the other hand, $\mathbb{Z}$ is an integral domain but not a field. In fact, 1 and -1 are the only elements of $\mathbb{Z}$ that have reciprocals.

The number system $\mathbb{N}$ has addition and multiplication, but it is not a ring because some (in fact, almost all) elements in it don't have additive inverses.

We have called addition and multiplication the two main operations in a ring. But in grade school, we learn that there are four basic operations of arithmetic: addition, subtraction, multiplication, and division. In higher mathematics, subtraction and division are viewed as

offshoots of the two basic operations and the inverse properties that relate to them. In other words, in any ring, $x - y$ means $x + (-y)$, and in a commutative ring with unity, x/y means $x \cdot y^{-1}$, provided that y^{-1} exists.

Example 8. The simplest examples of noncommutative rings are probably rings of matrices. Let R be a ring with unity. For each natural number n, the set of $n \times n$ matrices whose coefficients are in R, with the usual operations of matrix addition and multiplication, is also a ring with unity. (See the related discussion in Example 3.) But this ring is not commutative if $n > 1$. These noncommutative rings are also not division rings, since there are many nonzero square matrices that are not invertible.

Example 9. The simplest example of a ring without unity is the ring of even integers, with the usual operations. More generally, for each integer $n > 1$ the ring $n\mathbb{Z}$, whose elements are all multiples of n, is a commutative ring without unity. These rings also have no zero-divisors, so they are "almost" integral domains.

Exercise 2. Prove that the rings $m\mathbb{Z}$ and $n\mathbb{Z}$ are isomorphic if and only if $m = \pm n$. (Compare this exercise to the similar one about the groups $n\mathbb{Z}$.)

Exercise 3. Find a noncommutative ring without unity.

Example 10. The groups $\mathbb{Z}_n$ were defined in Example 4. These number systems become rings if we include the operation of **multiplication modulo** n that is analogous to addition modulo n. For instance, if we start at midnight and go five ten-hour periods into the future, the time will not be fifty o'clock. It will be two o'clock. We can determine this by first computing that $5 \times 10 = 50$, and then computing the *remainder* when 50 is divided by 12. So, in $\mathbb{Z}_{12}$, $5 \cdot 10 = 2$ (while $5 + 10 = 3$). Similarly, in $\mathbb{Z}_8$, $3 \cdot 7 = 5$. Arithmetic modulo n may also be viewed as "units place" arithmetic in base n.

It is easy to show that $\mathbb{Z}_n$ is a commutative ring with unity for $n > 1$. Beyond that, two different cases arise. If n is composite, $\mathbb{Z}_n$

cannot be an integral domain. For example, $2 \cdot 2 = 0$ in $\mathbb{Z}_4$, and $2 \cdot 3 = 0$ in $\mathbb{Z}_6$.

On the other hand, $\mathbb{Z}_p$ must be an integral domain if p is prime. For instance, zero-divisors in $\mathbb{Z}_7$ would be a pair of positive integers less than 7 whose product is a multiple of 7. This would clearly contradict the primality of 7. Furthermore, one of the important basic theorems of number theory says, in essence, that every nonzero element of $\mathbb{Z}_p$ (when p is prime) has a reciprocal. For instance, in $\mathbb{Z}_7$ we have $1^{-1} = 1$, $2^{-1} = 4$, $3^{-1} = 5$, and $6^{-1} = 6$. In other words, these rings $\mathbb{Z}_p$ are actually fields, and they are the simplest examples of finite fields.

In particular, consider $\mathbb{Z}_2$. This structure has only two elements, 0 and 1, with completely standard addition and multiplication except that $1 + 1 = 0$. Yet, somehow, this number system satisfies all the standard properties of addition, subtraction, multiplication, and division.

The fields $\mathbb{Z}_p$ have **finite characteristic**, meaning that some integer multiple of 1 (formally obtained by adding 1 to itself repeatedly) equals 0. For instance, $\mathbb{Z}_2$ has characteristic 2, since $1+1 = 0$ in it. Similarly, $\mathbb{Z}_p$ has characteristic p. It is easy to show that the characteristic of such a field—the smallest integer multiple of 1 that equals 0—must be prime. Trivially, every finite field has finite characteristic. But there are also infinite fields of finite characteristic.

Fields that do not have finite characteristic are said, perhaps illogically, to have **characteristic zero**. The familiar fields $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are of this type.

The notions of **subrings** and **subfields** are defined in the same way as subgroups. These terms can be used in "hybrid" ways: one can refer to a subring of a field, or a subfield of a ring, or even a subgroup of the additive group of a ring, etc.

Every field K has a smallest subfield, called its **prime field**. It is, as usual, the intersection of all subfields of K. If K has characteristic p (respectively, 0), then its prime field is the unique subfield of K that is isomorphic to $\mathbb{Z}_p$ (respectively, $\mathbb{Q}$).

Let F be a subfield of a field K. An element x of K is called **algebraic** over F if it is a root (or "zero") of some nonzero polynomial

with coefficients in F. Otherwise, x is **transcendental** over F. If every x in K is algebraic over F, then K is an **algebraic extension** of F.

When these terms are applied to complex (including real) numbers, the words "over $\mathbb{Q}$" are generally understood. So all rational numbers are algebraic, but so are all numbers that can be written using rational numbers and radicals. For instance, $\sqrt{5}$ is algebraic because it is a root of $x^2 - 5$. It's less obvious that a number like $\sqrt{7} + \sqrt[3]{10}$ is algebraic, but it is. Abel ushered in the modern age of algebra by proving that the converse of this is false: not every algebraic number is expressible by radicals. As Chapter 8 mentions, it took well into the nineteenth century to show that transcendental numbers exist. The most famous ones are π and e.

A field K is said to be **algebraically closed** if every polynomial with coefficients in K has a root in K. Finally, if K is algebraically closed and it is an algebraic extension of some subfield F, then K is called an **algebraic closure** of F. Here is one of the most important results of field theory, whose proof requires the axiom of choice:

Theorem D.4. *Every field F has an algebraic closure, which is unique "up to isomorphism over F." In other words, if K_1 and K_2 are both algebraic closures of F, then there is an isomorphism between K_1 and K_2 that is the identity on F.*

Example 11. The fundamental theorem of algebra says precisely that the field $\mathbb{C}$ is algebraically closed. Furthermore, it is easy to show that $\mathbb{C}$ is an algebraic extension of $\mathbb{R}$; in fact, every complex number is a root of a polynomial, with real coefficients, of degree at most 2. Therefore, $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$.

On the other hand, $\mathbb{C}$ is an not algebraic extension of $\mathbb{Q}$, since $\mathbb{C}$ includes transcendental numbers. The algebraic closure of $\mathbb{Q}$ is, almost by definition, the field of complex algebraic numbers.

Ordered algebraic structures

In the basic algebra of the real numbers and other familiar number systems, one considers inequalities as well as equations. In other words,

these algebraic structures have orderings defined on them. It is fruitful to generalize this idea:

Definition. An **ordered group** is a triple $(A, +, <)$ satisfying these conditions:

1. $(A, +)$ is an abelian group.
2. $<$ is an (irreflexive) total ordering on A.
3. Whenever x, y, and z are in A and $x < y$, then $x + z < y + z$.

Note that condition (3) is familiar from high-school algebra: an inequality is preserved if you add the same number to both sides of it.

Definition. An **ordered ring** is a 4-tuple $(A, +, \cdot, <)$ satisfying these conditions:

1. $(A, +, \cdot)$ is a commutative ring.
2. $(A, +, <)$ is an ordered group.
3. Whenever x, y, and z are in A, $x < y$, and $z > 0$, then $xz < yz$.

Here we see another elementary property: an inequality is preserved if you multiply both sides by the same positive number.

Example 12.

(a) $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are ordered rings, with the usual operations and ordering. The last two are also fields, so they are called **ordered fields**.

(b) It is easy to show that there is no ordering on a finite group or ring that will turn it into an ordered group or ring. So, for example, the groups $\mathbb{Z}_n$ cannot be ordered.

(c) The field $\mathbb{C}$ also cannot be ordered: it is not hard to show that, in any ordered field, $x^2 \geq 0$ for every x. Therefore $1 = 1^2 > 0$, and so $-1 < 0$. But in $\mathbb{C}$, $i^2 = -1$. (See the discussion of formally real fields in Section 5.5.)