Math 533 Winter 2021, Lecture 2: Rings and ideals

website: `https://www.cip.ifi.lmu.de/~grinberg/t/21w/`

1. Rings and ideals (cont'd)

1.1. Calculating in rings

The intuition for commutative rings is essentially that all computations that can be performed with the operations $+$, $-$ and $\cdot$ on integers can be similarly made in any commutative ring. To some extent, this holds also for general (noncommutative) rings.

For instance, if $a_1, a_2, \ldots, a_n$ are n elements of a ring, then the sum $a_1 + a_2 + \cdots + a_n$ is well-defined, and can be computed by adding the elements $a_1, a_2, \ldots, a_n$ together in any order. More generally, finite sums of the form $\sum_{s \in S} a_s$ are defined when the a_s belong to a ring, and behave just like finite sums of numbers.[1] The same holds for finite products when the ring is commutative. If the ring is not commutative, then finite products in a specified order – like $a_1 a_2 \cdots a_n$ – are still well-defined, but unordered finite products – like $\prod_{s \in S} a_s$ – are not, unless you have "local commutativity" (i.e., the a_s commute with each other).[2]

In any ring, subtraction satisfies the rules you would expect: For any two elements a, b of a ring, we have

$$\begin{aligned} (-a)\, b &= a\, (-b) = -(ab)\,; \\ (-a)\, (-b) &= ab; \\ (-1)\, a &= -a. \end{aligned}$$

See [DF, §7.1, Proposition 1] for the easy proofs. Furthermore, any three elements a, b, c of a ring satisfy the "subtractive distributivity laws"

$$a\,(b-c) = ab - ac \qquad \text{and} \qquad (a-b)\,c = ac - bc.$$

(These follows easily from the standard distributivity laws that are part of the ring axioms.)

[1] It should be kept in mind that empty sums (i.e., sums of the form $\sum_{s \in \varnothing} a_s$) are defined to equal the zero of the ring.

[2] It should be kept in mind that empty products (i.e., products of the form $\prod_{s \in \varnothing} a_s$) are defined to equal the unity of the ring.

If n is an integer and a is an element of a ring R, then we define an element na of R by

$$na = \begin{cases} \underbrace{a+a+\cdots+a}_{n \text{ addends}}, & \text{if } n \geq 0; \\ -\left(\underbrace{a+a+\cdots+a}_{-n \text{ addends}}\right), & \text{if } n < 0 \end{cases}.$$

If n is a nonnegative integer and a is an element of a ring R, then a^n is a well-defined element of R (namely, $a^n = \underbrace{a \cdot a \cdot \cdots \cdot a}_{n \text{ factors}}$). In particular, applying this definition to $n = 0$, we obtain

$$a^0 = (\text{empty product}) = 1 \qquad \text{for each } a \in R.$$

Thus we can scale elements of a ring by integers, and take them to nonnegative integer powers. The identities you would expect are satisfied for these operations: For example, for any $a, b \in R$ (with R being a ring) and any $n, m \in \mathbb{Z}$, we have

$$\begin{aligned} (n+m)\, a &= na + ma; \\ n\,(a+b) &= na + nb; \\ (nm)\, a &= n\,(ma)\,; \\ (-1)\, a &= -a; \\ a^{n+m} &= a^n a^m; \\ a^{nm} &= (a^n)^m\,. \end{aligned}$$

Also,

$$1^n = 1 \qquad \text{for } n \in \mathbb{N};$$

$$0^n = \begin{cases} 0, & \text{if } n > 0; \\ 1, & \text{if } n = 0 \end{cases} \qquad \text{for } n \in \mathbb{N}.$$

Moreover, if $a, b \in R$ satisfy $ab = ba$, then

$$a^i b^j = b^j a^i \qquad \text{for } i, j \in \mathbb{N}$$

and

$$(ab)^n = a^n b^n \qquad \text{for } n \in \mathbb{N}$$

and (the binomial formula)

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \qquad \text{for } n \in \mathbb{N}.$$

All of this is proved just as for numbers.

Here are things that behave less familiar:

- It is not true that $a \neq 0$ and $b \neq 0$ implies $ab \neq 0$. This fails in the ring $\mathbb{Z}/6$ (for example, you can pick $a = \overline{2}$ and $b = \overline{3}$ to get $ab = \overline{2} \cdot \overline{3} = \overline{2 \cdot 3} = \overline{6} = \overline{0}$, even though a and b are $\neq \overline{0}$) and in matrix rings like $\mathbb{Z}^{2\times 2}$ (here you can pick $a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $b = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ to get $ab = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, even though a and b are not the zero matrix).
- It is not true that $ab = 1$ implies $ba = 1$. This would be true in the classical matrix rings $\mathbb{R}^{n\times n}$ and $\mathbb{C}^{n\times n}$, in any commutative ring (for obvious reasons), and in any finite ring (for less obvious reasons), but may fail in arbitrary rings. (Counterexamples are not easy to find; see [DF, §7.1, exercise 30 (a)] for one.)

1.2. Zero divisors and integral domains ([DF, §7.1])

Definition 1.2.1. An element of a ring R is said to be **nonzero** if it is $\neq 0$. (Here, 0 means 0_R.)

Definition 1.2.2. Let R be a commutative ring. A nonzero element $a \in R$ is called a **zero divisor** if there is a nonzero $b \in R$ such that $ab = 0$.

This definition is slightly controversial: Some people don't require a to be nonzero. Thus, to them, 0 is a zero divisor unless R is trivial. It's not a very well-conceived definition, but it's not used very much either.

Definition 1.2.3. Let R be a commutative ring. Assume that $0 \neq 1$ in R. (By this, we mean $0_R \neq 1_R$; that is, the zero and the unity of R are distinct. In other words, we assume that the ring R is not trivial.) We say that R is an **integral domain** if all nonzero $a, b \in R$ satisfy $ab \neq 0$.

Equivalently, a commutative ring R with $0 \neq 1$ (in R, that is) is an integral domain if and only if R has no zero divisors.

Examples:

- The rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are integral domains.
- The ring $\mathbb{Z}/n$ is an integral domain if and only if n is 0 or a prime or minus a prime. We will prove this later.
- The ring $\mathbb{S}'$ from the last lecture (i.e., the ring $\mathbb{S}$ whose elements are numbers of the form $a + b\sqrt{5}$ with $a, b \in \mathbb{Q}$, with multiplication $*$ given by $\left(a + b\sqrt{5}\right) * \left(c + d\sqrt{5}\right) = ac + bd\sqrt{5}$) is not an integral domain, since it has $1 * \sqrt{5} = 0$.
- The ring of all functions from $\mathbb{Q}$ to $\mathbb{Q}$ is not an integral domain, since any two functions with disjoint supports will multiply to 0. (For a specific example, we have $\delta_0 \cdot \delta_1 = 0$, where δ_y (for $y \in \mathbb{Q}$) is the function that sends y to 1 and all other rational numbers to 0.)

1.3. Units and fields ([DF, §7.1])

Definition 1.3.1. Let R be a ring.

(a) An element $a \in R$ is said to be a **unit** of R (or **invertible** in R) if there exists a $b \in R$ such that $ab = ba = 1$. In this case, b is unique and is known as the **inverse** (or **multiplicative inverse**, or **reciprocal**) of a, and is written a^{-1}.

(b) We let $R^\times$ denote the set of all units of R.

A few comments:

- It goes without saying that the "1" refers to the unity of the ring R.
- We required $ab = ba = 1$ rather than merely $ab = 1$ because R is not necessarily commutative. When R is commutative, of course, $ab = 1$ suffices.
- Why is b unique in part **(a)** of the definition? Because if b_1 and b_2 are two such b's (for the same a), then $ab_1 = b_1 a = 1$ and $ab_2 = b_2 a = 1$, so that $b_1 \underbrace{ab_2}_{=1} = b_1 1 = b_1$ and thus $b_1 = \underbrace{b_1 a}_{=1} b_2 = 1b_2 = b_2$. This is the exact same argument that proves the uniqueness of inverses in a group.
- Don't confuse "unit" (= invertible element) with "unity" (= neutral element for multiplication). The unity is always a unit, but not vice versa!
- Some people write R^* or R^x for $R^\times$.

Examples of units:

- The units of the ring $\mathbb{Q}$ are all nonzero elements of $\mathbb{Q}$. (This is because every nonzero element of $\mathbb{Q}$ has a reciprocal, and this reciprocal again lies in $\mathbb{Q}$.) The same holds for $\mathbb{R}$ and for $\mathbb{C}$.
- The units of the ring $\mathbb{Z}$ are 1 and -1 (with inverses 1 and -1, respectively). No other integer is a unit of $\mathbb{Z}$. For example, 2 has an inverse $\frac{1}{2}$ in $\mathbb{Q}$, but not in $\mathbb{Z}$.
- The units of the matrix ring $\mathbb{R}^{n\times n}$ are the invertible $n \times n$-matrices. You have seen many ways to characterize them in your linear algebra class. You might even remember that the set $\left(\mathbb{R}^{n\times n}\right)^\times$ of these units is known as the **n-th general linear group** of $\mathbb{R}$, and is called $\mathrm{GL}_n(\mathbb{R})$ or $\mathrm{GL}(n, \mathbb{R})$.
- In the ring of all functions from $\mathbb{Q}$ to $\mathbb{Q}$, the units are the functions that never vanish (i.e., that don't take 0 as a value). Inverses can be computed pointwise.

Our next example we state as a proposition:

Proposition 1.3.2. Let $n \in \mathbb{Z}$.

(a) The units of the ring $\mathbb{Z}/n$ are precisely the residue classes $\overline{a}$ with a coprime to n.

(b) Let $a \in \mathbb{Z}$. Then, $\overline{a}$ is a unit of $\mathbb{Z}/n$ if and only if a is coprime to n.

Proof. We begin by proving part **(b)**, which is the stronger claim. (Part **(a)** will then easily follow.)

(b) $\Longleftarrow$: Assume that $a \in \mathbb{Z}$ is coprime to n. Then, Bezout's theorem tells us that there exist $x, y \in \mathbb{Z}$ with $xa + yn = 1$. Thus, $xa \equiv xa + yn = 1 \bmod n$, so that $\overline{xa} = \overline{1}$ in $\mathbb{Z}/n$. Hence, $\overline{x} \cdot \overline{a} = \overline{xa} = \overline{1}$ in $\mathbb{Z}/n$. Since the ring $\mathbb{Z}/n$ is commutative, this shows that $\overline{a}$ is invertible (with inverse $\overline{x}$). In other words, $\overline{a}$ is a unit of $\mathbb{Z}/n$.

$\Longrightarrow$: Conversely, assume that $\overline{a}$ is a unit of $\mathbb{Z}/n$. Thus, $\overline{a}$ has an inverse $\overline{b} \in \mathbb{Z}/n$. This inverse $\overline{b}$ satisfies $\overline{ab} = \overline{1}$; in other words, $ab \equiv 1 \bmod n$. But this easily yields that[3] $\gcd(ab, n) = \gcd(1, n) = 1$. In other words, ab is coprime to n. Hence, a is coprime to n as well (since any common divisor of a and n must be a common divisor of ab and n).

(a) This follows easily from part **(b)**. □

Theorem 1.3.3. Let R be a ring. Then, the set $R^\times$ is a multiplicative group. More precisely: $(R^\times, \cdot, 1)$ is a group.

Proof. It suffices to show the following facts:

1. The unity 1 of R belongs to $R^\times$.
2. If $a, b \in R^\times$, then $ab \in R^\times$.
3. If $a \in R^\times$, then a has an inverse in $R^\times$.

All other group axioms for $R^\times$ follow from the ring axioms of R. So let us prove these three facts.

Proof of Fact 1: Fact 1 is obvious (as 1 has inverse 1).

Proof of Fact 2: Let $a, b \in R^\times$. Thus, the elements a, b are units, and thus have inverses a^{-1}, b^{-1}, respectively. These satisfy $aa^{-1} = a^{-1}a = 1$ and $bb^{-1} = b^{-1}b = 1$. Now, $a \underbrace{bb^{-1}}_{=1} a^{-1} = aa^{-1} = 1$ and $b^{-1} \underbrace{a^{-1}a}_{=1} b = b^{-1}b = 1$, so that ab is invertible as well (with inverse $b^{-1}a^{-1}$). That is, $ab \in R^\times$. This proves Fact 2.

Proof of Fact 3: Let $a \in R^\times$. Thus, a has an inverse a^{-1} in R. This inverse a^{-1}, in turn, has an inverse (namely, a), and thus also lies in $R^\times$. Hence, a has an inverse in $R^\times$. This proves Fact 3. □

[3] We are using the fact that if u and v are two integers satisfying $u \equiv v \bmod n$, then $\gcd(u, n) = \gcd(v, n)$. This is just a restatement of the classical result that the gcd of two integers does not change if we add a multiple of one to the other.

The group $R^\times$ from the above theorem is known as the **group of units** of R.

Theorem 1.3.4 (Shoe-sock theorem)**.** Let R be a ring. Let a, b be two units of R. Then, ab is a unit of R, and its inverse is $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. See the proof of Fact 2 in the preceding proof. □

Definition 1.3.5. Let R be a commutative ring. Assume that $0 \neq 1$ in R. We say that R is a **field** if every nonzero element of R is a unit.

Examples:

- The rings $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields. The ring $\mathbb{Z}$ is not (since 2 is not a unit).
- The ring $\mathbb{S}$ of all real numbers of the form $a + b\sqrt{5}$ with $a, b \in \mathbb{Q}$ (see the previous lecture) is a field, too. Indeed, the inverse of a nonzero element $a + b\sqrt{5}$ is

$$\left(a + b\sqrt{5}\right)^{-1} = \frac{1}{a + b\sqrt{5}} = \frac{a - b\sqrt{5}}{a^2 - b^2 \cdot 5} = \frac{a}{a^2 - 5b^2} + \frac{-b}{a^2 - 5b^2}\sqrt{5}$$

  (the denominators here are nonzero because $a + b\sqrt{5} \neq 0$ entails $a^2 - 5b^2 \neq 0$). So this is why they taught you rationalizing denominators in high school!
- The Hamiltonian quaternions $\mathbb{H}$ are not a field, but for a stupid reason: they are noncommutative. Otherwise, they would be a field. A noncommutative ring in which each nonzero element is invertible is called a **division ring** or **skew-field**.
- Let n be a positive integer. The ring $\mathbb{Z}/n$ is a field if and only if n is prime. (We will prove this below.)

1.4. Fields and integral domains: some connections ([DF, §7.1])

Proposition 1.4.1. (a) Every field is an integral domain.
(b) Every **finite** integral domain is a field. (Here, of course, "finite" means "finite as a set".)

Proof. **(a)** Let F be a field. Let $a, b \in F$ be nonzero. We must show that ab is nonzero.

Indeed, a and b are nonzero, and thus are units (since F is a field). Thus, they have inverses a^{-1} and b^{-1}.

Now, if we had $ab = 0$, then we would have $\underbrace{ab}_{=0} b^{-1}a^{-1} = 0$, which would yield $0 = a\underbrace{bb^{-1}}_{=1}a^{-1} = aa^{-1} = 1$, which would contradict the fact that $0 \neq 1$ in F (since F is a field). Thus, we cannot have $ab = 0$. In other words, ab is nonzero. This completes the proof of **(a)**.

(b) Let R be a **finite** integral domain. We must show that R is a field.

Let $a \in R$ be nonzero. We must show that a is a unit.

Since R is an integral domain, we know that $ab \neq 0$ for any $b \neq 0$. Thus, $ax \neq ay$ for any two distinct elements x and y of R (because if x and y are two distinct elements of R, then $x - y \neq 0$, and thus the previous sentence yields $a(x-y) \neq 0$; but this rewrites as $ax - ay \neq 0$, so that $ax \neq ay$). In other words, the map

$$R \to R, \qquad x \mapsto ax$$

is injective. Hence, this map is also bijective (since any injective map between two **finite** sets of the **same size** is bijective – this is one of the Pigeonhole Principles). Thus, in particular, this map is surjective, and hence takes 1 as a value. In other words, there exists an $x \in R$ such that $ax = 1$. Since R is commutative, this x must be an inverse of a, and thus we conclude that a is a unit. This finishes the proof of **(b)**. □

Without the word "finite", Proposition 1.4.1 **(b)** would not be true; for instance, $\mathbb{Z}$ is an integral domain but no field. The polynomial ring $\mathbb{R}[x]$ (consisting of univariate polynomials with real coefficients) is another example of an integral domain that is not a field. (We will prove this later.)

Our above study of units of $\mathbb{Z}/n$ lets us now easily obtain the following:

Corollary 1.4.2. Let n be a positive integer. Then, the following chain of equivalences holds:

$$(\mathbb{Z}/n \text{ is an integral domain}) \iff (\mathbb{Z}/n \text{ is a field}) \iff (n \text{ is prime}).$$

Proof. The first of the two $\iff$ signs follows from Proposition 1.4.1 (since $\mathbb{Z}/n$ is finite). Let's now prove the second.

$\Longrightarrow$: Assume that $\mathbb{Z}/n$ is a field. Then, the $n-1$ residue classes $\overline{1}, \overline{2}, \ldots, \overline{n-1}$ are units of $\mathbb{Z}/n$ (since they are nonzero). Hence, the $n-1$ integers $1, 2, \ldots, n-1$ are coprime to n (by Proposition 1.3.2 **(b)**). Hence, n is either 1 or prime. However, if n was 1, then we would have $\overline{0} = \overline{1}$, which would mean that $0 = 1$ in $\mathbb{Z}/n$; but this is forbidden for a field. Thus, n cannot be 1, and therefore must be prime.

$\Longleftarrow$: Assume that n is prime. Then, $n > 1$, so that $\overline{0} \neq \overline{1}$. That is, $0 \neq 1$ in $\mathbb{Z}/n$. Furthermore, if $\overline{a}$ (for some integer a) is a nonzero element of $\mathbb{Z}/n$, then the integer a is not divisible by n (since $\overline{a}$ is nonzero), so that a is coprime to n (since n is prime), and this entails (by Proposition 1.3.2 **(b)**) that $\overline{a}$ is a unit of

$\mathbb{Z}/n$. So we have shown that every nonzero element of $\mathbb{Z}/n$ is a unit. In other words, $\mathbb{Z}/n$ is a field. □

Back to the general case. Rings have addition, subtraction and multiplication; but we can also divide two elements of a ring, as long as the denominator (i.e., the element we are dividing by) is a unit. If the ring is noncommutative, this is somewhat complicated by the fact that there are two kinds of division ("left" and "right" division); however, for commutative rings, it is as simple as for numbers:

Definition 1.4.3. Let R be a commutative ring. Let $a \in R$ and $b \in R^\times$. Then, $\dfrac{a}{b}$ means the element $ab^{-1} = b^{-1}a \in R$. This element is also written a/b, and is called the **quotient** of a by b. The operation $(a, b) \mapsto a/b$ is called **division**.

Thus, in a field, we can divide by any nonzero element.

Division satisfies the rules you would expect: If R is a commutative ring, and if $a, c \in R$ and $b, d \in R^\times$, then

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}; \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Division undoes multiplication: Three elements $a \in R$, $b \in R^\times$ and $c \in R$ satisfy $\dfrac{a}{b} = c$ if and only if $a = bc$.

1.5. Subrings ([DF, §7.1])

Groups have subgroups; vector spaces have subspaces (and so do topological spaces, although the two notions have little in common). Not surprisingly, the same is true for rings, and you can guess the definition:

Definition 1.5.1. Let R be a ring. A **subring** of R is a subset S of R such that

- $a + b \in S$ for any $a, b \in S$;
- $ab \in S$ for any $a, b \in S$;
- $-a \in S$ for any $a \in S$;
- $0 \in S$ (where the 0 means the zero of R);
- $1 \in S$ (where the 1 means the unity of R).

The five conditions in Definition 1.5.1 are called the "**subring axioms**". The first of these five axioms is often reformulated as "S is closed under addition"; the second then becomes "S is closed under multiplication"; the third becomes

"S is closed under negation". Thus, a subring of a ring is a subset that is closed under addition, closed under multiplication, closed under negation, and contains the zero and the unity.

The following is essentially obvious:

Proposition 1.5.2. Let S be a subring of a ring R. Then, S automatically is a ring in its own right (with its operations $+$ and $\cdot$ obtained by restricting the corresponding operations of R, and with its elements 0 and 1 passed down from R).

Here are some examples of subrings:

- From the classical construction of the number systems, you know that $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. Each of these three "$\subseteq$" signs can be strengthened to "is a subring of" (for example, $\mathbb{Z}$ is a subring of $\mathbb{Q}$).
- We can extend this chain further to the right: $\mathbb{C}$ is a subring of $\mathbb{H}$ (the quaternions).
- However, we **cannot** extend this chain to the left: The only subring of $\mathbb{Z}$ is $\mathbb{Z}$ itself. Indeed, a subring of $\mathbb{Z}$ would have to contain 0 and 1 (by definition), thus also any sum of the form $1+1+\cdots+1$ (since a subring is closed under addition), i.e., any positive integer, and therefore also any negative integer (since it is closed under negation), and thus any integer. But this means it is $\mathbb{Z}$.

  This would be different if we used [DF]'s definitions. For example, the nonunital ring $2\mathbb{Z}$ is a subring of $\mathbb{Z}$ in [DF]'s sense.
- There are lots of rings between $\mathbb{Z}$ and $\mathbb{Q}$ (that is, rings $\mathbb{B}$ such that $\mathbb{Z}$ is a subring of $\mathbb{B}$ and $\mathbb{B}$ in turn is a subring of $\mathbb{Q}$). You will see some of these in exercise 1 on homework set #1.
- There are myriad rings between $\mathbb{Q}$ and $\mathbb{R}$. For example, the ring $\mathbb{S}$ from the previous lecture is one of these.
- There are no rings between $\mathbb{R}$ and $\mathbb{C}$. That is, if a subring of $\mathbb{C}$ contains $\mathbb{R}$ as a subring, then this subring must be either $\mathbb{R}$ or $\mathbb{C}$ itself. This is not hard to prove (but I won't do so here).
- There are rings between $\mathbb{Z}$ and $\mathbb{C}$ that are neither subrings nor "superrings" of $\mathbb{R}$. A particularly important one is the ring $\mathbb{Z}[i]$ of **Gaussian integers**. A **Gaussian integer** is a complex number of the form $a+bi$ where a and b are integers (and where i is the imaginary unit $\sqrt{-1}$). For example, $3+5i$ and $-7+8i$ are Gaussian integers. It is easy to see that $\mathbb{Z}[i]$ is indeed a subring of $\mathbb{C}$, and of course $\mathbb{Z}$ is a subring of $\mathbb{Z}[i]$. But $\mathbb{Z}[i]$ is not an intermediate stage on the $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ "chain"; it is a "detour".

Likewise, there is a ring $\mathbb{Q}[i]$ of **Gaussian rationals**, which are defined just as Gaussian integers but using rational numbers (instead of integers) for a and b. This ring $\mathbb{Q}[i]$ is sandwiched between $\mathbb{Q}$ and $\mathbb{C}$.

- Recall the ring of functions from $\mathbb{Q}$ to $\mathbb{Q}$. Similarly, there is a ring of functions from $\mathbb{R}$ to $\mathbb{R}$. The latter has a subring consisting of all **continuous** functions from $\mathbb{R}$ to $\mathbb{R}$. To see that this is indeed a subring, you need to show that the sum and the product of two continuous functions are continuous, and that the constant-0 and constant-1 functions are continuous.

Beware that [DF] does **not** require $1 \in S$ for a subring, because [DF] does not require rings to have a 1 in the first place. This is a confusing point, because it is possible that S and R are two rings in our sense (i.e., they both have unities), and S is a subring of R in [DF]'s sense (i.e., S satisfies our definition of a subring, minus the "$1 \in S$" axiom), but not a subring of R in our sense (because its unity is not the unity of R). For example, the zero ring is a subring of $\mathbb{Z}$ in [DF]'s sense, but not in ours (since the unity of the zero ring is the number 0). Alas, there are less pathological examples, too, so this isn't something you can ignore. For example, you can pretend that each 2×2-matrix is secretly a 3×3-matrix by inserting a zero row at the bottom and a zero column at the right (i.e., identifying each 2×2-matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with the 3×3-matrix $\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{pmatrix}$; note that I am not saying you **should** do that), and this makes $\mathbb{R}^{2\times 2}$ a subring of $\mathbb{R}^{3\times 3}$ in [DF]'s sense, but not in ours. Of course, this is one of the situations where you really need subscripts under the "1" to avoid confusing different unities.