Fundamental issues of abstraction
UTK – M351 – Algebra I
Jochen Denzler

This is in particular for those of you who find the mere list of field and ring axioms "abstract and confusing" already from the beginning.

A Parable: The FBI puts out a poster: WANTED FOR ⟨whatever⟩: John Doe, and a picture. They seize somebody who matches the picture and is otherwise suspected for the charge. He says: "I can't be the guy: you were looking for John Doe, but my name is Charly Miller." Pretty dumb excuse, isn't it? John Doe was not meant as the name of one particular individual, but represents an unknown (unspecified) name. A certain man (identified by a drivers license as named John Doe; his SSN is 123-45-6789) complains since he has nothing to do with the charges by the FBI. A dimwit. *His* name John Doe *is* the name of an individual and thus distinct from the "John Doe" on the FBI poster. Distinct means they are not necessarily the same (even though the person John Doe (SSN 123-45-6789) might just happen to be the wanted man, by a quirky accident).

Abstract Algebra:
In the axiom about the identity (or neutral) element for addition, which reads:

$$\text{There is some element } 0 \in X \text{ such that for every } a \in X \text{ it holds } a + 0 = 0 + a = a \quad (N+)$$

the '0' is like the FBI's 'John Doe'. Expanded version of the axiom: There is some element in X (we'll call it 0), such that etc.

Of course we call it 0 because it plays a similar role like the number 0 plays among the real numbers. Like the FBI thinks John Doe is kind of a 'typical name' for suspects living here. They won't call their unidentified suspects Maximilian Hinterhuber.

For those with some computer science background, the double use of symbols like 0 or 1 is the same issue as using 'metacharacters').

How to avoid thinking outside the box:
There is some benefit either way, but right at the beginning, you think 'out of the box' so naturally, that I must train your ability *not* to do it. Consider the set X of odd integers with the usual addition and multiplication of integers. I ask you: "Does it satisfy the axiom (N+)?" You answer: "No, because 0 (the neutral (alias identity) element for addition) is not an odd number, i.e., not in X." In some sense you are right, but you are already thinking outside the box. If you thought inside the box, you would say: "No, because there is no odd integer which, when added to any odd integer a, returns that same integer a." Rather than saying (outside the box) there is some 0, but it's disqualified, you say (inside the box): no there isn't any; I don't know nor care what's outside.

In some sense, I have already worsened the difficulty by posing the very problem: I seduced you to think outside the box, when I said "set X of odd integers with the usual addition…". Usual addition? In posing the very problem, *I* have thought outside the box. Inside the box there *is no* addition at all. $5 + 3$? No, not 8, because there is no such a thing called 8 in X. Strictly speaking I should not have given this problem. But I had to perpetrate such inaccuracy first, so I could teach you this distinction.

I asked to check the commutative law (C+). You say: True, order is not of essence when adding (any) integers; so in particular it is not of essence when adding odd integers. You are right of course, but you are again thinking outside the box. If you thought inside the box, you'd say: "(C+)? — not applicable! After all, how could I claim or deny $a + b = b + a$ if

the very + in this statement already fails to make sense."

An occasion where you would automatically think inside the box:
I gave you the example of the set $\{E, O\}$ with the definitions for $+$ and $\cdot$: $E + E = E$, $E + O = O + E = O$, $O + O = E$. $E \cdot O = O \cdot E = E \cdot E = E$, $O \cdot O = O$. This set does not come as a subset of some other larger set (unlike the previous example). In this case there is no "outside the box". If I give you a problem of this kind, I could not even make up one that fails to satify the closure axioms! If you want to check if (Inv+) holds in this set, you *cannot* start to find out what $-E$ would be and then see if it's one of E and O. Instead you have to examine the elements E and O and see which of them (if any) qualifies as an additive inverse of E.

These bloody closure axioms are a foggy obfuscation at this stage. They wouldn't even be in the textbooks (*), were it not for the sole purpose to adapt to preexistent difficulties with abstraction. — When I say: "There is a function $+ : X \times X \to X$ that maps (a, b) to (something called) $a + b$", then I have already included the (Clo+) axiom: it's buried in the X behind the arrow, here marked boldface for emphasis: $+ : X \times X \to \mathbf{X}$. No need to repeat it. (*) Note that our textbook honorably omits closure axioms. *I* perpetrated them viciously to connect this class to what we had in 300 and to clarify a fundamental point.

Subsets, Subrings and Sub⟨whatever⟩'s: If you already have a ring (like $\mathbb{Z}$, or $\mathbb{R}$) or a field (like $\mathbb{R}$), then you can consider a subset, as we did before, when considering the set of *odd* integers (subset of $\mathbb{Z}$), or the set of rationals, $\mathbb{Q}$ (subset of $\mathbb{R}$). Then you can ask if this subset is a ring (or a field) in its own right (with the $+$ and $\cdot$ defined already in the larger set). This is quite familiar to you, and it is in this spirit that you studied the problems which axioms are verified in $\mathbb{Z}$, in the set of even integers, in the set of odd integers, etc. When this is how you start your exploration, the laws of associativity, commutativity and distributivity become easy: They hold for *all* integers, therefore in particular for the odd ones. When the set you are studying comes as a *sub*set of some larger set, then it is appropriate to think 'out of the box' (as you naturally do in this case.)

So I did not mean above to say it's wrong to think of a certain set as a subset of a larger set (that is known to be a field, or a ring). I only mean to say you are on the *wrong track* if you can think of it *only* that way.

When you are studying a *subset* of a ring and ask if this subset is a ring in it's own right (and if so, we'll call it a subring), then closedness is *the* big issue. And other issues are whether the special objects whose existence is required by certain axioms are *in the subset* rather than only in the larger set 'outside the box'. Existence of something is required in the neutral (alias identity) element and inverse axioms; in this situation you will check if neutrals and inverses (known from the larger set) lie in the subset or not, but refer to known information from the larger set for associativity, commutativity, distributivity.

Overview list of axioms:

Field axioms: (from Hwk 1)

A set X with two functions $+ : X \times X \to X$ and $\cdot : X \times X \to X$ is called a field if the following properties hold:

Name	$+$	$\cdot$	convenient abbrev's
Closure	for all $a, b \in X$: $a + b \in X$	for all $a, b \in X$: $a \cdot b \in X$	(Clo $+$), (Clo $\cdot$) actually redundant
Associative Law	for all $a, b, c \in X$: $a+(b+c) = (a+b)+c$	for all $a, b, c \in X$: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$	(A $+$), (A $\cdot$)
Commutative Law	for all $a, b \in X$: $a + b = b + a$	for all $a, b \in X$: $a \cdot b = b \cdot a$	(C $+$), (C $\cdot$)
Existence of neutral (or identity) element	there is some $0 \in X$ st. $a + 0 = a$ for all a	there is some $1 \in X$ st. $a \cdot 1 = a$ for all a, and $1 \neq 0$	(N $+$), (N $\cdot$) or (Id $+$), (Id $\cdot$)
Existence of Inverse	for each $a \in X$, there is some $x \in X$ st. $a + x = 0$	for each $a \in X \setminus \{0\}$, there is some $x \in X$ st. $a \cdot x = 1$	(Inv $+$), (Inv $\cdot$)
Distributive Law	for all $a, b, c \in X$: $a \cdot (b + c) = a \cdot b + a \cdot c$		(D)

Notes: • 'st.' means 'such that'

• When we say "for each $a \in X$, there is some $x \in X$ st. $a + x = 0$", we mean that x may depend on a. (You were expected to know this already from 300, but I taught 300 twice already `;-)`

Ring axioms:

A set X with two functions $+ : X \times X \to X$ and $\cdot : X \times X \to X$ is called a ring if the following properties hold: (vacant slots: axiom is NOT required)

Abbrev's :	$+$	$\cdot$	comments
(Clo $+$), (Clo $\cdot$)	as above	as above	still redundant
(A $+$), (A $\cdot$)	as above	as above	
(C $+$)	as above		If (C $\cdot$) holds: *commutative ring*
(N $+$)	as above	not req'd for ring; — for *ring with identity* we require (N $\cdot$) in the form $a \cdot 1 = 1 \cdot a = a$. $1 \neq 0$ not req'd here (but it holds in all but one trivial example)	
(Inv $+$)	as above	not req'd for ring; — but *when* we speak of an inverse, we require $a \cdot x = x \cdot a = 1$ (*)	
(D)	for all $a, b, c \in X$: $a \cdot (b + c) = a \cdot b + a \cdot c$ $(b + c) \cdot a = b \cdot a + c \cdot a$		need two here, since (C $\cdot$) wasn't required

(*) Note that speaking of an inverse only makes sense in a ring with identity!

• Synonyms for "Ring with identity" are "Ring with unity" or "Ring with 1".

• There are many interesting examples that don't have (C $\cdot$). (More so than this class may suggest). Think of matrices in particular!

Abstaining from the requirement (N $\cdot$) is a much lesser issue: most interesting rings have a multiplicative identity anyway.

Group axioms:

This will only be needed much later, but I collect it now, so that you have things together for *systematic* comparison when we will study groups

A set X with one function $\circ : X \times X \to X$ is called a group if the following properties hold:

Abbrev's :	$\circ$	comments
(Clo)	for all $a, b \in X$: $a \circ b \in X$	redundant again
(A)	for all $a, b, c \in X$: $a \circ (b \circ c) = (a \circ b) \cdot c$	
(C)	NOT req'd	If (C) holds: *commutative group*, alias *abelian group*
(N)	there is some $e \in X$ st. $a \circ e = e \circ a = a$ for all a	(*)
(Inv)	for each $a \in X$, there exists x st. $a \circ x = x \circ a = e$	(*)

Notes: (C) means of course $a \circ b = b \circ a$. The generality to consider groups without (C) is very important: if we were to say "we'll only study commutiative groups in this class", we could just as well save the time and not study groups at all. The word "abelian" is in honor of the Norwegian mathematician Niels Henrik Abel. But its use as an adjective has become so commonplace that it is usually not capitalized nowadays, in spite of its origin from a name.

The operation $\circ$ comes under different names in different examples: e.g., $*$, $\cdot$. In commutative groups (only then), the operation is often denoted as $+$. The neutral element likewise comes under different names in specific examples. Often 1. In commutative groups often 0. As there is only one operation, no risk of confusion arises.

(*) You may find in some books the following reduced axioms instead of (N) and (Inv):
(N') There is some $e \in X$ st. $a \circ e = a$ for all a
(Inv') For each $a \in X$, there exists x st. $a \circ x = e$.

Actually, even without (C), one can prove (N) and (Inv) together from (N') and (Inv') together; not separately (N) from (N') alone, nor (Inv) from (Inv') alone, only both from both. (The proof is tricky, but a weak B student can still understand it)