Operations and fields

Lecture notes for Math 524
9/1/06

These notes are a non-comprehensive summary to supplement your own class notes.

1. Operations and their properties

1.1. **Binary operations.**

Definition 1. *A* (binary) operation *on the set S is a function $\circ : S \times S \to S$.*

The customary notation is to write $x \circ y$ instead of $\circ(x, y)$.

So the criterion for $\circ$ to be an operation on S is that for all $x, y \in S$, $x \circ y$ is an element of S. Another way to say $x \circ y \in S$ for all $x, y \in S$ is that S is *closed* under $\circ$. Notice that being an operation is a property of $\circ$ with respect to S, while being closed is a property of S with respect to $\circ$. Which is more convenient to say depends on the context. You can use either, but don't confuse them. Again, saying things like $\circ$ is closed makes no sense.

Example 1. *$\circ$ defined by $x \circ y = x - y$ is an operation on $\mathbb{R}$ because $x - y$ is a real number whenever $x, y \in \mathbb{R}$.*

Example 2. *$\circ$ defined by $x \circ y = x/y$ is not an operation on $\mathbb{R}$ because x/y is not always a real number if $x, y \in \mathbb{R}$. E.g. $1 \circ 0 = 1/0$ does not even exist.*

Example 3. *$\circ$ defined by $x \circ y = \sqrt{xy}$ is not operation on $\mathbb{Q}$ because $\sqrt{xy}$ is not always a rational number if $x, y \in \mathbb{Q}$. E.g. $1 \circ 2 = \sqrt{(1)(2)}$ is well-known to be irrational.*

Exercises: Prove that the following are operations:

1. $+$ on $\mathbb{N}$
2. $+$ on $\mathbb{Q}$
3. $+$ on $\mathbb{C}$
4. $\cdot$ on $\mathbb{N}$
5. $\cdot$ on $\mathbb{Q}$
6. $\cdot$ on $\mathbb{C}$
7. $-$ on $\mathbb{Z}$
8. $/$ on $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$
9. $x \circ y = (x+1)(y-1)$ on $\mathbb{C}$.
10. Composition of functions on the set of functions $\mathbb{R} \to \mathbb{R}$.
11. Composition of functions on $\mathbb{Q}[x]$, which is the set of all polynomials with rational coefficients.

Prove that the following are not operations:

1. $-$ on $\mathbb{N}$
2. $/$ on $\mathbb{Q}$
3. $/$ on $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$
4. $x \circ y = \sqrt{xy}$ on $\mathbb{R}$.
5. Dot product of vectors on $\mathbb{R}^2$.

1.2. **Associativity.**

Definition 2. *An operation $\circ$ on the set S is* associative *if $(x \circ y) \circ z = x \circ (y \circ z)$ for all $x, y, z \in S$.*

Notice that commutativity and associativity are properties of the operation $\circ$ and not of the set S. Saying things like $\mathbb{R}$ is associative makes about as much sense as claiming that the temperature is purple today.

Example 4. *$\cdot$ on $\mathbb{Z}$ is associative because $(xy)z = x(yz)$ for any integers x, y.*

Example 5. *$-$ on $\mathbb{Z}$ is not associative because $(x-y)-z \neq y-(x-z)$ in general, e.g. $(0-1)-1 \neq 0-(1-1)$.*

Example 6. *Composition of functions on the set of functions $\mathbb{R} \to \mathbb{R}$ is associative. To see this we need to convince ourselves that $(f \circ g) \circ h = f \circ (g \circ h)$ for any functions f, g, h. We are comparing two functions here. Two functions are equal if they have the same domain and codomain and their values agree on all elements of this common domain. Both $(f \circ g) \circ h$ and $f \circ (g \circ h)$ have $\mathbb{R}$ for the domain and the codomain. So let's see if they agree for all $x \in \mathbb{R}$.*

$$(f \circ g) \circ h(x) = f \circ g(h(x)) = f(g(h(x)))$$
$$f \circ (g \circ h)(x) = f(g \circ h(x)) = f(g(h(x)))$$

These are indeed the same for all x.

Exercises: Which of the following operations are associative?

1. $\cdot$ on $\mathbb{C}$
2. $/$ on $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$
3. $x \circ y = (x+1)(y-1)$ on $\mathbb{C}$
4. $x \circ y = x^y$ on $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$.

1.3. **Commutativity.**

Definition 3. *An operation $\circ$ on the set S is* commutative *if $x \circ y = y \circ x$ for all $x, y \in S$.*

The "for all" part in this definition is crucial. Given any operation on any set, it's easy to find two elements $x, y \in S$ such that $x \circ y = y \circ x$. E.g. you could just take $y = x$. The real question is whether you can find $x, y \in S$ such that $x \circ y \neq y \circ x$. If not, $\circ$ is commutative.

Example 7. *$+$ on $\mathbb{Z}$ is commutative because $x + y = y + x$ for any integers x, y.*

Example 8. *$-$ on $\mathbb{Z}$ is not commutative because $x - y \neq y - x$ in general, e.g. $0 - 1 \neq 1 - 0$.*

Example 9. *Composition of functions on the set of functions $\mathbb{R} \to \mathbb{R}$ is not commutative because $f \circ g \neq g \circ f$ in general. E.g. let $f(x) = -x$ and $g(x) = x^2$. Then $f \circ g(x) = f(g(x)) = -x^2$ and $g \circ f(x) = g(f(x)) = (-x)^2 = x^2$ are not the same.*

Exercises: Which of the following operations are commutative?

1. $\cdot$ on $\mathbb{R}$
2. $\cdot$ on $\mathbb{C}$
3. $/$ on $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$
4. $x \circ y = x^y$ on $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$.

1.4. **Identity.**

Definition 4. *Given an operation $\circ$ on a set S, we say $e \in S$ is an* identity *if $e \circ x = x$ for all $x \in S$ and $x \circ e = x$ for all $x \in S$.*

Example 10. *For $+$ on $\mathbb{Z}$, 0 is an identity because $0 + x = x = x + 0$ for all $x \in \mathbb{Z}$.*

Example 11. *For composition on the set of functions $\mathbb{R} \to \mathbb{R}$, the identity function $f(x) = x$ is an identity since $f \circ g(x) = f(g(x)) = g(x)$ and $g \circ f(x) = g(f(x)) = g(x)$ for every function g.*

Example 12. *The operation $x \circ y = xy - 1$ on $\mathbb{Z}$ has no identity. If $y \in \mathbb{Z}$ were an identity, it would have to satisfy $x = x \circ y = xy - 1$ for all x. In particular, if $x = 1$, we get $y = 2$ and if $x = 2$ we get $y = 3/2$, and y cannot be both at the same time, not to mention that $3/2$ is not even in $\mathbb{Z}$.*

Example 13. *The operation $x \circ y = x\overline{y}$ on $\mathbb{C}$ does not have an identity either. If $y \in \mathbb{C}$ were an identity, it would have to satisfy $x = x \circ y = x\overline{y}$ for all $x \in \mathbb{C}$, which suggests $\overline{y} = 1$ and hence $y = 1$. But $1 \circ x = 1\overline{x} \neq x$ in general. E.g. $\overline{i} \neq i$.*

Exercises: Which of the following operations have identities and what are they?

1. $-$ on $\mathbb{Z}$
2. $+$ on the set of all functions $\mathbb{R} \to \mathbb{R}$ (recall $f + g$ is defined by $(f + g)(x) = f(x) + g(x)$)

3. / on $\mathbb{R}^*$
4. $x \circ y = (x+1)(y-1)$ on $\mathbb{C}$
5. $x \circ y = x^y$ on $\mathbb{R}^+$.

Proposition 1. *If an operation $\circ$ on the set S has an identity, this identity is unique.*

Proof: Suppose e and f are both identities. Using the fact that e is an identity, $e \circ f = f$. Now using the fact that f is an identity, $e \circ f = e$. So

$$e = e \circ f = f.$$

□

1.5. **Inverses.**

Definition 5. *Let $\circ$ be an operation on the set S and assume $\circ$ has an identity e. We say that $x \in S$ has an* inverse *if there exists a $y \in S$ such that $x \circ y = e$ and $y \circ x = e$.*

Example 14. *Consider $+$ on $\mathbb{Z}$. We know 0 is the identity (we can say "the" identity because we now know there can only be one). Every $x \in \mathbb{Z}$ has an inverse, namely $-x$ because $x + (-x) = 0$ and $(-x) + x = 0$.*

Example 15. *Consider $\cdot$ on $\mathbb{R}$. We know 1 is the identity. The element 2 then has inverse $1/2$. The element 0 has no inverse because no matter what you multiply 0 by, you never get 1. In fact, if $x \in \mathbb{R}$ and $x \neq 0$, then x has inverse $1/x$ with respect to this operation.*

Example 16. *Consider composition on all functions $\mathbb{R} \to \mathbb{R}$. We know that the identity is $f(x) = x$. The function $g(x) = x - 1$ has inverse $g^{-1}(x) = x + 1$. The function $g(x) = 3x$ has inverse $g^{-1}(x) = x/3$. The function $g(x) = x^2$ has no inverse because it is not one-to-one. (Why can't a function that is not one-to-one have an inverse?) The function $f(x) = e^x$ has no inverse either because it is not onto. You might now say, but wait, I learned in precalculus that the inverse of e^x is $\log(x)$. But the problem is that $\log(x)$ is not a function $\mathbb{R} \to \mathbb{R}$ because its domain only includes the positive real numbers. So the way we defined our operation, e^x has no inverse. In fact, the function has an inverse with respect to our operation iff it is both one-to-one and onto.*

Exercises: Which of the following operations are such that every element of the underlying set has an inverse?

1. $\cdot$ on $\mathbb{Z}^+ = \{x \in \mathbb{Z} \mid x > 0\}$
2. Composition of functions on $\mathbb{Q}[x]$, which is the set of all polynomials with rational coefficients.
3. $\cdot$ on the set of all functions $\mathbb{R} \to \mathbb{R}$ (recall fg is defined by $(fg)(x) = f(x)g(x)$)
4. $\cdot$ on $\mathbb{R}[x]$, the set of all polynomials with real coefficients
5. $\cdot$ on $\mathbb{R}(x)$, which is the set of all rational functions with real coefficients.

Proposition 2. *Let $\circ$ be an associative operation on the set S and assume that it has an identity e. If $x \in S$ has an inverse, then this inverse is unique.*

In other words, an element can have no inverse, or one inverse, but it cannot have two distinct inverses. The proof is similar to the proof that an identity is unique and is left as an exercise. Can you find an example of an operation with an identity for which inverses don't have to be unique? By the above theorem, such an operation would have to be nonassociative. (Finding such an example may be quite hard.)

2. Fields

Definition 6. *A* field *is a set F with two operations $+$ and $\cdot$ such that*

1. *$+$ and $\cdot$ are both commutative and associative*
2. *$+$ has an identity denoted by $0 \in F$*
3. *$\cdot$ has an identity denoted by $1 \in F$*
4. *Every element has an inverse with respect to $+$*

5. *Every element except* 0 *has an inverse with respect to* $\cdot$
6. $+$ *and* $\cdot$ *are distributive, which means* $x \cdot (y + z) = x \cdot y + x \cdot z$ *for all* $x, y, z \in F$
7. $0 \neq 1$

Note that $+$ and $\cdot$ may have nothing to do with the addition and multiplication of numbers you are familiar with. But their properties indeed mimic those of usual addition and multiplication. The operation $+$ is referred to as addition and $\cdot$ is referred to as multiplication. $\cdot$ is usually omitted in formulas, just like multiplication of numbers. 0 is called zero and 1 is called one, although they may have nothing to do with the real numbers 0 and 1. The rules about additive and multiplicative inverses in essence say that you can subtract any element from any element and you can divide any element by any nonzero element (0 has no multiplicative inverse).

Example 17. *$\mathbb{R}$ with ordinary addition and multiplication is a field. In this case the additive identity and the multiplicative identity are the numbers* 0 *and* 1 *you are familiar with. The additive inverse of a number is its usual negative and the multiplicative inverse is the usual reciprocal. (Notice* 0 *has no reciprocal, but it doesn't have to have a multiplicative inverse.) Commutativity, associativity, and distributivity are properties you learned about long ago.*

Example 18. *$\mathbb{Z}$ with ordinary addition and multiplication is not a field because not every nonzero element has a multiplicative inverse. E.g.* 2 *does not.*

Example 19. *The subset* $\mathbb{Q}[\sqrt{2}] = \left\{x + y\sqrt{2} \mid x, y \in \mathbb{Q}\right\}$ *of* $\mathbb{R}$ *is a field with usual addition and multiplication. In fact, we can say it is a subfield of* $\mathbb{R}$*. It is closed under* $+$ *because*

$$(x + y\sqrt{2}) + (x' + y'\sqrt{2}) = (x + x') + (y + y')\sqrt{2}) \in \mathbb{Q}[\sqrt{2}]$$

It is closed under $\cdot$ *because*

$$(x + y\sqrt{2})(x' + y'\sqrt{2}) = (xx' + 2yy') + (xy' + x'y)\sqrt{2}) \in \mathbb{Q}[\sqrt{2}]$$

It has additive and multiplicative identities $0 = 0 + 0\sqrt{2}$ *and* $1 = 1 + 0\sqrt{2}$*. The element* $x + y\sqrt{2}$ *has an additive inverse because*

$$-(x + y\sqrt{2}) = -x + (-y)\sqrt{2} \in \mathbb{Q}[\sqrt{2}$$

If $x + y\sqrt{2} \neq 0$*, that is at least one of* x *or* y *is not* 0*, then it has multiplicative inverse because*

$$\frac{1}{x + y\sqrt{2}} = \frac{1}{x + y\sqrt{2}} \frac{x - y\sqrt{2}}{x - y\sqrt{2}} = \frac{x - y\sqrt{2}}{x^2 - 2y^2} = \frac{x}{x^2 - 2y^2} + \frac{-y}{x^2 - 2y^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

(Why can't $x^2 - 2y^2 = 0$*? Remember* x, y *are rational numbers.) The two commutativity and associativity axioms and the distributivity axiom hold because they hold for* $+$ *and* $\cdot$ *on* $\mathbb{R}$*, which contains* $\mathbb{Q}[\sqrt{2}]$*.*

Example 20. *Consider the set of all functions* $\mathbb{R} \to \mathbb{R}$ *with addition defined by* $(f + g)(x) = f(x) + g(x)$ *and multiplication* $fg(x) = f(g(x))$*. In other words, multiplication is composition here. Is this a field? You can easily check that addition is indeed an operation, is commutative and associative, has the zero function* $f(x) = 0$ *for identity, and every function* f *has an inverse* $-f$ *defined by* $(-f)(x) = -f(x)$*. The multiplication (which is composition in this case) is an operation, is associative, and has the identity function* $f(x) = x$ *for an identity. But it is not commutative, and not every nonzero function has a multiplicative inverse. For example,* $f(x) = x^2$ *is not invertible because it is not one-to-one. Distributivity also fails:*

$$\begin{aligned}[f(g + h)](x) &= f(g(x) + h(x)) \\ (fg + fh)(x) &= f(g(x)) + f(h(x))\end{aligned}$$

which are in general not equal. E.g. try $f(x) = x^2$*,* $g(x) = x$*, and* $h(x) = x$*.*

Example 21. *The set* $\{1\}$ *with addition defined as* $1 + 1 = 1$*, and multiplication* $1 \cdot 1 = 1$ *is not a field. Actually, it satisfies almost all axioms. It even has an additive identity and a multiplicative identity. But they are the same thing, so it fails the axiom* $0 \neq 1$*.*

Exercises: Which of the following are fields?

1. $\mathbb{C}$ with usual addition and multiplication.
2. $\mathbb{Q}$ with usual addition and multiplication.
3. The set of all functions $\mathbb{R} \to \mathbb{R}$ with usual addition and multiplication of functions.
4. The set of all functions $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) \neq 0$ for any $x \in \mathbb{R}$ with usual addition and multiplication of functions.
5. $\mathbb{R}(x)$, the set of all (formal) rational functions with real coefficients with usual addition and multiplication of functions. That they are formal rational functions means you don't have to worry about what the domain is when you add and multiply them.
6. The subset $\mathbb{Z}[i] = \{x + yi \mid x, y \in \mathbb{Z}\}$ of $\mathbb{C}$ with ordinary addition and multiplication.
7. The subset $\mathbb{Q}[i] = \{x + yi \mid x, y \in \mathbb{Q}\}$ of $\mathbb{C}$ with ordinary addition and multiplication.