Operations, fields, and modular arithmetic

Lecture notes for MCS 221

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 $\circ(x, y)$.

Example 1. *Ordinary addition is an operation on the set of integers $\mathbb{Z}$ because if x and y are integers then $x + y$ is also an integer.*

Example 2. *Ordinary multiplication is an operation on the set of integers $\mathbb{Z}$ because if x and y are integers then xy is also an integer.*

Example 3. *Ordinary multiplication is an operation on the set of rational numbers $\mathbb{Q}$ because if $x = m/n$ and $y = s/t$ are rational numbers, that is $m, n, s, t \in \mathbb{Z}$ and $n, t \neq 0$ then*

$$xy = \frac{m}{n}\frac{s}{t} = \frac{ms}{nt}$$

is also a rational number as ms and nt must be integers and $nt \neq 0$.

Example 4. *Ordinary subtraction is an operation on $\mathbb{R}$ because $x - y$ is a real number whenever $x, y \in \mathbb{R}$.*

Example 5. *Ordinary division is not an operation on $\mathbb{R}$ because x/y is not always a real number if $x, y \in \mathbb{R}$. E.g. $1/0$ is not even defined, and it is definitely not a real number.*

Example 6. $\circ$ *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.*

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. Saying things like $\circ$ is closed makes no sense.

Exercises: Are the following operations?

1. $+$ on the set of nonnegative integers or natural numbers $\mathbb{N}$.
2. $-$ on $\mathbb{N}$
3. $\cdot$ on $\mathbb{N}$
4. $/$ on $\mathbb{N}$
5. $-$ on $\mathbb{Z}$
6. $-$ on $\mathbb{Q}$
7. $/$ on the set of nonzero real numbers $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$
8. $x \circ y = (x + 1)(y - 1)$ on $\mathbb{R}$.
9. $x \circ y = x^y$ on the set of positive real numbers $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$.
10. Composition of functions $\circ$ on the set of functions $\mathbb{R} \to \mathbb{R}$.
11. Composition of functions on the set of all polynomials with rational coefficients $\mathbb{Q}[x]$.

1.2. **Commutativity.**

Definition 2. 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 $\mathbb{Z}$
2. $\cdot$ on $\mathbb{R}$
3. $/$ on the set of nonzero rational numbers $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$
4. $x \circ y = x^y$ on the set of positive real numbers $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$.

1.3. **Associativity.**

Definition 3. 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 10. *$\cdot$ on $\mathbb{Z}$ is associative because $(xy)z = x(yz)$ for any integers x, y.*

Example 11. *$-$ 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 12. *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 $\mathbb{N}$
2. $/$ on $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$
3. $x \circ y = (x + 1)(y - 1)$ on $\mathbb{R}$
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 13. *For $+$ on $\mathbb{Z}$, 0 is an identity because $0 + x = x = x + 0$ for all $x \in \mathbb{Z}$.*

Example 14. *For composition on the set of functions $\mathbb{R} \to \mathbb{R}$, the identity function $I(x) = x$ is an identity since $I \circ g(x) = I(g(x)) = g(x)$ and $g \circ I(x) = g(I(x)) = g(x)$ for every function g.*

Example 15. *The operation $x \circ y = xy - 1$ on $\mathbb{Z}$ has no identity. (Why is $\circ$ an operation?) 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 $\mathbb{Z}$.*

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 $\mathbb{R}$
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 16. *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 17. *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 18. *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 $\ln(x)$. But the problem is that $\ln(x)$ 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 if and only if it is both one-to-one and onto.*

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

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

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. $+$ is commutative,
2. $+$ is associative,
3. $+$ has an identity denoted by $0 \in F$,
4. Every element of F has an inverse with respect to $+$,
5. $\cdot$ is commutative,
6. $\cdot$ is associative,
7. $\cdot$ has an identity denoted by $1 \in F$,
8. every element of F except 0 has an inverse with respect to $\cdot$,
9. $\cdot$ is distributive over $+$, which means that for all $x, y, z \in F$

$$x \cdot (y + z) = x \cdot y + x \cdot z$$
$$(x + y) \cdot z = x \cdot z + y \cdot z$$

10. $0 \neq 1$

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 no matter what they actually are. By convention, $\cdot$ is often 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 19. *$\mathbb{R}$ 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 20. *$\mathbb{Z}$ with ordinary addition and multiplication is not a field because not every nonzero element has a multiplicative inverse. E.g. 2 does not.*

Example 21. *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, $f(x) = x^2$ has no inverse because it is not one-to-one. Distributivity also fails:*

$$[f(g + h)](x) = f(g(x) + h(x))$$
$$(fg + fh)(x) = f(g(x)) + f(h(x))$$

which are in general not equal. E.g. try $f(x) = x^2$, $g(x) = x$, and $h(x) = 1$.

Example 22. *The set $\{0\}$ with addition defined as $0 + 0 = 0$, and multiplication $0 \cdot 0 = 0$ is not a field. Actually, it satisfies almost all properties. It even has an additive identity and a multiplicative identity (yes, 0 is a multiplicative identity in this case). But they are the same thing, so it fails the property $0 \neq 1$.*

Exercises: Which of the following are fields?

1. $\mathbb{Q}$ with usual addition and multiplication.
2. The set of all irrational numbers $\mathbb{R}$
   $\mathbb{Q}$ 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.

3. Modular arithmetic

Definition 7. Let $n \in \mathbb{Z}^+$ and $x, y \in \mathbb{Z}$. Let

$$x \equiv y \mod n$$

mean that $x - y$ is divisible by n.

You can pronounce $x \equiv y \mod n$ as "x is congruent to y modulo n."

Example 23.

- $12 \equiv 5 \mod 7$ *because* $12 - 5 = 7$ *is divisible by 7.*
- $5 \equiv 12 \mod 7$ *because* $5 - 12 = -7$ *is divisible by 7.*
- $5 \not\equiv 8 \mod 6$ *because* $5 - 8 = -3$ *is not divisible by 6.*
- $47 \equiv -1 \mod 8$ *because* $47 - (-1) = 48$ *is divisible by 8.*
- *Any two integers x and y are congruent modulo 1 because $x - y$ is always divisible by 1.*

Notice that you can think about congruence as the result of integer division with remainder: two numbers x and y are congruent modulo n is dividing them by n gives the same remainder.

Define the set $\mathbb{Z}_n$ as having n elements $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$:

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}.$$

So far all we have said is that $\mathbb{Z}_n$ is a set of n elements, but it will help to think that $\overline{0}$ stands for every integer that is congruent to 0 modulo n, $\overline{1}$ stands for every integer that is congruent to 1 modulo n, etc. In fact, $\mathbb{Z}_n$ is a set of the sets

$$\begin{aligned}
\overline{0} &= \{\ldots, -2n, -n, 0, n, 2n \ldots\} = \{kn \mid k \in \mathbb{Z}\}\\
\overline{1} &= \{\ldots, -2n+1, -n+1, 1, n+1, 2n+1 \ldots\} = \{kn+1 \mid k \in \mathbb{Z}\}\\
&\vdots\\
\overline{n-1} &= \{\ldots, -2n-1, -n-1, -1, n-1, 2n-1 \ldots\} = \{kn-1 \mid k \in \mathbb{Z}\}
\end{aligned}$$

So what we did is we sorted the integers into n buckets according to their remainders when divided by n. E.g. the elements of $\mathbb{Z}_3$ are

$$\begin{aligned}
\overline{0} &= \{\ldots, -6, -3, 0, 3, 6 \ldots\} = \{3k \mid k \in \mathbb{Z}\}\\
\overline{1} &= \{\ldots, -5, -2, 1, 4, 7 \ldots\} = \{3k+1 \mid k \in \mathbb{Z}\}\\
\overline{1} &= \{\ldots, -4, -1, 2, 5, 8 \ldots\} = \{3k+2 \mid k \in \mathbb{Z}\}
\end{aligned}$$

Now, let us allow any of the elements y of the set $\overline{x}$ to represent $\overline{x}$ in the sense that $\overline{x} = \overline{y}$ if y is an element of $\overline{x}$. E.g. in $\mathbb{Z}_3$, $\overline{2} = \overline{5} = \overline{-4}$ etc.

Define addition on $\mathbb{Z}_n$ as follows:

$$\overline{x} + \overline{y} = \overline{z}$$

if $z \equiv x + y \mod n$. E.g. in $\mathbb{Z}_5$,

$$\overline{2} + \overline{4} = \overline{1}$$

because $2 + 4 = 1 \mod 5$. It is not immediately obvious that this is really a legitimate thing to do, as it could be that choosing different elements of the sets $\overline{x}$ and $\overline{y}$ to represent the set would give different results for $\overline{x} + \overline{y}$. For example, in $\mathbb{Z}_5$, $\overline{2} = \overline{17}$ and $\overline{4} = \overline{9}$, so $\overline{2} + \overline{4}$ should be the same thing as $\overline{17} + \overline{9}$. In fact,

$$\overline{2} + \overline{4} = \overline{6} = \overline{1}$$

and

$$\overline{17} + \overline{9} = \overline{26} = \overline{1},$$

so they do give the same result. It can be proved that this must always be the case. But we are not going to do it here because we do not need to become experts at modular arithmetic at this time. So let us just believe that it is true.

Similarly, we can define multiplication on $\mathbb{Z}_n$ as follows:

$$\overline{x} \cdot \overline{y} = \overline{z}$$

if $z \equiv xy \mod n$. E.g. in $\mathbb{Z}_5$,

$$\overline{2} \cdot \overline{4} = \overline{3}$$

because $2 \cdot 4 = 3 \mod 5$. Like with addition, it would be good to know that this is well-defined in the sense that the result does not depend on which numbers from $\overline{x}$ and $\overline{y}$ we choose to represent these sets. We will not give the proof here, but let us at least verify that choosing $\overline{17}$ and $\overline{9}$ instead of $\overline{2}$ and $\overline{4}$ would have given the same result:

$$\overline{17} \cdot \overline{9} = \overline{153} = \overline{3},$$

which is the same we got above for $\overline{2} \cdot \overline{4}$.

Note that the addition and multiplication we defined above are operations on $\mathbb{Z}_n$. This is because no matter what integers x and y are, $x + y$ and xy are also integers and they belong to one of the sets

$$\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1},$$

which is another way of saying that $\overline{x} + \overline{y}$ and $\overline{x} \cdot \overline{y}$ are both elements of $\mathbb{Z}_n$.

We can now easily verify that $+$ and $\cdot$ on $\mathbb{Z}_n$ are both commutative and associative. For example,

$$\overline{x} + \overline{y} = \overline{x + y} = \overline{y + x} = \overline{y} + \overline{x}$$

because x and y are just integers and therefore $x + y = y + x$. Similarly,

$$(\overline{xy})\overline{z} = \overline{xy}\,\overline{z} = \overline{(xy)z} = \overline{x(yz)} = \overline{x}\,\overline{yz} = \overline{x}(\overline{yz})$$

because x, y and z are integers, so they satisfy $(xy)z = x(yz)$. Try your hand at checking that addition is associative and multiplication is commutative. The hardest thing here is to understand what it is that you need to prove.

Exercises: Verify the following in $\mathbb{Z}_n$.

1. $\overline{0}$ is an additive identity.
2. For every $\overline{x}$ in Z_n, $\overline{-x}$ is an additive inverse.
3. $\overline{1}$ is a multiplicative identity.
4. Multiplication is distributive over addition on $\mathbb{Z}_n$.
5. If $n \geq 2$, then $\overline{0} \neq \overline{1}$ in Z_n.

If you have made your way through the exercises above then you have verified that $\mathbb{Z}_n$ satisfies all of the properties of a field except for the one that says every nonzero element has a multiplicative inverse. So does every nonzero element have a multiplicative inverse? Not necessarily. That depends on n. It turns out, the if n is prime, then every nonzero element in $\mathbb{Z}_n$ has a multiplicative inverse, and if n is a composite number then not every nonzero element in $\mathbb{Z}_n$ has a multiplicative inverse. We will not prove this here, but let us at least see two examples:

Example 24. *In* $\mathbb{Z}_5$*,*

$$\begin{aligned}\overline{1}\cdot\overline{1} &= \overline{1}\\ \overline{2}\cdot\overline{3} &= \overline{1}\\ \overline{4}\cdot\overline{4} &= \overline{1}\end{aligned}$$

So $\overline{1}$ *and* $\overline{4}$ *are their own multiplicative inverses, while* $\overline{3}$ *serves as an inverse of* $\overline{2}$ *and vice versa. So every nonzero element does indeed have a multiplicative inverse. It may at first surprise you that* $\overline{44} = \overline{1}$*, but realizing that* $\overline{4} = \overline{-1}$ *may make this look less strange.*

Example 25. *In* $\mathbb{Z}_6$*,*

$$\begin{aligned}\overline{2}\cdot\overline{0} &= \overline{0}\\ \overline{2}\cdot\overline{1} &= \overline{2}\\ \overline{2}\cdot\overline{2} &= \overline{4}\\ \overline{2}\cdot\overline{3} &= \overline{0}\\ \overline{2}\cdot\overline{4} &= \overline{2}\\ \overline{2}\cdot\overline{5} &= \overline{4}\end{aligned}$$

So $\overline{2}$ *does not have a multiplicative inverse.*

What we are saying is that $\mathbb{Z}_n$ is a field if and only if $\mathbb{Z}_n$ is a prime number. Notice that these are rather different examples of a fields than the ones we had before in that it has finitely many elements. The reason we talked about $\mathbb{Z}_n$ is to understand that fields can look quite different from the ones you are used to, such as rational numbers, or real numbers with the usual operations of addition and multiplication.

Finite fields such as $\mathbb{Z}_p$ where p is prime play an important role in cryptographic algorithms and code breaking. The National Security Agency will neither confirm nor deny this.