WELL-DEFINED FUNCTIONS

KEITH CONRAD

1. Introduction

When defining an operation or function or formula, care has to be taken in the definition if the operation or function or formula involves *making choices* along the way.

Example 1.1. In elementary school we learned how to add fractions by a rule amounting to

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}. \tag{1.1}$$

For instance,

$$\frac{1}{2}+\frac{1}{3}=\frac{5}{6}, \quad \frac{2}{4}+\frac{1}{3}=\frac{10}{12}=\frac{5}{6}.$$

What is not emphasized in elementary school is that changing the numerator and denominator without changing the fraction (e.g., writing 1/2 as 2/4) does *not* change the answer. All students implicitly accept this, but for a rigorous development of fractions this feature should be explained: if $a/b = a'/b'$ and $c/d = c'/d'$ why is $(ad+bc)/bd = (a'd'+b'c')/(b'd')$?

Here is how this can be shown. If $a/b = a'/b'$ and $c/d = c'/d'$ then $ab' = a'b$ and $cd' = c'd$ in $\mathbf{Z}$. To show $(ad+bc)/bd = (a'd'+b'c')/(b'd')$ we check that $(ad+bc)(b'd') = (a'd'+b'c')(bd)$:

$$(ad+bc)(b'd') = (ab')dd' + bb'(cd') = (a'b)dd' + bb'(c'd) = (a'd' + b'c')(bd). \checkmark$$

Someone may ask why we can't add fractions using the different rule

$$\frac{a}{b}\oplus\frac{c}{d}=\frac{a+c}{b+d}, \tag{1.2}$$

where we write $\oplus$ rather than $+$ to emphasize that this is a different operation. This operation doesn't make sense (ignore that it isn't actual addition of fractions), since its output can change if we change a numerator and denominator without changing the fraction, *e.g.*,

$$\frac{1}{2}\oplus\frac{1}{3}=\frac{2}{5}, \quad \frac{2}{4}\oplus\frac{1}{3}=\frac{3}{7},$$

and $2/5 \neq 3/7$.

We say that $+$ in (1.1) is a *well-defined* operation on fractions while (1.2) is not a well-defined operation on fractions. If you change the way you write fractions (different numerators and denominators, but keeping the same values of the fractions), the answer does not change in (1.1) but it does change in (1.2).[1]

[1] We could make (1.2) well-defined by insisting the fractions a/b and c/d are in reduced form with positive denominators. A fraction can be written like that in just one way. The resulting operation on fractions, at least those that are positive, is called the mediant and occurs in the study of Farey fractions and continued fractions.

Example 1.2. In elementary school we are told that the number π is the ratio C/D where C is the circumference and D is the diameter of a circle. Did you ever ask yourself why this is the same for all circles? Why does changing the size of a circle not change the ratio C/D? Don't try to show that by using the formula $C = 2\pi r$, as it is just another version of the proposed definition $\pi = C/D$, since $D = 2r$, so it would be circular reasoning (literally). The history behind this formula, going back to ancient Greece, is in [1].

That the ratio C/D is independent of the choice of circle in the plane tells us that π is *well-defined*.

Example 1.3. In calculus, $\int_a^b f(x)dx$ can be computed as

$$\int_a^b f(x)dx = F(b) - F(a),$$

where $F(x)$ is an arbitrary anti-derivative of $f(x)$ on $[a, b]$, *i.e.*, $F'(x) = f(x)$ for all x in $[a, b]$. This formula for $\int_a^b f(x)dx$ involves a choice of anti-derivative for $f(x)$, but the formula does *not* depend on the choice: every anti-derivative $G(x)$ of $f(x)$ on $[a, b]$ differs from $F(x)$ by a constant, say $G(x) = F(x) + C$ for all x in $[a, b]$, and changing the anti-derivative $G(x)$ does not change the difference of its values at the endpoints:

$$G(b) - G(a) = (F(b) + C) - (F(a) + C) = F(b) - F(a).$$

So the difference of the values of an anti-derivative of $f(x)$ at $x = a$ and $x = b$ is independent of the choice of anti-derivative of $f(x)$ on the interval $[a, b]$.[2]

In contrast, the "rule" $F(b)+F(a)$ depends on the choice of anti-derivative of $f(x)$, since

$$G(b) + G(a) = (F(b) + C) + (F(a) + C) = F(b) + F(a) + 2C,$$

which is a new value if $C \neq 0$. Taking differences in an anti-derivative cancels the effect of the undetermined additive constant, so the expression $F(b) - F(a)$ is a well-defined value based on the original input function $f(x)$ and the interval $[a, b]$.

2. Well-definedness in modular arithmetic

In algebra, there are many times when we want to define a function on $\mathbf{Z}/(m)$, the integers modulo m. Usually the value of the function on a congruence class mod m involves a *choice* of representative for that congruence class, and we must check this is well-defined, *i.e.*, the function's value does not depend on the choice of representative.

Example 2.1. If $a \equiv b \bmod 2$, then $(-1)^a = (-1)^b$. Therefore, we have a *well-defined* function $f \colon \mathbf{Z}/(2) \to \{\pm 1\}$ given by the rule

$$f(a \bmod 2) = (-1)^a.$$

You need to train yourself to check that functions you want to define on $\mathbf{Z}/(m)$ in terms of congruence class representatives mod m are in fact well-defined (that is, independent of the choices made). The following table lists examples of well-defined functions on various $\mathbf{Z}/(m)$'s. Some functions that are not well-defined, *i.e.*, are nonsense, will be given later.

[2] This is why in physics, potential energy has no intrinsic meaning (the zero level of potential energy can be anywhere), but *differences* in potential energy are physically meaningful.

Group	Rule
$\mathbf{Z}/(2)$	$(-1)^a$
$\mathbf{Z}/(4)$	$(-1)^a$
$\mathbf{Z}/(4)$	i^a
$\mathbf{Z}/(12)$	i^a
$\mathbf{Z}/(4)$	$2^a \bmod 5$
$\mathbf{Z}/(3)$	$2^a \bmod 7$
$\mathbf{Z}/(3)$	$a^3 \bmod 9$
$\mathbf{Z}/(4)$	$\frac{a(a-1)}{2} \bmod 2$

In all cases, to show a function $f\colon \mathbf{Z}/(m) \to S$ that takes values in some set S is well-defined (that is, makes sense), we must show

$$a \equiv b \bmod m \Longrightarrow f(a \bmod m) = f(b \bmod m).$$

Let's run through this kind of check for the examples in the table above.

- if $a \equiv b \bmod 2$, then $a = b + 2k$ for $k \in \mathbf{Z}$, so $(-1)^a = (-1)^{b+2k} = (-1)^b(-1)^{2k} = (-1)^b$.
- if $a \equiv b \bmod 4$, then $a = b + 4k$ for $k \in \mathbf{Z}$, so $(-1)^a = (-1)^{b+4k} = (-1)^b(-1)^{4k} = (-1)^b$.
- if $a \equiv b \bmod 4$, then $a = b + 4k$ for $k \in \mathbf{Z}$, so $i^a = i^{b+4k} = i^b i^{4k} = i^b(i^4)^k = i^b$.
- if $a \equiv b \bmod 12$, then $a = b + 12k$ for $k \in \mathbf{Z}$, so $i^a = i^{b+12k} = i^b i^{12k} = i^b(i^4)^{3k} = i^b$.
- if $a \equiv b \bmod 4$, then $a = b + 4k$ for $k \in \mathbf{Z}$, so $2^a = 2^{b+4k} = 2^b(2^4)^k \equiv 2^b \bmod 5$ since $2^4 = 16 \equiv 1 \bmod 5$.
- if $a \equiv b \bmod 3$, then $a = b + 3k$ for $k \in \mathbf{Z}$, so $2^a = 2^{b+3k} = 2^b(2^3)^k \equiv 2^b \bmod 7$ since $2^3 = 8 \equiv 1 \bmod 7$.
- if $a \equiv b \bmod 3$, then $a = b + 3k$ for $k \in \mathbf{Z}$, so $a^3 = (b + 3k)^3 = b^3 + 3b^2(3k) + 3b(3k)^2 + (3k)^3 = b^3 + 9(b^2k + 3bk^2 + 3k^3) \equiv b^3 \bmod 9$.
- if $a \equiv b \bmod 4$, then $a(a-1) \equiv b(b-1) \bmod 4$. Both $a(a-1)$ and $b(b-1)$ are even, since a or $a-1$ is even and b or $b-1$ is even. Therefore we can divide both sides of the congruence and the modulus by 2 to obtain $\frac{a(a-1)}{2} \equiv \frac{b(b-1)}{2} \bmod 2$.

Before looking at more complicated examples that show how to check a function on $\mathbf{Z}/(m)$ is well-defined, let's see why some "functions" on $\mathbf{Z}/(m)$ are *not* well-defined.

Group	Bad Rule
$\mathbf{Z}/(3)$	$(-1)^a$
$\mathbf{Z}/(5)$	$2^a \bmod 5$
$\mathbf{Z}/(3)$	$a^2 \bmod 9$
$\mathbf{Z}/(2)$	$\frac{a(a-1)}{2} \bmod 2$

To show a rule introduced on $\mathbf{Z}/(m)$ is not well-defined, we just need to find an example of a and b with $a \equiv b \bmod m$ and the rule leads to different values in the two cases:

- $(-1)^a$ is not a well-defined function on $\mathbf{Z}/(3)$, since $4 \equiv 1 \bmod 3$, but $(-1)^4 = 1$ while $(-1)^1 = -1$.
- $2^a \bmod 5$ is not a well-defined function on $\mathbf{Z}/(5)$ since $5 \equiv 0 \bmod 5$ and $2^5 = 32 \equiv 2 \bmod 5$ while $2^0 \equiv 1 \bmod 5$.
- $5 \equiv 2 \bmod 3$, but $5^2 = 25 \equiv 7 \bmod 9$ and $2^2 \equiv 4 \bmod 9$. (Compare this with cubing, as in the first table: $5^3 \equiv 2^3 \bmod 9$.)

- $5 \equiv 3 \bmod 2$ and $\frac{5(5-1)}{2} \equiv 0 \bmod 2$ while $\frac{3(3-1)}{2} \equiv 1 \bmod 2$. (Compare with the first table, where we saw $\frac{a(a-1)}{2} \bmod 2$ is well-defined when we treat a as belonging to $\mathbf{Z}/(4)$ instead of $\mathbf{Z}/(2)$.)

While showing a function is not well-defined requires just one counterexample, as above, to show a function *is* well-defined requires more work than checking one example! You must verify that the rule for the function is truly independent of the representative you pick from the congruence class, for all congruence classes. Look again at the proofs above that the various well-defined functions given earlier in the first table are in fact well-defined.

There is a point of terminology worth noting here. Speaking about "a well-defined function" is in some sense an *abuse of language*, since a function has to make sense before it is really called a function in the first place. However, the conventional manner of writing and speaking is to introduce a formula on some $\mathbf{Z}/(m)$ and call it a function before right away doing the check that it is well-defined (that is, it is independent of the choice of representative) and thus worthy of being called a function.

Now that we have seen how to check a function is or is not well-defined for some explicit choices of the modulus, we consider some situations where the modulus is a parameter (it is not fixed to a specific value).

Theorem 2.2. *The function $\mathbf{Z}/(m) \to \mathbf{Z}$ given by $f(a \bmod m) = (a, m)$ is well-defined. In other words, the greatest common divisor of an integer with m does not change if we adjust the integer modulo m.*

Let's see what the theorem is saying in an example before we prove the theorem. In $\mathbf{Z}/(10)$ the congruence class of 4 is a list of integers $\{\dots, -6, 4, 14, 24, \dots\}$ and every single integer in this congruence class has the same gcd with 10: $\gcd(4, 10) = 2$, $\gcd(14, 10) = 2$, $\gcd(-6, 10) = 2$, and so on. If $a \equiv 4 \bmod 10$ then $\gcd(a, 10) = 2$.

Proof. Let $a \equiv b \bmod m$, say $a = b + mk$ for $k \in \mathbf{Z}$. Set $d = (a, m)$ and $d' = (b, m)$. We will show $d = d'$.

Since d divides both a and m, it divides $a - mk = b$. Thus d is a common divisor of b and m, so $d \leq d'$.

Since d' divides both b and m, it divides $b + mk = a$. Thus d' is a common divisor of a and m, so $d' \leq d$.

Comparing the two inequalities on d and d', we have $d = d'$. □

Theorem 2.3. *If G is a finite group and $g \in G$ satisfies $g^n = e$ for some $n \in \mathbf{Z}^+$ then the function $f \colon \mathbf{Z}/(n) \to G$ given by $f(a \bmod n) = g^a$ is well-defined.*

Proof. If $a \equiv b \bmod n$, write $a = b + nk$ for some $k \in \mathbf{Z}$. Then $g^a = g^{b+nk} = g^b(g^n)^k = g^b$ since $g^n = e$. □

The point of Theorem 2.3 is that, while we are used to viewing g^a with a as an integer, we can also view g^a as having the exponent a belong to $\mathbf{Z}/(n)$ if $g^n = e$.

Note we do not need n to be the order of g in Theorem 2.3. All that was used in the proof was the condition $g^n = e$, and that n might well be a multiple of the order. (Recall the example of $(-1)^a$ with $a \in \mathbf{Z}/(4)$.)

Theorem 2.4. *If $d \mid n$, the reduction map $r \colon \mathbf{Z}/(n) \to \mathbf{Z}/(d)$ given by the rule $r(a \bmod n) = a \bmod d$ is well-defined.*

Proof. If $a \equiv b \bmod n$, then $n \mid (a - b)$. Since $d \mid n$, we have $d \mid (a - b)$, so $a \equiv b \bmod d$. □

For example the function $r\colon \mathbf{Z}/(10) \to \mathbf{Z}/(5)$ where $r(a \bmod 10) = a \bmod 5$ is well-defined: if two integers are congruent mod 10 then they are also congruent mod 5.

The "function" $r\colon \mathbf{Z}/(10) \to \mathbf{Z}/(4)$ given by $r(a \bmod 10) = a \bmod 4$ is *not* well-defined (it is not a function at all), since $10 \equiv 0 \bmod 10$ but $10 \not\equiv 0 \bmod 4$.

3. More examples of well-definedness

In this last section we describe more instances where a definition is well-defined: rational powers, a projection formula, and arc length integrals.

Rational powers. Our first example is the definition of rational powers. Fix $a > 0$. For each $k \in \mathbf{Z}^+$, a has a unique positive kth root. This number is the unique positive solution to the equation $x^k = a$ and it is often denoted as $\sqrt[k]{a}$. We define $a^{1/k} = \sqrt[k]{a}$, and for a fraction m/n where $m \in \mathbf{Z}$ and $n \in \mathbf{Z}^+$, we define $a^{m/n} = (a^{1/n})^m = (\sqrt[n]{a})^m$. There is absolutely nothing ambiguous about the notation $a^{1/n}$, but there is something potentially ambiguous about writing $(\sqrt[n]{a})^m$ as $a^{m/n}$: a fraction can be written in many ways as a ratio of integers m/n (with $n > 0$), so to show $a^{m/n}$ is well-defined we have to show any two ways of writing a fraction as m/n leads to the same meaning for $(\sqrt[n]{a})^m$.

Theorem 3.1. *Fix a positive number a. If $m/n = m'/n'$ where n and n' are in $\mathbf{Z}^+$ and m and m' are in $\mathbf{Z}$, then $(\sqrt[n]{a})^m = (\sqrt[n']{a})^{m'}$.*

Proof. Set $u = (\sqrt[n]{a})^m$ and $v = (\sqrt[n']{a})^{m'}$. We want to show $u = v$. Since $m/n = m'/n'$ and the denominators are positive, the numerators have the same sign (positive or negative) or the numerators are both 0.

Case 1: $m = m' = 0$. We have $u = (\sqrt[n]{a})^0 = 1$ and $v = (\sqrt[n']{a})^0 = 1$.

Case 2: $m > 0$ and $m' > 0$. We will show $u^k = v^k$ for a certain positive integer k, and then it would follow that $u = v$ by the uniqueness of the kth root of positive numbers.

Since u involves an nth root and v involves an n'th root, we compute

$$u^n = ((\sqrt[n]{a})^m)^n = ((\sqrt[n]{a})^n)^m = a^m$$

and

$$v^{n'} = ((\sqrt[n']{a})^{m'})^{n'} = ((\sqrt[n']{a})^{n'})^{m'} = a^{m'}.$$

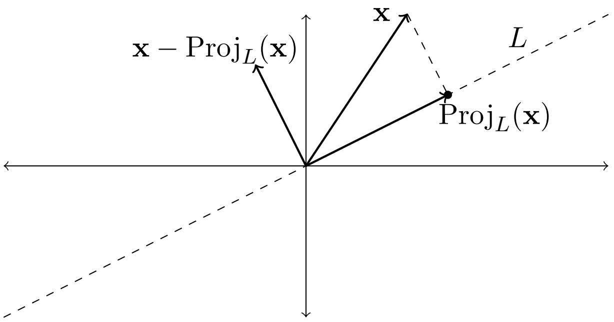
Since $m/n = m'/n'$, we have $nm' = n'm$, so we further compute

$$(u^n)^{m'} = (a^m)^{m'} = a^{mm'}, \qquad (v^{n'})^m = (a^{m'})^m = a^{m'm} = a^{mm'}.$$

Both expressions are $a^{mm'}$, so $u^{nm'} = v^{n'm}$. The exponents here are equal in $\mathbf{Z}^+$, so by the uniqueness of the kth root when $k = nm' = n'm$, we have $u = v$.

Case 3: $m < 0$ and $m' < 0$. From $m/n = m'/n'$ we have $(-m)/n = (-m')/n$, so by Case 2, $(\sqrt[n]{a})^{-m} = (\sqrt[n']{a})^{-m'}$. Inverting both sides, $(\sqrt[n]{a})^m = (\sqrt[n']{a})^{m'}$. □

Projection formula. Our next example is from linear algebra. For a one-dimensional subspace L in $\mathbf{R}^n$ and each $\mathbf{x} \in \mathbf{R}^n$, $\mathrm{Proj}_L(\mathbf{x})$ denotes the vector in L for which the difference $\mathbf{x} - \mathrm{Proj}_L(\mathbf{x})$ is perpendicular to L, as illustrated in the picture below ($n = 2$).


$\mathbf{x}$
$\mathbf{x} - \mathrm{Proj}_L(\mathbf{x})$
L
$\mathrm{Proj}_L(\mathbf{x})$

Calculations with dot products lead to a formula for this projection:

$$\mathrm{Proj}_L(\mathbf{x}) = \left(\frac{\mathbf{x}\cdot\mathbf{v}}{\mathbf{v}\cdot\mathbf{v}}\right)\mathbf{v}$$

where $\mathbf{v}$ is a choice of nonzero vector in L. Let's check this formula is independent of the choice of $\mathbf{v}$ in its definition.

Theorem 3.2. *If L is a one-dimensional subspace of $\mathbf{R}^n$ and $\mathbf{v}$ is a nonzero vector lying in L then for each $\mathbf{x}$ in $\mathbf{R}^n$, the vector*

$$\left(\frac{\mathbf{x}\cdot\mathbf{v}}{\mathbf{v}\cdot\mathbf{v}}\right)\mathbf{v}$$

is independent of the choice of $\mathbf{v}$.

Proof. Let $\mathbf{v}$ and $\mathbf{w}$ be two nonzero vectors in L. Since L is one-dimensional, $\mathbf{v}$ and $\mathbf{w}$ are scalar multiples of each other, say $\mathbf{w} = c\mathbf{v}$ with $c \in \mathbf{R}$. Then $c \neq 0$, so

$$\left(\frac{\mathbf{x}\cdot\mathbf{w}}{\mathbf{w}\cdot\mathbf{w}}\right)\mathbf{w} = \left(\frac{\mathbf{x}\cdot(c\mathbf{v})}{(c\mathbf{v})\cdot(c\mathbf{v})}\right)(c\mathbf{v}) = \frac{c(\mathbf{x}\cdot\mathbf{v})}{c^2(\mathbf{v}\cdot\mathbf{v})}(c\mathbf{v}) = \frac{c^2(\mathbf{x}\cdot\mathbf{v})}{c^2(\mathbf{v}\cdot\mathbf{v})}\mathbf{v} = \left(\frac{\mathbf{x}\cdot\mathbf{v}}{\mathbf{v}\cdot\mathbf{v}}\right)\mathbf{v}. \qquad \square$$

Arc length integrals. Let C be a "nice" parametrized curve in $\mathbf{R}^n$: there is a function $\gamma\colon [a,b] \to \mathbf{R}^n$ such that

- $C = \gamma([a,b])$,
- γ is continuously differentiable,
- $\gamma'(t) \neq \mathbf{0}$ for all t.

Using γ we define the length of C to be

$$\int_a^b \|\gamma'(t)\|\,dt.$$

We will show this notion of length is independent of the choice of parametrization used in γ: it is unaffected by a "change of variables" in the path.

Theorem 3.3. *If $\varphi\colon [c,d] \to [a,b]$ is a continuously differentiable bijection with $\varphi' \neq 0$ then the composition $\widetilde{\gamma} := \gamma\circ\varphi\colon [c,d] \to \mathbf{R}^n$ is also a "nice" parametrization of C and the length of C using $\widetilde{\gamma}$ is the same*[3] *as the length of C using γ:*

$$\int_a^b \|\gamma'(t)\|\,dt = \int_c^d \|\widetilde{\gamma}'(u)\|\,du.$$

[3] Parametrizations of C that are not related in this way might not yield the same notion of length: consider two parametrizations of a circle that go once and twice around.

Proof. $\underline{\widetilde{\gamma} \text{ is “nice” parametrization of } C}$. By $C = \gamma([a,b])$ and $[a,b] = \varphi([c,d])$, we have $C = \gamma(\varphi([c,d])) = \widetilde{\gamma}([c,d])$. A composition of continuously differentiable functions is continuously differentiable, so $\widetilde{\gamma}$ is continuously differentiable. Using the chain rule on $\widetilde{\gamma} = \gamma \circ \varphi$, we have $\widetilde{\gamma}'(u) = (\gamma \circ \varphi)'(u) = \gamma'(\varphi(u))\varphi'(u)$, so $\widetilde{\gamma}'(u) \neq \mathbf{0}$ since $\gamma'(\varphi(u)) \neq \mathbf{0}$ and the scalar $\varphi'(u)$ is nonzero.

$\underline{\text{Length is not changed}}$. Since φ' is continuous and nonvanishing, either $\varphi' > 0$ on $[c,d]$ or $\varphi' < 0$ on $[c,d]$. If $\varphi' > 0$ then $a = \varphi(c)$, $b = \varphi(d)$, and $\|\widetilde{\gamma}'(u)\| = \|\gamma'(\varphi(u))\||\varphi'(u)| = \|\gamma'(\varphi(u))\|\varphi'(u)$, so

$$\int_c^d \|\widetilde{\gamma}'(u)\|\,du = \int_c^d \|\gamma'(\varphi(u))\|\varphi'(u)\,du.$$

By the substitution $t = \varphi(u)$ we get $dt = \varphi'(u)\,du$ and

$$\int_c^d \|\gamma'(\varphi(u))\|\varphi'(u)\,du = \int_{\varphi(c)}^{\varphi(d)} \|\gamma'(t)\|\,dt = \int_a^b \|\gamma'(t)\|\,dt.$$

If $\varphi' < 0$ then $a = \varphi(d)$, $b = \varphi(c)$, and $\|\widetilde{\gamma}'(u)\| = \|\gamma'(\varphi(u))\||\varphi'(u)| = \|\gamma'(\varphi(u))\|(-\varphi'(u))$, so

$$\int_c^d \|\widetilde{\gamma}'(u)\|\,du = -\int_c^d \|\gamma'(\varphi(u))\|\varphi'(u)\,du.$$

By the substitution $t = \varphi(u)$ we get $dt = \varphi'(u)\,du$ and

$$-\int_c^d \|\gamma'(\varphi(u))\|\varphi'(u)\,du = -\int_{\varphi(c)}^{\varphi(d)} \|\gamma'(t)\|\,dt = -\int_b^a \|\gamma'(t)\|\,dt = \int_a^b \|\gamma'(t)\|\,dt. \qquad \square$$

References

[1] D. Richeson, Circular Reasoning: Who First Proved That C Divided by D Is a Constant? *College Math. J.* **46** (2015), 162–171.