Reminders

Fields A field F is a triple

$$F = (\{\text{elements in } F\}, +, \cdot)$$

of a set and two operations defined on it:

$+ : F \times F \longrightarrow F$ (addition)

$\cdot : F \times F \longrightarrow F$ (multiplication)

such that:

i) addition is commutative

ii) addition is associative

iii) there is an element $0 \in F$ such that for every $x \in F$ $x + 0 = 0 + x = x$.

iv) for every $x \in F$ there is an element $-x \in F$ such that $x + (-x) = (-x) + x = 0$.

i') multiplication is commutative

ii') multiplication is associative

iii') there is an element $1 \in F$, different from 0, such that for every $x \in F$ $x \cdot 1 = 1 \cdot x = x$

iv') for every $x \in F$, $x \neq 0$, there is an element $x^{-1} \in F$ such that $x \cdot x^{-1} = x^{-1} \cdot x = 1$.

ix) for every $x, y, z \in F$

$(x+y) \cdot z = x \cdot z + y \cdot z$, (right distributive property)

$z \cdot (x+y) = z \cdot x + z \cdot y$. (left distributive property)

Structure Preserving Functions

Definition Let F_1, F_2 be two fields:
$F_1 = (\{\text{elements in } F_1\}, +_1, \cdot_1)$,
$F_2 = (\{\text{elements in } F_2\}, +_2, \cdot_2)$.

A function $\varphi: F_1 \longrightarrow F_2$ is a field homomorphism if for every $x, y \in F_1$

i) $\varphi(x +_1 y) = \varphi(x) +_2 \varphi(y)$

and ii) $\varphi(x \cdot_1 y) = \varphi(x) \cdot_2 \varphi(y)$

and iii) $\varphi(1_{F_1}) = 1_{F_2}$.

Remark To say that the structure is preserved, we should also have

iv) $\varphi(0_{F_1}) = 0_{F_2}$

and v) for every $x \in F_1$ $\varphi(-x) = -\varphi(x)$

($-x$: additive inverse of x in F_1; $-\varphi(x)$: additive inverse of $\varphi(x)$ in F_2)

and vi) if $x \neq 0_{F_1}$, then $\varphi(x) \neq 0_{F_2}$ too

and $\varphi(x^{-1}) = (\varphi(x))^{-1}$.

(x^{-1}: multiplicative inverse of x in F_1; $(\varphi(x))^{-1}$: multiplicative inverse of $\varphi(x)$ in F_2)

But these follow from the definition we gave!

Proposition If $\varphi: F_1 \longrightarrow F_2$ is a field homomorphism, then Range(φ) is a subfield of F_2.

Proof First we check that iv), v) and vi) from the above remark hold true.

For every $x \in F_1$

$$\varphi(x) = \varphi(x +_1 0_{F_1}) = \varphi(x) +_2 \varphi(0_{F_1})$$

Also $\varphi(x) = \varphi(x) +_2 0_{F_2}$, therefore by the cancellation law for addition in F_2, we get that

$$\varphi(0_{F_1}) = 0_{F_2}.$$

Similarly for every $x \in F_1$

$$\varphi(x) +_2 \varphi(-x) = \varphi(x +_1 (-x)) = \varphi(0_{F_1}) = 0_{F_2}$$

and also $\varphi(x) +_2 (-\varphi(x)) = 0_{F_2}$,
therefore $\varphi(-x) = -\varphi(x)$.

Finally, recall that we have seen that a field homomorphism is injective. Therefore for every $x \in F_1$, $x \neq 0_{F_1}$, we have

$$\varphi(x) \neq \varphi(0_{F_1}) = 0_{F_2}.$$

But then $(\varphi(x))^{-1}$ exists, and moreover we have
$\varphi(x) \cdot \varphi(x^{-1}) = \varphi(x \cdot x^{-1}) = \varphi(1_{F_1}) = 1_{F_2}$
as well as $\varphi(x) \cdot (\varphi(x))^{-1} = 1_{F_2}$.
Thus by the cancellation law for multiplication in F_2, we get that $\varphi(x^{-1}) = (\varphi(x))^{-1}$.

We now have to show, using the above, that Range(φ) is a subfield of F_2.

Reminder Given a field $F = (\{\text{elements in } F\}, +, \cdot)$ and a subset K of F, to show that K is a subfield of F it suffices to check that

- K has at least two elements
- K is closed under the addition $+$ in F, that is, if $x, y \in K$ then $x+y$ is in K too
- K is closed under the multiplication $\cdot$ in F
- K is closed under taking additive inverses, that is if $x \in K$ then $-x$ (the additive inverse of x in F) is also in K
- K is closed under taking multiplicative inverses, that is, if $x \in K$ and $x \neq 0_F$, then x^{-1} is in K too.

Returning to the proof of the Proposition, we have to check the above for Range(φ).

Recall that Range$(\varphi) = \{ \varphi(z) : z \in F_1 \}$ (the collection of all images of elements in F_1 under φ).

By definition of a field homomorphism

$$1_{F_2} = \varphi(1_{F_1}) \in \text{Range}(\varphi).$$

We also saw that $0_{F_2} = \varphi(0_{F_1}) \in \text{Range}(\varphi)$.

Since $0_{F_2} \neq 1_{F_2}$, these are two different elements of Range(φ).

Now we check that Range(φ) is closed under addition, multiplication and taking additive and multiplicative inverses.

Let u, v be two elements in Range(φ). Then there exist $x, y \in F_1$ such that

$$u = \varphi(x), \quad v = \varphi(y).$$

Range(φ) closed under addition: we need to show that $u +_2 v \in$ Range(φ). But

$$u +_2 v = \varphi(x) +_2 \varphi(y) = \varphi(\overbrace{x +_1 y}^{\text{an element of } F_1}) \in \text{Range}(\varphi)$$

(= by definition of a field homomorphism)

Range(φ) closed under multiplication: we need to show that $u \cdot_2 v \in$ Range(φ). But

$$u \cdot_2 v = \varphi(x) \cdot_2 \varphi(y) = \varphi(\overbrace{x \cdot_1 y}^{\text{an element of } F_1}) \in \text{Range}(\varphi)$$

(= by def. of field homomorphism)

Range(φ) closed under taking additive inverses: we need to show that $-u$ is in Range(φ). But, as we showed above,

$$-u = -\varphi(x) = \varphi(-x) \in \text{Range}(\varphi).$$

Range(φ) closed under taking multiplicative inverses:

assume that v is non-zero too; we need to show that v^{-1} (which exists since $v \neq 0_{F_2}$) is in Range(φ).

We first observe that, if $y \in F_1$ is such that $\varphi(y) = v$, then $y \neq 0_{F_1}$. Indeed, we already showed that

$$\varphi(0_{F_1}) = 0_{F_2} \neq v,$$

hence 0_{F_1} cannot be a preimage of v.

Therefore y^{-1} exists in F_1, and, as we showed above

$$(\varphi(y))^{-1} = \varphi(y^{-1})$$

$$\Rightarrow v^{-1} = (\varphi(y))^{-1} = \varphi(y^{-1}) \in \text{Range}(\varphi).$$

Combining all the above, we conclude that Range(ℓ) is a subfield of F_2.

MATH 227 Jan 8

Composition of Functions

Let A, B be sets, and let $\ell : A \to B$ a function. Recall that we call A the domain of ℓ, and B the codomain of ℓ.

In addition, the set $\{\ell(a) : a \in A\}$ is called the range of ℓ, and denoted by Range(ℓ):

$$\text{Range}(\ell) := \{\ell(a) : a \in A\}.$$

Observe that Range(ℓ) is a subset of B.

Consider now a third set C, and a function $h : B_0 \to C$, where B_0 is some subset of B.

If $\text{Range}(\ell) \subseteq B_0$, then we can define the composition of h with ℓ:

$h \circ \ell$ is a function from A to C such that, for every $a \in A$

$$(h \circ \ell)(a) := h(\ell(a)).$$

$\ell(a) \in \text{Range}(\ell) \subseteq B_0 = \text{Domain}(h)$ by our assumption

Note that $\text{Range}(h \circ \ell) = \{h(\ell(a)) : a \in A\}$

$= \{h(b) : b \in \text{Range}(\ell)\}$

$\subseteq \{h(b') : b' \in B_0\} = \text{Range}(h)$.

Examples 1) Recall that $\cos : \mathbb{R} \to \mathbb{R}$ takes values in $[-1,1]$, $\quad \text{Range}(\cos) = [-1,1]$.

Therefore, if $g_1(x) = \frac{1}{x-2}$, $\text{Domain}(g_1) = \mathbb{R} \setminus \{2\}$,

then we can consider the composition of g_1 with $\cos$:

$$(g_1 \circ \cos)(x) = \frac{1}{\cos(x) - 2}.$$

2) On the other hand, if $g_2(x) = \frac{x^2}{x+1}$, $\text{Domain}(g_2) = \mathbb{R} \setminus \{-1\}$

then $g_2 \circ \cos$ is not defined.

Inverse of a Function

Let $f : A \to B$ be a function, and assume f is bijective, that is, it is both injective and surjective.

Then we have that, for every $b \in B$, there is a unique $a \in A$ such that

$$b = f(a).$$

b has a preimage $a \in A$, and every other element of A is mapped to an element in B different from b.

Thus if we pair each $b \in B$ with its unique preimage in A, we get a function $g : B \to A$.

This function satisfies:

i) $g \circ f = id_A$ where $id_A : A \to A$ is the identity function on A (for every $a \in A$, $id_A(a) = a$)

and ii) $f \circ g = id_B$ where $id_B : B \to B$ is the identity function on B.

Indeed, let's confirm (i): for every $a \in A$

$$(g \circ f)(a) = g(f(a)) = \text{unique preimage of } f(a) \quad \text{by def. of } g$$

($f(a)$: an element of B)

$$= a$$

Thus, for every $a \in A$,

$$(g \circ f)(a) = id_A(a),$$

so the two functions are equal.

Given a function $f : A \to B$, if there exists a function $g : B \to A$ satisfying (i) and (ii), then we call this function g the inverse of f and usually denote it by f^{-1}.

We just saw that, if $f : A \to B$ is bijective, then f has an inverse (or in other words, it is invertible).

The converse is also true: if $f : A \to B$ has an inverse function, then f is bijective (practice)

Examples 1) $\cos : \mathbb{R} \to \mathbb{R}$ is not bijective (in fact, it is neither injective nor surjective). Therefore it cannot have an inverse.

2) On the other hand,

$$\cos: [0,\pi] \longrightarrow [-1,1]$$

is bijective, so it does have an inverse function $\cos^{-1}: [-1,1] \longrightarrow [0,\pi]$, most commonly written as arccos.

3) The conjugate function

$$\psi: \mathbb{C} \longrightarrow \mathbb{C}, \quad \psi(z) := \bar{z} = Re(z) - i\,Im(z)$$
$$\| \psi(Re(z) + i\,Im(z))$$

has an inverse function: in fact, it is (the) an inverse of itself, $\psi \circ \psi = id_{\mathbb{C}}$.

Important Remark If a function $f: A \to B$ has an inverse $f^{-1}: B \to A$, then this is unique.

Next we want to see whether, when we discuss functions that have more special properties, composition and/or taking inverses (wherever this makes sense) preserves the "nice" properties.

Proposition 1 Let F_1, F_2, F_3 be three fields:
$F_i = (\{\text{elements in } F_i\}, +_i, \cdot_i)$ for $i = 1,2,3$
and let $\varphi: F_1 \to F_2$
and $\psi: F_2 \to F_3$
be field homomorphisms. Then $\psi \circ \varphi: F_1 \to F_3$ is defined (since $Range(\varphi) \subseteq F_2 = Domain(\psi)$).
We have that $\psi \circ \varphi$ is a field homomorphism too.

Proof We have to check that $\psi \circ \varphi$ satisfies the definition of a field homomorphism. That is, we need to check that

1. for every $x, y \in F_1$

a) $(\psi \circ \varphi)(x +_1 y) = (\psi \circ \varphi)(x) +_3 (\psi \circ \varphi)(y)$

and b) $(\psi \circ \varphi)(x \cdot_1 y) = (\psi \circ \varphi)(x) \cdot_3 (\psi \circ \varphi)(y)$

and 2. $(\psi \circ \varphi)(1_{F_1}) = 1_{F_3}$.

Let $x, y \in F_1$. Then

$(\psi \circ \varphi)(x +_1 y) = \psi(\varphi(x +_1 y))$

$= \psi(\varphi(x) +_2 \varphi(y))$ — since φ is a field homomorphism from F_1 to F_2

$= \psi(\varphi(x)) +_3 \psi(\varphi(y))$ — since ψ is a field homomorphism from F_2 to F_3

$= (\psi \circ \varphi)(x) +_3 (\psi \circ \varphi)(y)$

Similarly $(\psi \circ \varphi)(x \cdot_1 y) = \psi(\varphi(x \cdot_1 y))$

φ field homom. $\rightsquigarrow = \psi(\varphi(x) \cdot_2 \varphi(y))$

ψ field homom. $\rightsquigarrow = \psi(\varphi(x)) \cdot_3 \psi(\varphi(y))$

$= (\psi \circ \varphi)(x) \cdot_3 (\psi \circ \varphi)(y)$.

Since x, y were arbitrary, we have confirmed 1. above

Moreover $(\psi \circ \varphi)(1_{F_1}) = \psi(\varphi(1_{F_1})) = \psi(1_{F_2}) = 1_{F_3}$.

Reminder

Definition Let F_1, F_2 be fields, and let $\varphi: F_1 \to F_2$ a field homomorphism. We call φ a field isomorphism if φ is bijective.

More standard definition, but equivalent:

Definition Let F_1, F_2 be fields, and let $\varphi: F_1 \to F_2$ a field homomorphism. If there exists a field homomorphism $\psi: F_2 \to F_1$ such that

$$\psi \circ \varphi = id_{F_1} \quad \text{and} \quad \varphi \circ \psi = id_{F_2},$$

we say that φ is a field isomorphism.

Terminology Two fields F_1, F_2 are called isomorphic if there exists a field isomorphism $\varphi: F_1 \to F_2$.

The two definitions are equivalent (and hence we can choose to work with the former one, the easier of the two to check) because of the following

Proposition 2 Let $F_1 = (\{\text{elements in } F_1\}, +_1, \cdot_1)$ and $F_2 = (\{\text{elements in } F_2\}, +_2, \cdot_2)$ be two fields, and let $\varphi: F_1 \to F_2$ be a field homomorphism.

Suppose φ is bijective, and hence that it has an inverse $\varphi^{-1}: F_2 \to F_1$.

Then φ^{-1} is a field homomorphism too.