Dyn. Sys. es 1

ES 1

1

claim: let G be a group with group-law $*$

proof:

if $|G| \leq 4$, then $(G, *)$ is abelian

if $|G| = 1$, then $G = \{e\}$ which is abelian

if $|G| = 2$, then $G = \{e, a\}$. Then $a*e = a = e*a$

if $|G| = 3$, then $G = \{e, a, b\}$. Then $a*e = a = e*a$, similar for b and $a*b = e = b*a$

if $|G| = 4$: suppose G is not abelian: then $\exists\ x, y \in G$ s.t. $x*y \neq y*x$

but •) $x*y \neq e \neq y*x$ since $y = x^{-1}$

•) $x*y \neq x$ and $y*x \neq x$ since $y \neq e$

•) $x*y \neq y$ and $y*x \neq y$ since $x \neq e$

thus G contains 5 distinct elements: $e, x, y, x*y, y*x$ ↯ ✓

thus G is abelian

3

let $(G, *)$ be a group

1.

claim:

proof:

let H be a subgroup

$(H, e, *)$ is a group

according to Def 0.2 we have: (i) $e \in H$; (ii) $a+b \in H\ \forall\ a, b \in H$; (iii) $-a \in H\ \forall\ a \in H$

thus $e*a = e\ \forall\ a \in G$ (neutral element)

and $a*(-a) = e$ (inv. element)

let $a, b, c \in H$, thus $a, b, c \in G$ which is a group, hence associativity is "inherited" ✓

2.

Let G a finite group.

claim: $H = \{ g^n \mid n \in \mathbb{N} \}$ is a subgroup

proof: Let $g^n, g^m \in H$, $n, m \in \mathbb{N}$. Then $g^n * g^m = g^{n+m} \in H$

we have $e \in G$, hence $e^n = e \in H$

Let $g^n \in H$, thus $g \in G$ hence $g^{-1} \in G$, thus $(g^{-1})^n \in H$ s.t.

$$g^n * (g^{-1})^n = e$$

claim: H is abelian

proof: Let $h_1 = g_1^n$, $h_2 = g_2^m \in H$; then $\underbrace{g_1 * \dots * g_1}_{n\text{-times}} * \underbrace{g_2 * \dots * g_2}_{m\text{-times}} = g_{1n} * g_{2m} \in G$

$$\Rightarrow \underbrace{g_{1n} + g_{2m}}_{\in H} = g_{2m} + g_{1m} = \underbrace{g_2 * \dots * g_2}_{m\text{-times}} * \underbrace{g_1 * \dots * g_1}_{n\text{-times}}$$

Actually $\langle g \rangle \simeq \mathbb{Z}/n\mathbb{Z}$

5

Let $(G, e, +)$ be a group

(ii)

claim: $a + e = a \quad \forall a \in G$

proof: Let $a \in G$. Then $e + a = a = a + e$ since e is neutral

(iii)

claim: $\forall a \in G \ \exists a' \in G$ with $a' + a = a + a' = e$

proof: we have $a' + a = e \iff a' + a + a' = e + a' \iff a + a' = e$

2

Let G be a finite group, H a subgroup, $gH = \{ gh \mid h \in H \}$

1.

Let $g_1, g_2 \in G$

claim: $g_1 H \cap g_2 H \neq \emptyset \Rightarrow g_1 H = g_2 H$

proof: $g_1 H = \{ g_1 h \mid h \in H \}$, $g_2 H = \{ g_2 h \mid h \in H \}$

let $g_1 h_1 = g_2 h_2 \in g_1 H \cap g_2 H$

then $g_1 g_2^{-1} = \underbrace{h_2 h_1^{-1}}_{\in H} \Rightarrow g_1 g_2^{-1} = h$

$g_1 = g_2 h$ hence $g_1 \in g_2 \Rightarrow g_1 H = g_2 H$ ●

2.

claim:

proof:

$|H|$ divides $|G|$ as integers

cosets of H in G are equivalence classes

$x \sim y \iff \exists\ h \in H$ s.t. $x = yh \quad \forall x, y \in G$

each coset aH has the same cardinality as H because $x \mapsto ax$ is a bijection $H \to aH$ with inverse $y \mapsto a^{-1} y$

thus $|G| = [G : H] \cdot |H|$ ● ✓

4

claim:

proof:

let $(G, *)$ a group, p prime

$|G| = p \Rightarrow (G, *)$ is abelian

?

ES 2

1

let $b \geq 2$.

claim: $(\mathbb{Z}/b\mathbb{Z}, +, \cdot)$ is a ring

proof: we check Def. 0.3

1. $(\mathbb{Z}/b\mathbb{Z}, +)$ is an abelian group

$a + (b+c) = [a] + ([b] + [c]) = ([a] + [b]) + [c]$ (associativity in $\mathbb{Z}$) $\forall\, a,b,c \in \mathbb{Z}/b\mathbb{Z}$

- we have $e = [b] = [0]$: $e + a = [b] + [a] = [b+a] = [a]$ $\forall\, a \in \mathbb{Z}/b\mathbb{Z}$
- let $a \in \mathbb{Z}/b\mathbb{Z}$: then $[a] + [b-a] = [a+b-a] = [b] = [0]$
- let $a, c \in \mathbb{Z}/b\mathbb{Z}$: then $[a] + [c] = [a+c] = [c+a]$ (commutativity in $\mathbb{Z}$) $= [c] + [a]$

2. associativity of multiplication

$[a] \cdot ([f] \cdot [c]) = [a] \cdot ([fc]) = [afc] = [(af)c] = [af][c]$ (associativity in $\mathbb{Z}$)

$= ([a][f]) \cdot [c]$ $\forall\, [a],[f],[c] \in \mathbb{Z}/b\mathbb{Z}$

3. distributive properties

$[a] \cdot ([f] + [c]) = [a] \cdot ([f+c]) = [a(f+c)] = [af + ac]$ (distr. in $\mathbb{Z}$)

$= [af] + [ac] = [a][f] + [a][c]$ $\forall\, [a],[c],[f] \in \mathbb{Z}/b\mathbb{Z}$

analogous for $([a] + [f])[c]$

4. identity

let $[a] \in \mathbb{Z}/b\mathbb{Z}$: then $[1][a] = [1a] = [a1] = [a][1] = [a]$ (identity in $\mathbb{Z}$)

$b = 12$: zero divisors are $2, 6, 3, 4, 8, 9, 10$ all int. not coprime with 12

$b = 7$: there are no zero divisors in $\mathbb{Z}/7\mathbb{Z}$

I guess $[a] = a + \mathbb{Z} \cdot b$

why?

2

claim: $\mathbb{Z}/b\mathbb{Z}$ is an integral domain $\iff$ b is prime

"$\Rightarrow$" Let $\mathbb{Z}/b\mathbb{Z}$ be an integral domain.

Then we can't find $c, d \in \mathbb{Z}/b\mathbb{Z}$, $c \neq b \neq d$ s.t. $c \cdot d = b$

hence b is divisible only by ± 1 and $\pm b$, thus b is prime

"$\Leftarrow$" let b be a prime number

then $\mathbb{Z}/b\mathbb{Z} = \{[0], [1], [2], \dots, [b-1]\}$

since b is prime, it is only divisible by ± 1 and $\pm b$

thus we cannot find $c, d \in \mathbb{Z}/b\mathbb{Z}$, $c \neq 0 \neq d$, s.t. $c \cdot d = b$

hence $\mathbb{Z}/b\mathbb{Z}$ is an integral domain

Not a proof

claim: a prime p satisfies: $p \mid_{\mathbb{Z}} a \cdot b \iff p \mid_{\mathbb{Z}} a$ or $p \mid_{\mathbb{Z}} b$ for $a, b \in \mathbb{Z}$

"$\Rightarrow$" we have $p \mid_{\mathbb{Z}} ab$, hence $\exists\ q \in \mathbb{Z}$ s.t. $ab = qp$

if $\frac{q}{b} \in \mathbb{Z}$, then $p \mid_{\mathbb{Z}} a$ since $a = \frac{q}{b} \cdot p$

if $\frac{q}{b} \notin \mathbb{Z}$ then $b = p$, otherwise $\frac{q}{b} \cdot p = a \notin \mathbb{Z}$

since $b = p$ we can take $q = 1$ s.t. $b = qp$ and $p \mid_{\mathbb{Z}} b$

"$\Leftarrow$" assume $p \mid_{\mathbb{Z}} a$ (up to change a and b)

hence $\exists\ q \in \mathbb{Z}$ s.t. $a = qp \iff ab = qbp \in \mathbb{Z}$

hence $ab = mp$, $m = qb \in \mathbb{Z}$

thus $p \mid_{\mathbb{Z}} ab$

3

let $R := \{ f : \mathbb{R} \to \mathbb{R} \mid f \text{ is cont. function} \}$

claim: R is a commutative ring

proof:

1. $(R, +, 0)$ is an abelian group

associativity: $f + (g+h) = f + g + h \overset{*}{=} (f+g) + h \quad \forall\, f,g,h \in R$

neutral el.: let $\mathbb{0}(x) = 0 \ \forall\, x \in \mathbb{R}$. Then $\mathbb{0} + f = f \quad \forall\, f \in R$

inverse el.: let $f \in R$. then $f + (-f) \overset{*}{=} f - f = \mathbb{0} \quad \forall\, f \in R$

abelian: $f + g = (f+g) \overset{*}{=} (g+f) = g + f \quad \forall\, f,g \in R$

according operations on $\mathbb{R}$ ✓

2. multiplication is associative

$f \cdot (g \cdot h) = f \cdot g \cdot h \overset{*}{=} (f \cdot g) \cdot h \quad \forall\, f,g,h \in R$

3. distributive properties:

$f \cdot (g+h) = \left(f \cdot (g+h)\right) \overset{*}{=} (fg + fh) = fg + fh \quad \forall\, f,g,h \in R$

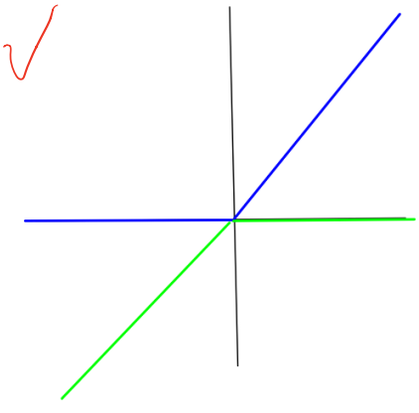
analogous for other direction

4. identity

let $\mathbb{1}(x) = 1 \ \forall\, x \in \mathbb{R}$. Then $f \cdot \mathbb{1} \overset{\text{commutativity}}{=} \mathbb{1} \cdot f = f \quad \forall\, f \in R$ ●

zero divisors: an example for a zero-divisor is:

$f(x) = \begin{cases} 0, & x \le 0 \\ x, & x \ge 0 \end{cases}$ $\qquad$ $g(x) = \begin{cases} x, & x \le 0 \\ 0, & x \ge 0 \end{cases}$ ✓



zero-divisors in R include functions that partly take value 0 and for which there exists $g \in R$ s.t. $g = 0$ whenever $f \neq 0$

Not very precise

4

claim: $\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

proof: $\mathbb{Q}[\sqrt{2}]$ is a ring

1. $\mathbb{Q}[\sqrt{2}]$ is an abelian group

$(a + b\sqrt{2}) + ((c + d\sqrt{2}) + (e + f\sqrt{2})) = a + b\sqrt{2} + (c + d\sqrt{2} + e + f\sqrt{2})$

$= a + b\sqrt{2} + c + d\sqrt{2} + e + f\sqrt{2} \overset{*}{=} (a + b\sqrt{2} + c + d\sqrt{2}) + e + f\sqrt{2}$

$\forall\, a, b, c, d, e, f \in \mathbb{Q}$

- $(a + b\sqrt{2}) + (0 + 0\sqrt{2}) = a + b\sqrt{2} + 0 = a + b\sqrt{2} \quad \forall\, a, b \in \mathbb{Q}$
- $(a + b\sqrt{2}) + (-a - b\sqrt{2}) = a - a + b\sqrt{2} - b\sqrt{2} = 0 \quad \forall\, a, b \in \mathbb{Q}$

abelian: $(a + b\sqrt{2}) + (c + d\sqrt{2}) \overset{*}{=} a + b\sqrt{2} + c + d\sqrt{2} = c + d\sqrt{2} + a + b\sqrt{2} \quad \forall\, a, b, c, d \in \mathbb{Q}$

* corresponding operation in $\mathbb{R}$

- multiplication is associative

$(a + b\sqrt{2}) \cdot ((c + d\sqrt{2})(e + f\sqrt{2})) = (a + b\sqrt{2})(c + d\sqrt{2})(e + f\sqrt{2})$

$\overset{*}{=} ((a + b\sqrt{2})(c + d\sqrt{2}))(e + f\sqrt{2}) \quad \forall\, a, b, c, d, e, f \in \mathbb{Q}$

- distributive properties:

$(a + b\sqrt{2})(c + d\sqrt{2}) + (a + b\sqrt{2})(e + f\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd + ae + af\sqrt{2} + be\sqrt{2} + 2bf$

$= [(ac + 2bd) + (ad + bc)\sqrt{2}] + [(ae + 2bf) + (af + be)\sqrt{2}] \quad \forall\, a, b, c, d, e, f \in \mathbb{Q}$

similar for other direction

- identity

$(1 + 0\sqrt{2}) \cdot (a + b\sqrt{2}) = 1 \cdot (a + b\sqrt{2}) \overset{*}{=} a + b\sqrt{2}$

●

claim: every $x \in \mathbb{Q}[\sqrt{2}] \setminus \{0\}$ is invertible, i.e. $\exists\, y \in \mathbb{Q}[\sqrt{2}] \setminus \{0\}$ s.t. $x \cdot y = 1$

proof:

$$a + b\sqrt{2} = a + b\sqrt{2} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a^2 - 2b}{a - b\sqrt{2}}$$

— we need $a \neq b\sqrt{2}$

hence $$(a + b\sqrt{2}) \cdot \frac{a - b\sqrt{2}}{a^2 - 2b} = \frac{a^2 - 2b}{a^2 - 2b} = 1$$

$\forall\, a, b \in \mathbb{Q}$ ●

ES 3

1

Let $b \geq$ an integer

characterisation of the invertible elements of $\mathbb{Z}/b\mathbb{Z}$

(i)

claim: in a finite commutative ring with unity, every element is either a unit or a zero divisor

proof: $\mathbb{Z}/b\mathbb{Z}$ is a commutative ring (ES 2)

let $a \in \mathbb{Z}/b\mathbb{Z}$. consider $\psi: \mathbb{Z}/b\mathbb{Z} \to \mathbb{Z}/b\mathbb{Z}$, $x \mapsto ax$

if ψ is injective, it must also be surjective, since $\mathbb{Z}/b\mathbb{Z}$ is finite

hence $ax = 1$ for some $x \in \mathbb{Z}/b\mathbb{Z}$ and a is a unit.

if ψ is not injective, then $\exists\ u, v \in \mathbb{Z}/b\mathbb{Z}$, $u \neq v$ s.t. $au = av$

but then $a(u-v) = 0$, hence a is a zero-divisor

zero-divisors are not invertible This is a tautology ●

(ii)

claim: $\mathbb{Z}/b\mathbb{Z}$ is a field $\Leftrightarrow$ b is prime

proof:

"$\Rightarrow$" by contraposition

assume b is not prime, hence $\exists\ a, c \in \mathbb{Z}/b\mathbb{Z} \setminus \{0\}$ s.t. $a \cdot c = b = 0$

hence a, c are zero-divisors, thus not invertible

hence $\mathbb{Z}/b\mathbb{Z}$ is not a field

"$\Leftarrow$" let b be prime, hence $\nexists\ a, c \in \mathbb{Z}/b\mathbb{Z} \setminus \{0\}$ s.t. $a \cdot c = b$ Ok

hence there are no zero-divisors

by part (i), we can deduce that all $d \in \mathbb{Z}/b\mathbb{Z}$ are invertible (Which part (i)?)

meaning that $\mathbb{Z}/b\mathbb{Z}$ is a field ●

2

Let A be an integral domain

$\mathrm{Frac}(A) = \{ \frac{a}{b} \mid a,b \in A, b \neq 0 \} / \sim$ where $\frac{a_1}{b_1} \sim \frac{a_2}{b_2} \iff a_1 b_2 - a_2 b_1 = 0$

operations: $\oplus$ $\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}$ $\forall \frac{a}{b}, \frac{c}{d} \in \mathrm{Frac}(A)$

$\odot$ $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ $\forall \frac{a}{b}, \frac{c}{d} \in \mathrm{Frac}(A)$

claim: $\oplus$ and $\odot$ are well-defined

proof: suppose $\frac{p}{q}, \frac{\hat{p}}{\hat{q}}, \frac{r}{s}, \frac{\hat{r}}{\hat{s}} \in \mathrm{Frac}(A)$ s.t. $\frac{p}{q} = \frac{\hat{p}}{\hat{q}}$ and $\frac{r}{s} = \frac{\hat{r}}{\hat{s}}$

we have to show that $\frac{ps+qr}{qs} = \frac{\hat{p}\hat{s}+\hat{q}\hat{r}}{\hat{q}\hat{s}}$ and $\frac{pr}{qs} = \frac{\hat{p}\hat{r}}{\hat{q}\hat{s}}$

we have $p\hat{q} = \hat{p}q$ and $r\hat{s} = \hat{r}s$

$$\frac{ps+qr}{qs} = \frac{ps}{qs} + \frac{qr}{qs} = \frac{p}{q} + \frac{r}{s} = \frac{\hat{p}}{\hat{q}} + \frac{\hat{r}}{\hat{s}} = \frac{\hat{p}\hat{s}+\hat{q}\hat{r}}{\hat{q}\hat{s}}$$

$$\frac{pr}{qs} = \frac{p}{q} \cdot \frac{r}{s} = \frac{\hat{p}}{\hat{q}} \cdot \frac{\hat{r}}{\hat{s}}$$

don't see the argument... ●

claim: $\mathrm{Frac}(A)$ is the smallest field containing A

proof: assume B is a field s.t. $A \subset B$ and $B \subsetneq \mathrm{Frac}(A)$

Then $\exists \frac{c}{d} \in \mathrm{Frac}(A)$ s.t. $\frac{c}{d} \notin B$, $d \neq 0$, hence also $c, d \in A$

but then $c, d \in B$ since $A \subset B$ ↯ ?? ●

3

claim: $\mathbb{Z}[i] = \{ a+bi \mid a,b \in \mathbb{Z} \}$ with the usual operations of $\mathbb{C}$ is a ring

proof: on $\mathbb{C}$ we have the following operations:

$$\oplus : \mathbb{C} \times \mathbb{C} \to \mathbb{C} \qquad ((a_1,b_1),(a_2,b_2)) \mapsto (a_1+b_1, a_2+b_2)$$

$$\odot : \mathbb{C} \times \mathbb{C} \to \mathbb{C} \qquad ((a_1,b_1),(a_2,b_2)) \mapsto (a_1a_2 - b_1b_2, a_1b_2 + b_1a_2)$$

Nullelement: $(0,0)$, Einselement: $(1,0)$

- $(\mathbb{Z}[i], +, 0)$ ist eine abelsche Gruppe

kommutativ:
$$(a,b) + ((c,d) + (e,f)) = (a,b) + (c,d) + (e,f) =$$
$$((a,b) + (c,d)) + (e,f) \qquad \forall\, a,b,c,d,e,f \in \mathbb{Z}$$

neutral el:
$$(0,0) + (a,b) = (0+a, 0+b) = (a,b) \qquad \forall\, a,b \in \mathbb{Z}$$

inv. el:
$$(a,b) + (-a,-b) = (a-a, b-b) = (0,0) \qquad \forall\, a,b \in \mathbb{Z}$$

abelsch:
$$(a,b) + (c,d) = (a+c, b+d) \overset{\text{commutativity of } + \text{ in } \mathbb{Z}}{=} (c+a, d+b) = (c,d) + (b,a)$$

- multiplication is associative

$$(a,b)((c,d)(e,f)) = (a,b)(c,d)(e,f) \overset{\text{associativity in } \mathbb{C}}{=} ((a,b)(c,d))(e,f)$$
$$\forall\, a,b,c,d,e,f \in \mathbb{Z}$$

- distributive properties

$$(a,b)\cdot((c,d)+(e,f)) = (a,b)(c+e, d+f)$$
$$= (a(c+e) - b(d+f),\ a(d+f) + b(c+e)) = (ac+ae-bd-bf,\ ad+af+bc+be)$$
$$= (ac-bd, ad+bc) + (ae-bf, af+be)$$
$$= (a,b)(c,d) + (a,b)(e,f)$$

analogous for other direction
$\forall\, a,b,c,d,e,f \in \mathbb{Z}$

identity:

$(1,0)\cdot(a,b) = (1\cdot a - 0\cdot b,\ 1\cdot b + a\cdot 0) = (a,b) \quad \forall\, a,b \in \mathbb{Z}$

same for other direction

Or: $\mathbb{Z}[i] \subseteq \mathbb{C}$ trivial

$$\mathrm{Frac}(\mathbb{Z}[i]) = \left\{ \frac{ai+b}{ci+d} \;\middle|\; ai+b,\ ci+d \in \mathbb{Z}[i],\ ci+d \neq 0 \right\} / \sim$$

where $\frac{ai+b}{ci+d} \sim \frac{a'i+b'}{c'i+d'} \iff (ai+b)(c'i+d') - (a'i+b')(ci+d) = 0$

$\forall\ ai+b,\ ci+d,\ a'i+b',\ c'i+d' \in \mathrm{Frac}(\mathbb{Z}[i])$

⊕: $\frac{ai+b}{ci+d} + \frac{a'i+b'}{c'i+d'} = \frac{(ai+b)(c'i+d') + (a'i+b')(ci+d)}{(ci+d)(c'i+d')}$

$\forall\ ai+b,\ ci+d,\ a'i+b',\ c'i+d' \in \mathrm{Frac}(\mathbb{Z}[i])$

⊙: $\frac{ai+b}{ci+d} \cdot \frac{a'i+b'}{c'i+d'} = \frac{(ai+b)(a'i+b')}{(ci+d)(c'i+d')}$

$\forall\ ai+b,\ ci+d,\ a'i+b',\ c'i+d' \in \mathrm{Frac}(\mathbb{Z}[i])$

That is not a characterization.

ES 4

1

Let A be an integral domain

Warum

Let $P, Q \in A[X]$ s.t. $PQ = 1 \Rightarrow \deg(PQ) = \deg(P) + \deg(Q) = \deg(1) = 0$

thus we must have that P and Q are non-zero constants, i.e.

$$P(X) = a \quad , \quad Q(X) = b \quad , \quad a, b \in A$$

(✓)

2

Let K be a field, $f(X) = f_n X^n + \dots + f_1 X + f_0 \in K[X]$

$f(a) := f_n a^n + \dots + f_1 a + f_0 \in K \quad , a \in K$

claim: $\deg(f) = n \Rightarrow f$ has at most n distinct roots

proof: we need the following Lemma

Lemma: $a \in K$ is a root of $f \Leftrightarrow (X-a)$ divides f

"$\Leftarrow$" assume that $(X-a)$ divides f

hence $\exists \; g \in K[X]$ s.t. $f = (x-a)\, g$

hence $f(a) = (a-a)\, g(a) = 0$ thus a is a root of p

"$\Rightarrow$" assume that a is a root of f, i.e. $f(a) = 0$

by euclidean division: $f(x) = (x-a) \cdot g(x) + r(x) \quad , \; g, r \in K[X]$

$\deg(r) < \deg(x-a) = 1$ ✓

hence $r(x) = \text{const}$ and $f(a) = (a-a) \cdot g(a) + r(a) = 0$

$\Rightarrow r(a) = 0 = r(x)$ ✓

hence $f(x) = (x-a)\, g(x) \Rightarrow (x-a) \mid f$ ●

now we go back to our main proof and proceed by induction:

$n=0$: f is a non-zero constant $\Rightarrow$ f has no roots

hypothesis: assume any $f \in K[X]$ of degree n has at most n roots.

let $p \in K[X]$ s.t. $\deg(p) = n+1$

if p has no roots, the claim follows

if p has at least one root $a \in K$, we can apply Lemma to find $q \in K[X]$ s.t. $p(x) = (x-a)\,q(x) \Rightarrow \deg(q) = n$ ✓

by hypothesis, q has at most n roots

any root of q is a root of p and if $b \neq a$ is a root of p, it must also be a root of q

thus p can at most have $n+1$ roots ●

3

for all primes, denote by $\mathbb{F}_p$ the field $\mathbb{Z}/p\mathbb{Z}$

claim: $a^p = a \mod p \quad \forall\, a \in \mathbb{F}_p$ (Fermat's little theorem)

proof:

let $a \in \mathbb{F}_p$, i.e. $1 \leq a \leq p-1$

let k be the order of a, i.e. the smallest positive int. s.t. $a^k \equiv 1 \mod p$

then $1, a, a^2, \dots, a^{k-1}$ reduced modulo p form a subgroup of $\mathbb{F}_p$ of order k

by Lagrange's Theorem, k divides the order of $\mathbb{F}_p$, which is $(p-1)$

hence $(p-1) = km$ for some $m \in \mathbb{N}$

then $a^{p-1} \equiv a^{km} = (a^k)^m \equiv 1^m \equiv 1 \pmod p$ ✓ ●

example: caridu $p = 3$, $\mathbb{Z}/3\mathbb{Z} = \{0,1,2\}$

let $f = x(x-1)(x-2) = (x^2-x)(x-2) = x^3 - 2x^2 - x^2 + 2x$

$= x^3 - 3x^2 + 2x$

$= x^3 + 2x$

$f(0) = 0^3 + 2\cdot 0 = 0$

$f(1) = 1^3 + 2\cdot 1 = 3 = 0$

$f(2) = 2^3 + 2\cdot 2 = 8 + 4 = 12 = 0$

ES 5

1

claim: Let K be a field, $P \in K[X]$ irreducible, $A, B \in K[X]$

$P \mid AB \Rightarrow P \mid A$ or $P \mid B$

proof: it suffices to prove the following statement:

claim: $P \mid AB$ and $P \nmid A \Rightarrow P \mid B$

proof: since $P \nmid A$ and P is irreducible, we have $\gcd(P, A) = 1$

hence $\exists\ s, t \in F[X]$ s.t. $1 = sA + tP$

then $B = B \cdot 1 = B(sA + tP) = \underbrace{s(AB) + (Bt)P}_{\text{RHS}}$

since $P \mid AB$, surely $P \mid \text{RHS} \Rightarrow P \mid B$ ✓ ●

2

Let $f \in F[X] \setminus \{0\}$, where F is a field

claim: Theorem 0.19

proof: we first show that f can be factored into irreducibles

if f is irreducible, we are done

if not, then $f = gh$ for some $g, h \in F[X]$ $\deg(g) < \deg(f)$, $\deg(h) < \deg(f)$

if g and h are irreducible, we are done

if not, we can factor g or h or both

we can continue like this since this process must stop for at every stage the degree goes down / Why?

uniqueness: suppose we can find two factorisations of f into irreducibles

$$p_1 p_2 p_3 \dots p_m = q_1 q_2 q_3 \dots q_n$$

since p_1 divides the LHS, it must also divide the RHS

but then p_1 must divide one of the factors on the RHS.

Up to reordering, assume $p_1 \mid q_1$

Since q_1 is irreducible, we must have $q_1 = u_1 p_1$, $u_1 = F[X]^*$ ✓

now we can replace q_1 by $u_1 p_1$ and cancel p_1 on both sides:

$$p_2 p_3 \cdots p_m = u_1 q_2 q_3 \cdots q_n$$

now we repeat the same argument with p_2 to get:

$$p_3 \cdots p_m = u_1 u_2 q_3 \cdots q_n$$

continuing this way, we eventually arrive at:

$$1 = u_1 u_2 \cdots u_m q_{m+1} q_{m+2} \cdots q_n$$

this is only possible if $m = n$ since q_i are irreducible

hence we get: $1 = u_1 u_2 \cdots u_m$ ✓

$\Rightarrow$ $p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$ up to reordering and unit factors •

ES 6

1

$(\mathbb{T}, S)$ a dynamical system

1.1

claim: let $P, Q \in Per(\mathbb{T}, S)$

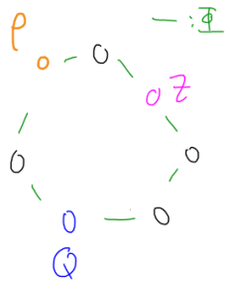
$O_{\mathbb{T}}(P) = O_{\mathbb{T}}(Q) \iff O_{\mathbb{T}}(P) \cap O_{\mathbb{T}}(Q) \neq \emptyset$

proof:

"$\Rightarrow$" by contraposition: if $O_{\mathbb{T}}(P) \cap O_{\mathbb{T}}(Q) = \emptyset$, then we cannot have $O_{\mathbb{T}}(P) = O_{\mathbb{T}}(Q)$

"$\Leftarrow$" assume $O_{\mathbb{T}}(P) \cap O_{\mathbb{T}}(Q) \neq \emptyset$

take $z \in O_{\mathbb{T}}(P) \cap O_{\mathbb{T}}(Q)$, i.e. $z = \mathbb{T}^n(P) = \mathbb{T}^m(Q)$ for some $n, m \in \mathbb{N}_0$



let a be the period of P, i.e. $\mathbb{T}^a(P) = P$

hence $n, m < a$ and $\mathbb{T}^{n-m}(P) = Q$

hence $O_{\mathbb{T}}(P) = O_{\mathbb{T}}(Q)$ Why?

2

2.1

claim: the restriction of $\mathbb{T}$ on the set $Per(\mathbb{T}, S)$ is bijective

proof: $P \in S$ is periodic for $\mathbb{T}$ if $\exists\, n > 0$ s.t. $\mathbb{T}^n(P) = P$

$\mathbb{T}|_{Per(\mathbb{T},S)} : Per(\mathbb{T}, S) \to S$

surjective: if P is a periodic point, $\mathbb{T}(P)$ is periodic as well

hence $Im\left(\mathbb{T}|_{Per(\mathbb{T},S)}\right) \subseteq$

injective: assume $\mathbb{T}(x) = \mathbb{T}(y)$, $x, y \in Per(\mathbb{T}, S)$

then $x = \mathbb{T}^n(x) = \mathbb{T}^n(y) = y$

hence $\mathbb{T}|_{Per(\mathbb{T},S)}$ is bijective

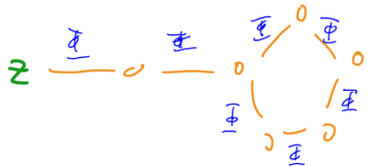
●

2.

2.1 Let S be a finite set

claim: Φ is bijective $\iff$ $Per(\Phi, S) = S$

"$\Leftarrow$" by 1.2



"$\Rightarrow$" by contraposition

assume $Per(\Phi, S) \neq S$, i.e. $\exists\ z \in S$ s.t. $z \notin Per(\Phi, S)$

then $z \in Ple\, Per(\Phi, S)$. But then Φ is not injective since $\Phi^m(z) = \Phi^{n-1}(\Phi^m(z))$ where n is the period of $\Phi^m(z)$ since S is finite •

Is this an argument?

2.2 $Per(\Phi, S) = S \Rightarrow \Phi$ bijective (where S is allowed to be infinite)

claim:

proof:

2.3 $\mathbb{R} \to \mathbb{R}$

$x \mapsto 2 \cdot x$

✓

3

Let G be a group and $\Phi : G \to G$ a homomorphism i.e. $\Phi(a \cdot b) = \Phi(a) \cdot \Phi(b)$ $\forall a, b \in G$

3.1

claim: $Per(\Phi, G)$ is a subgroup of G

proof: (i) let e be the neutral element of G

then $\Phi(a) = \Phi(a \cdot e) = \Phi(a) \cdot \Phi(e) \Rightarrow \Phi(e) = e$, i.e. $e \in Per(\Phi, G)$

(ii) let $a, b \in Per(\Phi, G)$, i.e. $\exists\, n \geq 0$ s.t. $\Phi^n(a) = a$ and $\Phi^n(b) = b$

$\Phi^n(a \cdot b) = \Phi^n(a) \cdot \Phi^n(b) = a \cdot b$, hence $a \cdot b \in Per(\Phi, G)$ ✓

(iii) let $a \in Per(\Phi, G)$. Then $\exists\, a^{-1} \in G$ s.t. $a \cdot a^{-1} = e$

$e = \Phi^n(e) = \Phi^n(a \cdot a^{-1}) = \Phi^n(a) \cdot \Phi^n(a^{-1}) = a \, \Phi^n(a^{-1})$

hence $\Phi^n(a^{-1}) = a^{-1}$ which means that $a^{-1} \in Per(\Phi, G)$

hence $Per(\Phi, G)$ is a subgroup of G •

(b)

claim: $PerPer(\Phi, G)$ is not a subgroup of G

proof: take $a, b \in PerPer(\Phi, G)$, i.e. $\Phi^{n+m}(a) = \Phi^m(a)$ and $\Phi^{k+m}(b) = \Phi^m(b)$

$\Phi^{m+k+n}(ab) = \Phi^{m+k+n}(a) \cdot \Phi^{m+k+n}(b) = \Phi^k(\Phi^m(a)) \cdot \Phi^n(\Phi^m(b)) \neq \Phi^{m+k}(ab)$ •

✗

ES 8

1

1.1

$\alpha = \frac{az+b}{cz+d}$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} z \\ 1 \end{pmatrix} = \begin{pmatrix} az+b \\ cz+d \end{pmatrix} \longmapsto \frac{az+b}{cz+d}$

$:= A$

$A^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

$A^{-1} \cdot A \cdot z = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} az+b \\ cz+d \end{pmatrix} = \frac{1}{ad-bc} \begin{pmatrix} d(az+b) - b(cz+d) \\ -c(az+b) + a(cz+d) \end{pmatrix}$

$= \frac{1}{ad-bc} \begin{pmatrix} daz - bcz \\ -caz - cb + acz + ad \end{pmatrix} = \frac{1}{ad-bc} \begin{pmatrix} z(ad-bc) \\ ad-bc \end{pmatrix} = z$

$\phi^{\alpha \circ n} = \alpha \circ \phi \circ \alpha^{-1} \circ \alpha \circ \phi \circ \alpha^{-1} \ldots =$

1.2

claim: $P \in K$ is a periodic point of ϕ $\iff$ $\alpha(P)$ is a periodic point of $\phi^{\alpha} = \alpha \circ \phi \circ \alpha^{-1}$ with same period

proof: let n be the period of P, i.e. $\phi^{\circ n}(P) = P$

$\phi^{\alpha \circ n} = \underbrace{\alpha \circ \phi \circ \alpha^{-1} \circ \alpha \circ \phi \circ \alpha^{-1} \ldots \alpha \circ \phi \circ \alpha^{-1}}_{n\text{-times}} = \alpha \circ \phi^{\circ n} \alpha^{-1}$

hence $\phi^{\alpha \circ n}(P) = \alpha \circ \phi^{\circ n}(P) \circ \alpha^{-1} = \alpha(P) \circ \alpha^{-1} = P$

1.3

$\phi(z) \in \mathbb{Q}(z)$, $\deg \phi = 2$

claim: $\exists$ unique $c \in \mathbb{Q}$ s.t. $\phi(z)$ and $z^2 + c$ are conjugate

proof: let $\alpha = \phi(\frac{x}{c}) \cdot c$ by 1.1, α is invertible hence $\phi(\frac{x}{c}) = \frac{y}{c} \iff x = \phi^{-1}(\frac{y}{c}) \cdot c$

then $\alpha \circ \phi \circ \alpha^{-1} = \phi(\frac{x}{c}) \cdot c \circ \phi \circ \phi^{-1}(\frac{x}{c}) \cdot c = \phi(\frac{x}{c}) \cdot c \cdot \frac{y}{c} \cdot c = \phi(\frac{x}{c}) \cdot cy$

to determine c, set: $\phi(\frac{x}{c}) \cdot cy \overset{!}{=} z^2 + c$

$\phi^2(\frac{x}{c}) \cdot c^2 = z^2 + c$

$\phi^2(\frac{x}{c}) c^2 - c - z^2 = 0$

look at $\phi(x-a)+a$ and $\phi(\frac{x}{c}) \cdot c$ 2 Möbiustransformationen

$\phi(\infty) = \infty$

2

$\phi_c(z) = z \quad = z^2 + c \quad \Rightarrow \quad z^2 - z + c = 0 \qquad \Delta = b^2 - 4ac = 1 - 4c$

n=1:

set c such that Δ is a square in $\mathbb{Q}$:

$1 - 4c = \left(\frac{p}{q}\right)^2$ for some $p, q \in \mathbb{Q}$

$\Leftrightarrow 1 - \frac{p^2}{q^2} = 4c$

$\Leftrightarrow \frac{1}{4} - \frac{p^2}{4q^2} = c$

c s.t. $1-4c$ ein Quadrat in $\mathbb{Q}$

also $1 - 4c > 0$

now we have infinitely many choices for p and q

n=2:

$\phi_c^2(z) = \phi_c(z^2+c) = (z^2+c)^2 + c \overset{!}{=} z$

$z^4 + 2z^2c + c^2 + c = z$

$z^4 + 2z^2c - z + c^2 + c = 0$ Subst. $z^2 = t$

$t^2 + 2tc$

$n=3$

$$\phi_c^{\circ 3}(z) = \phi_c^{\circ 2}(z^2+c) = \phi_c\left((z^2+c)^2+c\right) = \left((z^2+c)^2+c\right)^2+c$$

$$= \left(z^4+c^2+2z^2+c\right)^2 + c$$

$$=$$

1

Let p a prime integer and $|\cdot|_p$

Claim: $|\cdot|_p$ is a non-archimedean abs. value

proof: $|r|_p = p^{-v_p(r)}$ where $r = p^e \cdot \frac{a}{b}$, $r \in \mathbb{Q}$, $e, a, b \in \mathbb{Z}$, $b \neq 0$, $\gcd(a,b) = 1$, $p \nmid a$, $p \nmid b$

and $v_p(r) = e$, $v_p(0) = \infty$

1. $|r|_p = 0 \iff p^{-v_p(r)} = 0 \iff v_p(r) = \infty \iff r = 0$

2. set $x = p^n x'$ and $y = p^m y'$ s.t. $p \nmid x'y'$

then: $|xy|_p = |p^n x' p^m y'|_p = |p^{n+m} x'y'|_p = p^{-(n+m)} = p^{-n} \cdot p^{-m} = |p^n x'|_p \, |p^m y'|_p = |x|_p |y|_p$

3. wlog assume $|x|_p \geq |y|_p \Rightarrow p^{-v_p(x)} \geq p^{-v_p(y)} \Rightarrow v_p(x) \leq v_p(y)$

$\Rightarrow \min\{v_p(x), v_p(y)\} = v_p(x)$

since $v_p(x+y) \geq \min\{v_p(x), v_p(y)\} = v_p(x)$ it holds that $p^{-v_p(x+y)} \leq p^{-v_p(x)}$

$\Rightarrow |x+y|_p \leq |x|_p = \max\{|x|_p, |y|_p\}$ ●

2

Let $|\cdot|$ be an abs. value on $\mathbb{Q}$. $0 < \alpha \leq 1$

Claim: $|\cdot|^\alpha$ is an absolute value on $\mathbb{Q}$

proof: 1. $|x|^\alpha = \underbrace{|x||x|\ldots|x|}_{\alpha \text{ times}} = 0 \iff |x| = 0 \iff x = 0$ ($|\cdot|$ is abs. val.)

2. $|xy|^\alpha = \underbrace{|xy||xy|\ldots|xy|}_{\alpha \text{ times}} \overset{|\cdot| \text{ is abs. val}}{=} \underbrace{|x||y| \, |x||y| \ldots |x||y|}_{\alpha \text{ times}} \overset{\text{commutativity}}{=} |x|^\alpha |y|^\alpha$

3. $|x+y|^\alpha = \underbrace{|x+y||x+y|\ldots|x+y|}_{\alpha \text{ times}} \overset{|\cdot| \text{ is abs. val}}{\leq} (|x|+|y|)\ldots(|x|+|y|) = (|x|+|y|)^\alpha$ ●

Claim: $|\cdot|$ non-arch. $\Rightarrow$ $|\cdot|^\alpha$ non-arch.

proof: $|\cdot|$ non-arch., hence $|x+y| \leq \max\{|x|, |y|\}$

then $|x+y|^\alpha = \underbrace{|x+y|\,|x+y|\,\ldots\,|x+y|}_{\alpha \text{ times}}$ $\leq \max\{|x|,|y|\} \cdot \ldots \cdot \max\{|x|,|y|\}$ ($|\cdot|$ is non-arch.)

$= \left(\max\{|x|,|y|\}\right)^\alpha$ ●