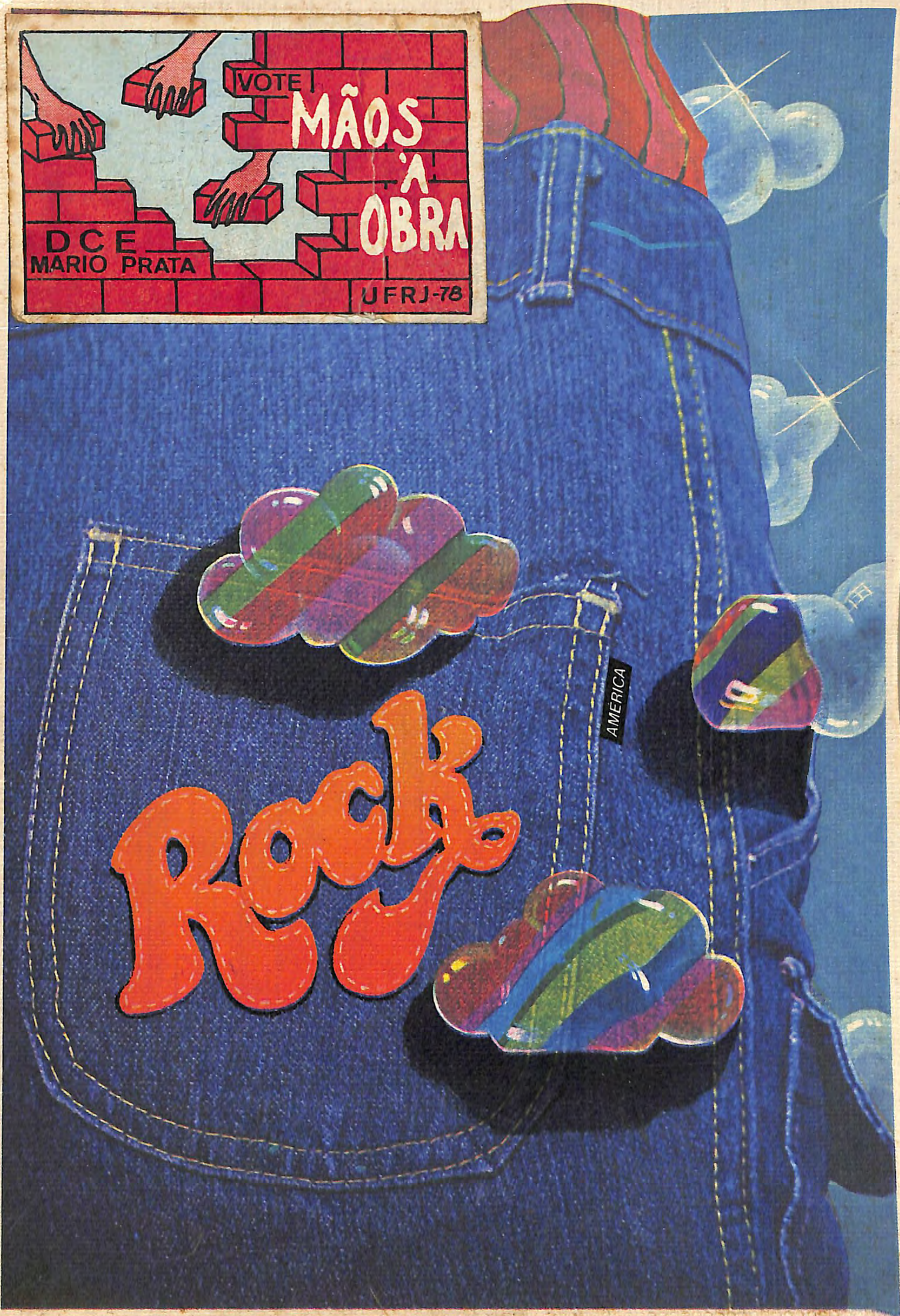

VOTE
MÃOS 'A OBRA
DCE
MARIO PRATA
UFRJ-78
AMERICA
Rock

ÍNDICE

MATÉRIA
cálculo núme-
rico

MATÉRIA
cálculo numérico

MATÉRIA
álgebra II

MATÉRIA
algebra II

ALUNO Ilenise medina de A França

N.º 7713174469 CLASSE F 0021 B-102

HORÁRIO

	SEGUNDA	TERÇA	QUARTA	QUINTA	SEXTA	SÁBADO
1.ª	8-10	algebra II		algeb II		
2.ª	10-12	cal. num		calc. num		
3.ª						
4.ª						
5.ª						

FUNDAÇÃO PROJETO RONDON
Jovens Construindo o Brasil
integrar para não entregar

TILIBRA

① Faça a tabela de multiplicacaõ da anel $Z_{10}, +, \cdot$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{9}$	$\bar{2}$	$\bar{5}$	$\bar{8}$	$\bar{1}$	$\bar{4}$	$\bar{7}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{8}$	$\bar{2}$	$\bar{6}$	$\bar{0}$	$\bar{4}$	$\bar{8}$	$\bar{2}$	$\bar{6}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{0}$	$\bar{5}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{2}$	$\bar{8}$	$\bar{4}$	$\bar{0}$	$\bar{6}$	$\bar{2}$	$\bar{8}$	$\bar{4}$
$\bar{7}$	$\bar{0}$	$\bar{7}$	$\bar{4}$	$\bar{1}$	$\bar{8}$	$\bar{5}$	$\bar{2}$	$\bar{9}$	$\bar{6}$	$\bar{3}$
$\bar{8}$	$\bar{0}$	$\bar{8}$	$\bar{6}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{8}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{9}$	$\bar{0}$	$\bar{9}$	$\bar{8}$	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}\}$

2) Quais os elementos inversíveis

são aquels que multiplicados dão 1

$\bar{1}, \bar{7}, \bar{3}, \bar{9}$

a) os subaneis de $Z_{10}, +, \cdot$

$A = \{\bar{0}, \ldots \bar{9}\}$

$F = \{\bar{0}, \bar{7}, \bar{4}, \bar{1}, \bar{5}, \bar{4}, \bar{6}, \bar{2}, \bar{8}\}$

$B - \emptyset$

$C = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$

$d = \{\bar{0}, \bar{5}\}$

② mostre que no anel Z_{24} existe elemento $x \neq q$

$x^2 = 1, \quad x \neq \bar{1} \quad x \neq \overline{23}$

$\{\bar{0}, \bar{1} \ldots \overline{23}\}$ $\quad x \cdot x = 1$

$\overline{46}$

É o $\bar{7}$

Denise Medina de A. França

③ mostre que os únicos elementos de um corpo K que satisfazem a condição $x^2 = 1$ são 1 e -1

seja $x^2 - 1 = 0 \Rightarrow (x-1)(x+1) = 0 \xRightarrow{K \text{ é corpo}} x = 1$ ou $x = -1$

⑨ mostre que um domínio de integridade finito é necessariamente um corpo.

D - domínio de integridade

D é corpo se

$\forall x, y \in D \Rightarrow xy = yx = 1$

corpo - element inverso

$D = \{x_1, \dots, x_n\}$

N.S

⑤ Quais os elementos inversíveis do anel $Q[x], +, \cdot$

$Q[x] = \{a_0 + a_1x^1 + a_2x^2 + \dots a_nx^n\}$

seja $p(x), g(x) \in Q[x]$

Para ser inversível

$p(x) \cdot g(x) = 1$

$\partial p(x) + \partial g(x) = \partial 1 = 0$

$\partial p(x) + \partial g(x) = 0 \quad \partial p(x) = 0 \; e \; \partial g(x) = 0$

$\Rightarrow p(x) = a \quad e \quad g(x) = b$

9
$\frac{\cancel{12}}{18}$

9

0

24

$\frac{13}{\times 2}$
46

$\{0, 1,$ 23$\}$
24 25

9 - 2
2

$\{0,$ 9$\}$
10

Rio, 11/5/78

1 - Sejam $A, +, \cdot$ e $S, +, \cdot$ dois anéis. Uma aplicação $f: A \to S$ é um homomorfismo se

$$\begin{cases} f(a+b) = f(a) + f(b) \\ f(a.b) = f(a)\,f(b) \end{cases}$$

① Seja $f: \mathbb{Z} \to \mathbb{Z}$ definida por $f(x) = 2x$, $x \in \mathbb{Z}$. f é um homomorfismo.

$f(x+y) = 2x + 2y = 2(x+y)$ (V)

$f(x) + f(y) = 2x + 2y = 2(x+y)$ (V)

$f(xy) = 2xy$

$f(x).f(y) = 2x.2y = 4xy$

$2xy \neq 4xy$ (F)

não é homomorfismo

② Seja $\phi: \mathbb{Q}[x] \to \mathbb{Q}$ definida por $\phi(g(x)) = g(2)$, $g(x) \in \mathbb{Q}[x]$

ϕ é um homomorfismo?

- $f(a+b) = f(a) + f(b)$

$\phi(g(x) + f(x)) = \phi(g+f)(x) = \phi(g+f)(2) = g(2) + f(2)$

$\phi g(x) + \phi f(x) = g(2) + f(2)$

- $f(ab) = f(a).f(b)$

$\phi(g(x).f(x)) = \phi(g.f)(x) = \phi(g.f)(2) = g(2)\,f(2)$

$\phi(g(x)).\phi(f(x)) = g(2).f(2)$

③ Seja $\phi : C[0,1] \to \mathbb{R}$ definida por $\phi(f) = f(1/3)$

mostre que.

(a) ϕ é um homomorfismo

$\theta(f+g) = f(\frac{1}{3}) + g(\frac{1}{3})$

$\theta(f) + \theta(g) = f(\frac{1}{3}) + g(\frac{1}{3})$ //

$\theta(f \cdot g) = f(\frac{1}{3}) \cdot g(\frac{1}{3})$

$\theta(f) \cdot \theta(g) = f(\frac{1}{3}) g(\frac{1}{3})$

(b) é sobjetiva?

$C(0,1] \longrightarrow \mathbb{R}$ Dado $a \in \mathbb{R}$ $\exists ? g \in C(0,1)$

seja $\phi[0,1] \to f(x) = a$

$\phi(g) = a$

$g(\frac{1}{3}$

ϕ é continua e $\phi f(f) = f(\frac{1}{3}) = a$

como a e qq então achamos uma $\phi f q$

$\phi(f) = a$

c) $A : C[0,1] \to \mathbb{R}$ $\quad g : C(0,1) \to \mathbb{R}$

$x \mapsto 1$ $\quad x \mapsto 3x$

vimos que $\phi(f) = f(\frac{1}{3}) = 1$

$\theta(g) = g(\frac{1}{3}) = 1$

$\phi(f) = \phi\, g(x)$ mas $f \neq g$

④. Seja $f : A \to B$ um homomorfismo de anéis

mostre que $f(0) = 0$; $f(-x) = -f(x)$ $\forall x \in A$

- $f(0) = f(0+0) = f(0) + f(0) = 0 + 0 = 0$

- $f(-x) + f(x) = f(-x+x) = f(0) \overset{por (0)}{=} 0$ //

$\Rightarrow f(-x) = -f(x)$

5) Seja $f : A \to S$ um hom de anéis, mostre que

f é injetiva $\Leftrightarrow [f(x) = 0 \to x = 0]$

6) Seja $f : \mathbb{Z} - \mathbb{Z}_n$, $f(x) = \bar{x}$

mostre que f é um hom. sobre $\mathbb{Z}_n$

Calcule $f^{-1}(\bar{0}) = \{x$

$f : A \to B$ homo

$f(a+b) = f(a) - f(b)$

$f(ab) = f(a) \cdot f(b)$

$\forall a, b \in A$

$f : A \to B$ é um homomorfismo, então

$f(0) = 0$, $f(-x) = -f(x)$

$f(A) = \{f(x) \mid x \in A\}$ é um subanel de B

dem:

$f(0) = f(0+0) = f(0) + f(0) = 0 f(0)$

$f(-x) = -f(x) \Rightarrow f(-x - 6x) = f(0) = 0$ //

$f(A)$ é subanel

5) $f: A \to B$ hom de anéis

f é injetiva $\iff [f(x)=0 \Rightarrow x=0]$

$[f(a)=f(b) \Rightarrow a=b]$

$\forall a, b \in A$ ($\Rightarrow$) sup. que f é injetiva

seja $x \in A$ tq

$f(x)=0$ então $f(x)=f(0)=0$ logo $x=0$

($\Leftarrow$) sup que sempre que $f(x)=0$, $x \in A$

Sejam $a, b \in A$ com $f(a)=f(b)$

Então $f(a)-f(b)=0$ e como f é homomorfismo,
$f(a-b)=0$ logo por hipótese
$a-b=0$, i e, $a=b$
f é injetiva

6) $f: \mathbb{Z} \to \mathbb{Z}_n$, $f(x)=\bar{x}$
f é um hom. sobre $\mathbb{k}$

calcule $f^{-1}(0) = \{x \in \mathbb{Z} \mid f(x) = \bar{0}\}$

$f(x+y) \overset{df}{=} \overline{x+y} = \bar{x}+\bar{y} \ (\Leftarrow) \underset{df}{=} f(x)+f(y)$

$f(xy) = \overline{xy} = \bar{x}\bar{y} = f(x) \cdot f(y)$

Dado $\bar{a} \in \mathbb{Z}_n$ basta tomar $a \in \mathbb{Z}$ e

temos $f(a) = \bar{a}$

$f^{-1}(0) = \{x \in \mathbb{Z} / f(x) = \bar{0}\} = \{x \in \mathbb{Z} / \bar{x} = \bar{0}\} =$

$= \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{n}\}$

ñ é injetiva

$= \{x \in \mathbb{Z} / x-0 = nk$ p/algum $k \in \mathbb{Z}\} = n\mathbb{Z}$

— // —

O único homomorfismo bijetivo de $\mathbb{R}$ sobre $\mathbb{R}$ é a identidade

dem. Seja $f: \mathbb{R} \to \mathbb{R}$ um homomorfismo bijetivo

Queremos mostrar que $f(x) = x \ \forall x \in \mathbb{R}$
Primeiro mostraremos que $f(n) = n \ \forall n \in \mathbb{Z}$
$\in \mathbb{Z}$ (por indução

$\vdash \forall n \geq 0$, $f(n) = n$

$f(0) = 0$
$f(1) = f(1.1) = f(1) \cdot f(1) \underset{\substack{f(1) \neq 0 \\ pois f \\ é\ injetiva}}{\Longrightarrow} f(1) = 1$

Sup: que $n \geq 1$ e $f(n-1) = n-1$

$f(n) = f((n-1)+1) = f(n-1) + f(1) = (n-1)+1 = n$

$\vdash \forall n < 0 \quad f(n) = n$

Se $n < 0$, $-n > 0$ $f(-n) = -n$

mas $f(-n) = -f(n)$ $\therefore$ $f(n) = n$
$f(n) = n$
$f(n) \ \forall n \in \mathbb{Z}$

$\vdash$ Se $a \neq 0$ em $\mathbb{R}$, $f(a)^{-1} = f(a^{-1})$

dem:

$f(a) f(a^{-1}) = f(a a^{-1}) = f(1) = 1$
$f(a^{-1}) = f(a)^{-1}$

|

5) $f: A \to B$ hom de anéis

f é injetiva $\iff [f(x)=0 \Rightarrow x=0]$

$[f(a)=f(b) \Rightarrow a=b]$

$\forall a, b \in A$ ($\Rightarrow$) sup. que f é injetiva

seja $x \in A$ tq

$f(x)=0$ então $f(x)=f(0)=0$ logo $x=0$

($\Leftarrow$) sup que sempre que $f(x)=0$, $x \in A$

sejam $a, b \in A$ com $f(a)=f(b)$

Então $f(a)-f(b)=0$ e como f é homomorfismo,
$f(a-b)=0$ logo por hipótese
$a-b=0$, ie, $a=b$
f é injetiva

6) $f: \mathbb{Z} \to \mathbb{Z}_n$, $f(x)=\bar{x}$
f é um hom - sobre κ

calcule $f^{-1}(0)=\{x \in \mathbb{Z} \mid f(x)=\bar{0}\}$

$f(x+y) \overset{df}{=} \overline{x+y} = \bar{x}+\bar{y} \underset{df}{\iff} f(x)+f(y)$

$f(xy)=\overline{xy} = \bar{x}\bar{y} = f(x).f(y)$

Dado $\bar{a} \in \mathbb{Z}_n$ basta tomar $a \in \mathbb{Z}$ e

temos $f(a)=\bar{a}$

$f^{-1}(0)=\{x \in \mathbb{Z} / f(x)=\bar{0}\} = \{x \in \mathbb{Z} / \bar{x}=\bar{0}\} =$

$=\{x \in \mathbb{Z} \mid x \equiv 0 \pmod n\}$

ñ é injetiva

$=\{x \in \mathbb{Z} / x-0 = nk$ p/algum $k \in \mathbb{Z}\} = n\mathbb{Z}$

— // —

O único homomorfismo bijetivo de $\mathbb{R}$ sobre $\mathbb{R}$ é a identidade

dem: Seja $f: \mathbb{R} \to \mathbb{R}$ um homomorfismo bijetivo

Queremos mostrar que $f(x)=x$ $\forall x \in \mathbb{R}$
Primeiro mostraremos que $f(n)=n$ $\forall n \in \mathbb{Z}$
$\in \mathbb{Z}$ (por indução

$\vdash$. $\forall n \geq 0$, $f(n)=n$

$f(0)=0$
$f(1)=f(1.1)=f(1).f(1) \underset{\substack{f(1) \neq 0 \\ pois f \\ é injetiva}}{\Longrightarrow} f(1)=1$

Sup: que $n \geq 1$ e $f(n-1)=n-1$

$f(n)=f((n-1)+1) = f(n-1)+f(1)=(n-1)+1=n$

$\vdash$ $\forall n<0$ $f(n)=n$

Se $n<0$, $-n>0$ $f(-n)=-n$

mas $f(-n)=-f(n)$ $\therefore$ $-f(n)=-n$
$f(n)=n$
$f(n)$ $\forall n \in \mathbb{Z}$

$\vdash$ Se $a \neq 0$ em $\mathbb{R}$, $f(a)^{-1}=f(a^{-1})$

dem:

$f(a)f(a^{-1})=f(aa^{-1})=f(1)=1$
$f(a^{-1})=f(a)^{-1}$

$f(a^{-1}) = f(a)^{-1}$

Sejam $n, m \in \mathbb{Z}$, $m \neq 0$

Então $f\left(\frac{n}{m}\right) = f(n \cdot m^{-1})$

$= f(n) \cdot f(m^{-1})$

$= f(n) \cdot f(m)^{-1}$

$= n \cdot m^{-1} = n/m$

$\vdash$ $a < b \Rightarrow f(a) < f(b)$

$a < b \Rightarrow b - a > 0$

seja $\alpha = \sqrt{b-a} \in \mathbb{R}$

Então $\alpha^2 = b - a$ e teremos

$0 < f(\alpha)^2 = f(\alpha) \cdot f(\alpha) = f(\alpha^2) = f(b-a)$

$f(\alpha) \neq 0$

$\therefore$

$f(a) < f(b)$

Seja $a \in \mathbb{R}$ e sup. que $a \neq f(a)$ digamos que $a < f(a)$ seja $q \in \mathbb{Q}$ tq
$a < q < f(a)$

$a < q < f(a)$

$a < q \Rightarrow f(a) < f(q) = q$.

Contradição f fixa os racionais

7) $f: A \to B$ um homomorfismo de anéis, mostre que $f^{-1}(0) = \{x \in A / f(x) = 0\}$ é um ideal de A
D

i) $D \neq \emptyset$ - óbvio
$\forall f(x) \in D$ $f(x) = 0 \in D$

ii) $f(x), g(x) \in D \overset{?}{\Rightarrow} f(x) - g(x) \in D$?

$\underset{0}{\overset{\in D}{f(x)}} - \underset{0}{\overset{\in D}{g(x)}} = 0 + 0 = 0 \in D$

ii) $h(x) \in A$ e $f(x) \in D \overset{?}{\Rightarrow} h(x) \cdot f(x) \in D$

$h(x) \cdot f(x) = h(x) \cdot 0 = 0 \in D$ //

Rio, 18/5/78

adjunção de Raízes

Exemplo:

L
$\cup$
K é corpo, L é corpo
L é extensão de K.

$x - \alpha \in L[x]$
$f(x) \in K[x]$
tq $f(\alpha) = 0$

$\mathbb{R} \ni \sqrt{3}$
|
$\mathbb{Q}$
π 3,14 ñ satisfaz

$f(x) = x^2 - 3 \in \mathbb{Q}[x]$
$f(\sqrt{3}) = 0$

- K = corpo ; $L \supset K$ uma extensão de K.
$\alpha \in L$ é algébrico sobre K se $\exists f(x) \in K[x] - \{0\}$ tq $f(\alpha) = 0$; caso contrário α é transcendente sobre K.

Se $\alpha \in L$ é algébrico sobre K, seja $p(x) \in K[x]$

o polinômio mônico de menor grau tq:

$p(\alpha)=0$

Então $p(x)$ é irredutível
$p(x)$ é único $Irr(\alpha, K) = p(x)$

-x-

Teorema:

Seja $\alpha \in L \supset K$ seja $K[\alpha]=\{f(\alpha) \mid f(x) \in K[x]\}$

Definimos $K[x] \xrightarrow{\varphi} L$
$f(x) \mapsto f(\alpha)$

φ é um homomorfismo

$\varphi(f \cdot g) = (f \cdot g)(\alpha) = f(\alpha) \cdot g(\alpha) = \varphi(f)\,\varphi(g)$

$\left(\varphi\left(\sum_{i=0}^{m} a_i x^i\right) = \sum_{i=0}^{m} a_i \alpha^i\right)$

Então
(i) $Im(\varphi) = K[\alpha]$

ii) α é transcendente sobre $K \Rightarrow \{f \in K[x] \mid f(\alpha)=0\}=(0)$

iii) se α é algébrico e $p(x) = Irr(\alpha, K)$, então $p(x) \cdot K[x]$ é um ideal maximal e $p(x) \cdot K[x] = \{f(x) \in K[x] \mid f(\alpha)=0\}$

$h(\alpha)=0$
$h(x) = p(x) \cdot q(x) + r(x)$

então $r(\alpha)=0$
se $r \neq 0$; $\partial r < \partial p$ * logo $r=0$

corolário → se $\alpha \in L \supset K$ é algébrico sobre K, então $K[\alpha]$ é um corpo

dem: $K[\alpha]$ é um subanel de L

i) $0 \in K[\alpha]$
ii) $f(\alpha) - g(\alpha) = (f-g)(\alpha) \in K[\alpha]$, $\forall f, g \in K[x]$
iii)

$K \subset K[\alpha] \subset L$

obs: dado $a \in K$, o polinômio cte $f(x)=a$ e tq $f(\alpha)=a \therefore a \in K[\alpha]$
Em particular $1 \in K[\alpha]$

K é um subanel de L. Sendo L um corpo é imediato que $K[\alpha]$ é um domínio de integridade

Inversos?
Seja $g(\alpha) \in K[\alpha]$ tq $g(\alpha) \neq 0$
vamos mostrar que $\exists h(\alpha) \in K[x]$ tq $g(\alpha) h(\alpha) = 1$

Como $g(\alpha) \neq 0$; temos que $Irr(\alpha, K) \nmid g(x)$

Sendo $\underbrace{Irr(\alpha, K)}_{=p(x)}$ irredutível concluímos que
$MDC(p(x), g(x)) = 1$

Logo, $\exists h(x), t(x) \in K[x]$ tq $h(x) \cdot p(x) + t(x) \cdot g(x) = 1$

$\therefore h(\alpha) \underbrace{p(\alpha)}_{0} + t(\alpha) \cdot g(\alpha) = 1$

importante!
Se $\alpha \in L \supset K$ é algébrico sobre K, e $\partial(Irr(\alpha, K))=n$
então $K[\alpha] = \{a_0, a_1\alpha + \ldots a_{n-1}\alpha^{n-1} \mid a_i \in K, i=0, \ldots n-1\}$

$$\begin{array}{c} \mathbb{R} \ni \sqrt[3]{2} \\ | \\ \mathbb{Q} \end{array} \quad x^3-2 = Irr(\sqrt[3]{2}, \mathbb{Q})$$

$\mathbb{Q}[\sqrt[3]{2}] = \{f(\sqrt[3]{2}) \mid f(x) \in \mathbb{Q}[x]\}$

$\mathbb{Q}[\sqrt[3]{2}] = \{a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2\}$

$f(\alpha) \in K[\alpha]$, $f(x) \in K[x]$, $f(\alpha) = Irr(\alpha, K)\, q(x) + r(x)$

Resumo

$$\begin{array}{c} L \\ \downarrow K[\alpha] \\ K \end{array}$$

Rio, 23/5/78

$\alpha \to$ algébrico sobre $K \to \exists f(x) \in K[x]-\{0\}$ tq $f(\alpha)=0$

$Irr(\alpha, K) = p(x)$

$K[\alpha] = \{f(\alpha) \mid f \in K[x]\}$ corpo se α é algébrico

prop: Seja $\alpha \in L \supset K$, α algébrico sobre K. Se $\partial(Irr(\alpha, K)) = n$ então

(1) Se $f(x) \in K[x]$, então $f(\alpha)$ pode ser escrito de maneira única como

$f(\alpha) = a_0 + a_1\alpha + \dots a_{n-1}\alpha^{n-1}$ onde $a_0 \dots a_{n-1} \in K$

dem Se $f(x) \in K[x]$, $f(x) = Irr(\alpha, K)\, q(x) + r(x)$ onde $r(x)=0$ ou $r(x) = a_0 + a_1 x + \dots a_{n-1}x^{n-1}$ segue que

$$\left.\begin{array}{l} f(\alpha) = a_0 + a_1\alpha \dots + a_{n-1}\alpha^{n-1} \\ f(\alpha) = b_0 + b_1\alpha \dots + b_{n-1}\alpha^{n-1} \end{array}\right\} 0 = (b_0 - a_0) + (b_1 - a_1)\alpha + \dots (b_{n-1} - a_{n-1})\alpha^{n-1}$$

α raiz de $\sum_{i=0}^{n-1} (b_i - a_i)x^i = g(x)$

como $\partial g < \partial\, irr(\alpha, K)$ se $g \neq 0$, devemos ter $g = 0$ $\therefore a_i = b_i$, $i = 0, \dots n-1$.

2. $K[\alpha] = \{a_0 + a_1\alpha + \dots a_{n-1}\alpha^{n-1} \mid a_0, \dots a_{n-1} \in K\}$

3 - Se $K = Z_p$, p primo, então $K[\alpha]$ é um corpo com p^n elementos.

Z_p tem p elementos, $Z_p[x] \to \underbrace{Z_p \times \dots \times Z_p}_{n \text{ vezes}}$

$a_0 + a_1 x + \dots a_{n-1}x^{n-1} \to (a_0, \dots a_{n-1})$

$$\begin{array}{c} \alpha \in L \\ | \\ Z_p[\alpha] \\ | \\ Z_p \end{array} \qquad n = \partial\, irr(\alpha, Z_p)$$

$\mathbb{C}$ corpo dos complexos
K subcorpo de $\mathbb{C}$

Teorema: $\mathbb{C}$ é um corpo algebricamente fechado (isto é, todo $f(x) \in \mathbb{C}[x]$ possui todas as raízes em $\mathbb{C}$)

consequência $\to$ Se $f(x) \in K[x]$ e $\alpha_1 \dots \alpha_r \in \mathbb{C}$ são as raízes distintas de f

então $f(x) = a(x-\alpha_1)^{m_1}(x-\alpha_2)^{m_2} \dots (x-\alpha_r)^{m_r}$ em $\mathbb{C}[x]$ onde $a \in K$ e $r, m_1 \dots m_r$ são inteiros positivos.

$f(x) = (x-\alpha_1)g(x)$; se $g(\alpha_1)=0$, $g = (x-\alpha_1)h(x)$

—//—

m_i é a multiplicidade de raiz α_i

$\alpha \in \mathbb{C}$, $f(x) \in K[x]$

α é uma raiz simples de f se tem multiplicidade 1

$f(x) = a_0 + a_1 x \dots a_n x^n$

$f'(x) = a_1 + 2a_2 x + \dots n a_n x^{n-1}$

prop: Seja $f(x) \in K[x]$, $\partial f(x) = n \geq 1$
Seja $\alpha \in \mathbb{C}$ uma raiz de $f(x)$

(1) α é uma raiz simples de $f(x) \iff f'(\alpha) \neq 0$

(2) se $f(x)$ é irredutível, todas as raízes de $f(x)$ são simples.

dem: raiz de $f(x) \Rightarrow f(x) = (x-\alpha)^m g(x)$ $m \geq 1$
multiplicidade de α

$f'(x) = m(x-\alpha)^{m-1} g(x) + (x-\alpha)^m \cdot g'(x)$

Se $m = 1$, $f'(x) = g(x) + (x-\alpha)\, g'(x)$ $(g(\alpha) \neq 0)$

conclusão
$f'(\alpha) \neq 0 \Leftrightarrow m = 1$

(2) suponhamos que f é um pol irredut.

seja $\alpha \in \mathbb{C}$ uma raiz de $f(x)$

seja $p(x) = \mathrm{Irr}(\alpha, K)$. Então $\exists\, h(x) \in K[x]$ tq $f(x) = p(x) \cdot h(x)$ como $f(x)$ é irredutível
$h(x) = a = $ cte
$f(x) = a\, p(x)$

$f'(\alpha) = a\, p'(\alpha)$
se $0 = f'(\alpha) = a\, p'(\alpha) \Rightarrow$ (como $a \neq 0$), $p'(\alpha) = 0$

Contradição! pois $p' \neq 0$ e $\partial p' < \partial p$

Logo $f'(\alpha) \neq 0$ e pelo item 1, α é uma raiz simples de f

$x^3 - 2 \in \mathbb{Q}[x]$, $\alpha = \sqrt[3]{2}$, $\beta = \sqrt[3]{2}$

$\left(\frac{1}{2}\left(\frac{\sqrt{3}}{2} i\right)\right)$ $\beta = \sqrt[3]{2}\left(-\frac{1}{2} - \frac{\sqrt{3}}{2} i\right)$

Sup. $\beta \in \mathbb{Q}[\sqrt[3]{2}]$; então $\frac{1}{\sqrt[3]{2}} \beta = -\frac{1}{2} + \frac{\sqrt{3}}{2} i \in \mathbb{Q}[\sqrt[3]{2}]$ então $\sqrt{3}\, i \in \mathbb{Q}[\sqrt[3]{2}]$

$\mathbb{Q}[\sqrt[3]{2}] = \{ f(\sqrt[3]{2}) \mid f \in \mathbb{Q}[x] \}$

$a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$

Essas raízes estão em $\mathbb{C} \supseteq \mathbb{Q}[\sqrt[3]{3}][\beta] \leftarrow \mathbb{Q}[i\ldots$

Rio, 30 de maio de 1978

Para que todas as equações quadráticas tenham solução precisamos introduzir a <u>unidade imaginária</u>, $i = \sqrt{-1}$

Um número (introduzido formalmente) da forma $a + bi$, $a, b \in \mathbb{R}$; é chamado nº complexo

$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ conj de todos os nºs complexos.

Dois nºs complexos $a + bi$ e $c + di$ são iguais $\Leftrightarrow$ $a = c$ e $b = d$

Dois nºs complexos que diferem apenas no sinal de suas partes imaginárias (p.e. $a + bi$ e $a - bi$) são ditos conjugados.

Em $\mathbb{C}$ definimos duas operações

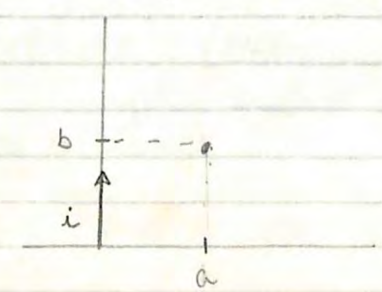
$(a+bi) + (c+di) = (a+c) + (b+d)i$

$(a+bi)(c+di) = (ac-bd) + (ad+bc)i$

com essas operações esse conj é 1 anel.

Representação geométrica dos nºs complexos.

Representamos o nº complexo $a+bi$ pelo pto $P(a+bi)$ de coordenadas (a, b). Em particular i é representado por $(0,1)$



Em R^2 podemos definir 2 operações

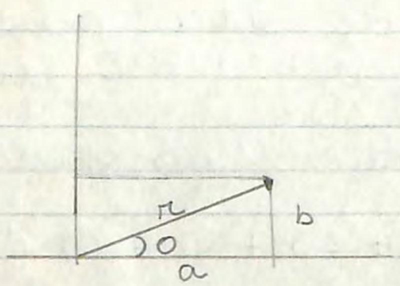
$(a,b) + (c,d) = (a+c, b+d)$

$(a,b)(c,d) = (ac-bd, ad+bc)$

a aplicação $\varphi : \mathbb{C} \to R^2$
$a+bi \mapsto (a,b)$
é um homomorfismo injetivo e sobrejetivo

Portanto $\mathbb{C} \cong R^2$

Representação trigonométrica (polar



$r = \sqrt{a^2+b^2}$

$a = r\cos\theta$

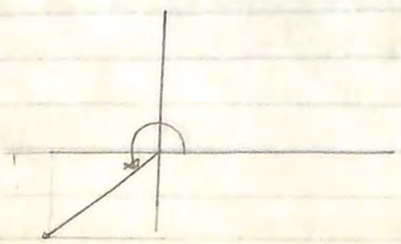
$b = r \operatorname{sen}\theta$ $\quad tg\theta = \frac{b}{a}$

Então $a+bi = r(\cos\theta + i\operatorname{sen}\theta)$

O comprimento r é chamado modulo do nº complexo $a+bi$ e denotado por $|a+bi|$

Exemplo $-3-3i \in \mathbb{C}$ $\quad |-3-3i| = \sqrt{9+9} = \sqrt{18}$

então
$-3-3i = 3\sqrt{2}(\cos 225° + i \operatorname{sen} 225°)$



Exemplo 2 $\quad 3-4i \in \mathbb{C}$

$tg\theta = \frac{-4}{3}$

$\theta = 306.9$

$|3-4i| = \sqrt{25} = 5$

$3-4i = 5(\cos 306.9 + i \operatorname{sen} 306.9)$

$a+bi = r_1(\cos\theta_1 + i\operatorname{sen}\theta_1)$; $c+di = r_2(\cos\theta_2 + i\operatorname{sen}\theta_2)$

$(a+bi)(c+di) = r_1 r_2 [(\cos\theta_1\cos\theta_2 - \operatorname{sen}\theta_1\operatorname{sen}\theta_2) + (\cos\theta_1\operatorname{sen}\theta_2$
$+ \operatorname{sen}\theta_1\cos\theta_2)] =$
$= r_1 r_2 [\cos(\theta_1+\theta_2) + i\operatorname{sen}(\theta_1+\theta_2)]$

Teorema de Moivre

$[r(\cos\theta + i\operatorname{sen}\theta)]^n = r^n(\cos n\theta + i \operatorname{sen} n\theta)$

Raízes de números complexos

Para encontrar as raízes n-ésimas de um nº complexo $a+bi$, escreveremos primeiro o nº da forma trigonométrica geral

$a+bi = |a+bi|(\cos\theta + k360° + i\operatorname{sen}\theta + k360°)$

Consideremos os números $\sqrt[n]{|a+bi|}\left[\cos\left(\frac{\theta + k360}{n}\right) + i\operatorname{sen}\left(\frac{\theta + k360°}{n}\right)\right]$ $\quad k = 0, 1, \ldots, n-1$

É fácil ver (usando de Moivre) que estes números são n raízes distintas de $a+bi$ na verdade estas são as raízes de $a+bi$. De fato suponhamos que $R(\cos\alpha + i\operatorname{sen}\alpha)$ é uma raiz n-ésima de $a+bi$

Então $(R(\cos\alpha + i\operatorname{sen}\alpha))^n =$

$= R^n(\cos n\alpha + i\operatorname{sen} n\alpha) =$

$= |a+bi| \, (\cos \theta + K\cdot 360° + i \, sen\, \theta + K\, 360)$

Logo $R^n = |a+bi|$ e $n\alpha = \theta + K\cdot 360°$

e temos $R = \sqrt[n]{|a+bi|}$, $\alpha = \frac{\theta + K\cdot 360}{n}$

e esta raiz é da forma já considerada.

"Todo nº complexo $a+bi = r(\cos\theta + i\, sen\,\theta)$, exceto zero, possui n raízes n-ésimas, a saber

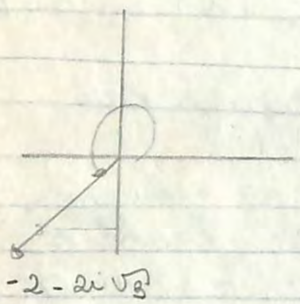
$r^{1/n} = [\cos(\frac{\theta + K\cdot 360°}{n}) + i\, sen\,(\frac{\theta + K\cdot 360°}{n})]$ $K = 0, 1, \ldots n-1$" $n = m$

Encontrar as raízes do polinomio $x^4 - (2 - 2i\sqrt{3})$

$x^4 - (2 - 2i\sqrt{3}) = 0$

$|-2-2\sqrt{3}\, i| = 4$

$-2-2\sqrt{3}\, i = 4(\cos\theta + i\, sen\,\theta)$



$-2-2i\sqrt{3}$

$\theta = 240°$

$\sqrt[4]{-2-2\sqrt{3}\, i} = \sqrt[4]{4}\, (\cos \frac{240 + K\, 360}{4} + i\, sen \frac{240+K\,360}{n}$

$K = 0, 1, \ldots n-1$

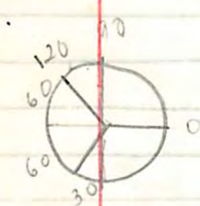
p/ $K=0$ obtemos $\sqrt{2}\, (\cos 60 + i\, sen\, 60) =$

$= \sqrt{2}\, (\frac{1}{2} + i\frac{\sqrt{3}}{2})$

b) Encontrar as raízes cúbicas de 8 e representá-las graficamente

Em geral a interpretação gráfica das raízes n-ésimas de um nº complexo $r(\cos\theta + i\, sen\,\theta)$ serão pts em um círculo de raio $\sqrt[n]{r}$ de centro na origem.

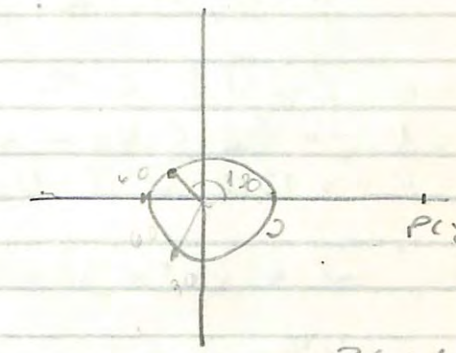
Um ponto representando uma raiz n-ésima é determinado pelo angulo $\frac{\theta}{n}$ e pelo circulo de centro na origem e raio $\sqrt[n]{r}$. As outras raízes serão pts igualmente espaçadas $\frac{360°}{n}$ a partir da 1ª raiz



b) $8 = 8 + 0i$

$= 8(\cos 0 + i\, sen\, 0)$

$\sqrt[3]{8} = 2($



$360/3 = 120$

Rio 1/6/78

Recordamos que se $\alpha \in L \supset K$ é algebrico sobre K, então $K[\alpha] = \{f(\alpha) \mid f(x) \in K[x]\}$ $= \{a_0 + a_1\alpha + \ldots \alpha^{n-1}\}$ de maneira única onde $n = \partial(Irr(\alpha, K))$

Por ex $\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}] = \{a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2\} \subset \mathbb{R}$

Ex: Seja $\mathbb{Q}[x]$ o anel de polinomios em x sobre $\mathbb{Q}$

$\mathbb{Q}[x]$ é 1 domínio de integridade

$\mathbb{Q} \subset \mathbb{Q}[x] \subset \mathbb{Q}(x)$ corpo das funções racionais em x sobre $\mathbb{Q}$.

$\mathbb{Q}(x) \ni x$ — x é transcendente sobre $\mathbb{Q}$

$\mathbb{Q}$

De fato se $a_0 + a_1 x + \ldots a_n x$ então $a_0 = a_1 = \ldots a_n = 0$

Se x é algebrico sobre $\mathbb{Q}$ então $\exists$ polinomio não nulo $f(y) \in \mathbb{Q}(y)_n$ tq $f(x) = 0$

Digamos que $f(y) = \sum_{i=0}^{n} a_i y^i$, então

$f(x) = \sum_{i=0}^{n} a_i x^i = 0$

Logo $a_0 = a_1 = \dots = a_n = 0$ contradição pois $f(y) \neq 0$

Ex

seja β uma raiz cubica de 2, $\beta \notin \mathbb{R}$

$2 = 2 + 0i = 2(\cos 0 + i \operatorname{sen} 0)$

$\sqrt[3]{2} = \sqrt[3]{2}\left(\cos k\frac{360}{3} + i \operatorname{sen} k\frac{360}{3}\right)$

$k = 0, 1 \dots 2.$

$k=0 \to \sqrt[3]{2} \in \mathbb{R}$
$k=1 \to \sqrt[3]{2}(-1/2 + i\sqrt{3}/2)$
$k=2 \to \beta = \sqrt[3]{2}(-1/2 - i\sqrt{3}/2)$

$x^3 - 2 \in \mathbb{Q}[x]$ é irred sobre $\mathbb{Q}$

$\operatorname{Irr}(\sqrt[3]{2}, \mathbb{Q}) = \operatorname{Irr}(\beta, \mathbb{Q}) = x^3 - 2$

$\mathbb{Q}[\sqrt[3]{2}] = \{a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2 \mid a_i \in \mathbb{Q}\}$

$\mathbb{Q}[\beta] = \{a_0 + a_1\beta + a_2\beta^2 \mid a_i \in \mathbb{Q}\}$

$$\begin{array}{ccc} \mathbb{C} & & \\ | & & \mathbb{Q}[\beta] \\ \mathbb{R} & & \| \\ | & & \\ \mathbb{Q}[\sqrt[3]{2}] & & \\ & \mathbb{Q} & \end{array}$$

agora, $\mathbb{Q}[\sqrt[3]{2}] \xrightarrow{\psi} \mathbb{Q}[\beta]$

aplicação que fixa os racionais e manda $\sqrt[3]{2}$ em beta

$a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2 \to a_0 + a_1\beta + a_2\beta^2$
é um homomorfismo sobrejetivo
afirmamos que ψ é injetiva, i.e, $\psi(u) = \psi(v)$ $\Rightarrow u = v$
como ψ é um homomorfismo ψ é injetiva se e só se $\{u \in \mathbb{Q}[\sqrt[3]{2}] \mid \psi(u) = 0\}$

suponhamos então que $\psi(a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2)$
$\Rightarrow \beta$ é raiz de $(\underbrace{a_0 + a_1 x + a_2 x^2}_{f(x)})$. Logo

$\underbrace{\operatorname{Irr}(\beta, \mathbb{Q})}_{x^3-2}$ divide $f(x)$. $\therefore$ $f(\sqrt[3]{2}) = 0$

isto é $a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2 = 0$

Se $\alpha, \beta \in F \supset K$ são algebricos sobre K tq $\operatorname{Irr}(\alpha, K) = \operatorname{Irr}(\beta, K) \Rightarrow K[\alpha] \simeq K[\beta]$

(i.e $\exists$ um homomorfismo biunívoco e sobre de $K[\alpha]$ em $K[\beta]$)

Exemplo $\mathbb{R}$

$$\begin{array}{ll} \mathbb{Q}[\sqrt[8]{2}] & \\ \cup\!\!\! + & x^2 - \sqrt[4]{2} \\ \mathbb{Q}[\sqrt[4]{2}] & \\ \cup\!\!\! + & x^2 - \sqrt{2} \\ \mathbb{Q}[\sqrt{2}] & \\ \cup\!\!\! + & x^2 - 2 \\ \mathbb{Q} & \end{array}$$

$x^8 - 2$ $\quad$ $x^4 - 2$

$\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \dots \subset \mathbb{Q}[\sqrt[2^i]{2}] \subset \dots$ uma cadeia de corpos entre $\mathbb{Q}$ e $\mathbb{R}$

(o mesmo ocorre com $\mathbb{Q}[\sqrt[n]{p}]$ p primo ≥ 2

$\mathbb{Q} \subseteq K$ = corpo $\subseteq \mathbb{C}$

seja $f(x) \in K[x]$, então f pode ser escrito como $f(x) = c(x - \alpha_1)^{m_1} \dots (x - \alpha_r)^{m_r}$

em $\mathbb{C}[x]$ $(c \in K)$

Seja L o menor subcorpo de $\mathbb{C}$ que contem K e todas as raízes de $f(x)$. L = intersecção de todas os subcorpos de $\mathbb{C}$ que contém K e as raízes de f

modo construtivo de obter L

$(K \subset K[\alpha_1] \subset K[\alpha_1][\alpha_2] \subset \text{----})$

$K \subset K_1 = K[\alpha_1] \subset K_2 = K_1[\alpha_2] \subset \text{--} K_r.$

$K_r[\alpha_r] \quad L = L_r = K[\alpha_1, \alpha_2 \ldots, \alpha_r]$

P/ a $\overline{B}$ pertencer o modulo p/ tem que ser racional

L é chamado corpo de composição de $f(x)$ sobre K

notação: $L = gal(f\,K)$

Exercício
Calcular $gal(x^3 - 2, \mathbb{Q})$

$x^3 - 2 = 0$
$x = \sqrt[3]{2} = r_0 \qquad k = 0, 1, 2.$

$r_1 = r^{1/3}\left(\cos k \frac{360}{3} + i \operatorname{sen} \frac{360k}{3}\right)$

$r_1 = \sqrt[3]{2}\,(1 + i0) = \sqrt[3]{2}$ //

$r_2 = \sqrt[3]{3}\left(-1/2 + i\frac{\sqrt{3}}{2}\right)$

$r_3 = \sqrt[3]{2}\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right) = \mathbb{Q}[\alpha][B]\ [B] = \mathbb{Q}[r_0, r_1, r_2]$

$\mathbb{Q}[\alpha, B, e] = \mathbb{Q}[\alpha, B]$

$\mathbb{Q}[\alpha] = a_0 + a_1\alpha + a_2\alpha^2 / a_i \in \mathbb{Q}\}$

$\mathbb{Q}[\alpha][B] = \{b_0 + b_1 B / b_i \in \mathbb{Q}[\alpha]\} =$

$= \{(a_0 + a_1\alpha_1 + a_2\alpha^2) + (a_0' + a_1'\alpha + a_2'\alpha^2) B / a_i, a_i' \in \mathbb{Q}$

8 O são, 2 O V!

KH 100 HeHÁ é ~~A~~.

Rio, 6/6/78

Se $L \supset K$ é uma extensão de corpos, então L pode ser visto como um espaço vetorial K (L, + é um grupo abeliano)

(1) $x + (y+z) = (x+y) + z$.
(2) $\exists\, 0 \in L$ tq $x + 0 = x = 0 + x$
(3) $\forall\, x \in L$, $\exists\, y \in L$ tq $x + y = 0 = y + x$
(4) $x + z = z + x$
(5) $\lambda(x+y) = \lambda(x+y) = \lambda x + \lambda y$, $(\lambda + \mu)x = \lambda x + \mu x$
(6) $(\lambda\mu)x = \lambda(\mu x) = \mu(\lambda x)$
(7) $1x = x$

$\mathbb{C} \supset \mathbb{R}$; $\mathbb{C}$ é um espaço vetorial sobre $\mathbb{R}$.
$\mathbb{C}$ é de dimensão finita sobre $\mathbb{R}$

$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$; $\{1, i\}$ = base de $\mathbb{C}$ sobre $\mathbb{R}$

$\mathbb{C} = \mathbb{R}[i]$

$\mathrm{Irr}(i, \mathbb{R}) = x^2 + 1$

$$\begin{array}{c} \mathbb{Q}[\sqrt[3]{2}] \\ | \\ \mathbb{Q} \end{array} \quad x^3 - 2 = \mathrm{Irr}(x^3 - 2, \mathbb{Q})$$

$$\mathbb{Q}[\sqrt[3]{2}] = \{a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2 \mid a_0, a_1, a_2 \in \mathbb{Q}\}$$

Uma extensão de corpos $K \subset L$ é finita se a dimensão de L sobre K é finita, caso contrario $L \supset K$ é uma extensão infinita

Exemplo:

$\mathbb{Q} \subsetneq \mathbb{Q}[\sqrt{2}] \subsetneq \ldots \subsetneq \mathbb{Q}[\sqrt[2^i]{2}] \subsetneq \ldots$

$[\mathbb{Q}[\sqrt{2}] . \mathbb{Q}] = 2$ (dimensão = 2)

$[\mathbb{Q}[\sqrt[4]{2}] . \mathbb{Q}] = 4$

Seja $M = \bigcup_{i=0}^{\infty} \mathbb{Q}[\sqrt[2^i]{2}]$ M é um corpo

($x, y \in M$, $x \in \mathbb{Q}[\sqrt[2^i]{2}]$, $y \in \mathbb{Q}[\sqrt[2^j]{2}]$

$[M:\mathbb{Q}]$ não é finita

(caso contrário, $[\mathbb{Q}[\sqrt[i]{2}] : \mathbb{Q}] \leq [M:\mathbb{Q}] = n \quad \forall i \geq 0$

$$\begin{array}{c} \mathbb{C} \\ \downarrow \text{ é finito} \\ \mathbb{R} \\ \downarrow \to \infty \\ \mathbb{Q} \end{array}$$

prop: seja $L \supset K$ uma extensão de corpos

(a) se $L \supset K$ é uma extensão finita, então $L \supset K$ é uma extensão algébrica

(b) Se $\alpha \in L \supset K$ é algébrico sobre K e $\partial(\mathrm{irr}(\alpha, K)) = n$, então $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ é uma base de $K[\alpha]$ sobre K. Em particular $[K[\alpha] : K] = n$

dem

(a) suponhamos que $[L:K] = m < \infty$

Seja $\alpha \in L$, então $1, \alpha, \alpha^2, \dots, \alpha^{m-1}, \alpha^m$ são $m+1$ elementos de L, logo são l. dependentes sobre K. Isto é, $\sum_{i=0}^{m} a_i \alpha^i = 0$ onde os $a_i \in K$ e não todos nulos. Então α é raiz do polinomio não nulo $\sum_{i=0}^{m} a_i x^i \in K[x]$ $\therefore$ α é algébrico sobre K

Se $L \supset K$ é uma extensão de corpos a dimensão de L sobre K, $[L:K]$ é tbem chamada "grau da extensão $L \supset K$"

$$\begin{array}{c} \mathbb{Q}[\sqrt[3]{2}][\beta] \\ | \\ \mathbb{Q}[\sqrt[3]{2}] \\ 3 \,| \\ \mathbb{Q} \end{array}$$

$x^3 - 2 \in \mathbb{Q}[x]$

$\alpha = \sqrt[3]{2}, \quad \beta = \sqrt[3]{2}\left(-\frac{1}{2} + \frac{\sqrt{3}}{2} i\right), \quad \bar{\beta} = \sqrt[3]{2}\left(-\frac{1}{2} - \frac{\sqrt{3}}{2} i\right)$

$\mathrm{gal}(x^3 - 2, \mathbb{Q}) = \mathbb{Q}[\alpha, \beta]$

Em $\mathbb{Q}[\sqrt[3]{2}]$ podem escrever $x^3 - 2 = (x - \sqrt[3]{2})\, g(x)$
onde $\partial g(x) = 2$ e $g(\beta) = 0$

$\mathbb{Q}[\sqrt[3]{2}][\beta] = \{ b_0 + b_1 \beta \mid b_0, b_1 \in \mathbb{Q}[\sqrt[3]{2}] \}$

$= \{ a_0 + a_1 \sqrt[3]{2} + a_2 (\sqrt[3]{2})^2 + (c_0 + c_1 \sqrt[3]{2} + c_2 (\sqrt[3]{2})^2)\beta \mid a_i, c_i \in \mathbb{Q} \}$

$1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \beta, \sqrt[3]{2}\beta, (\sqrt[3]{2})^2 \beta$

$$\mathbb{Q} \xrightarrow[1,\, \sqrt[3]{2},\, (\sqrt[3]{2})^2]{3} \mathbb{Q}[\sqrt[3]{2}] \xrightarrow[1,\, \beta]{2} \mathbb{Q}[\sqrt[3]{2}][\beta]$$

---

teorema: sejam $M \supset L \supset K$ corpos tais que $[M:L]$ e $[L:K]$ são finitos. Então $[M:K] = [M:L][L:K]$

dem: sejam $u_1, u_2, \dots, u_n$ base de M sobre L ($[M:L] = n$) $v_1, v_2, \dots, v_m$ base de L sobre K ($[L:K] = m$)

$\vdash$ $u_i v_j$, $1 \leq i \leq n$, $1 \leq j \leq m$, é uma base de M sobre K

são lin. independentes sobre K

$\sum_{i,j} \alpha_{ij} u_i v_j = 0, \ \alpha_{ij} \in K \to \sum_i \alpha_{i1} u_i v_1 +$

$\underbrace{\left(\sum_j \alpha_{1j} v_j\right)}_{\in L} u_1 + \underbrace{\left(\sum_j \alpha_{2j} v_j\right)}_{\in L} u_2 + \dots + \underbrace{\left(\sum_j \alpha_{nj} v_j\right)}_{\in L} u_n = 0$

$\therefore$ ($\{u_i\}$ é l.i sobre L) $\sum_j \alpha_{ij} v_j = 0 \quad \forall i$

como $\{v_j\}$ é l.i sobre K, segue que $\alpha_{ij} = 0 \ \forall i, \forall j$

$\vdash$ geram M sobre K

se $x \in M$, então $x = \sum_{i=1}^{n} \alpha_i u_i$, ($\alpha_i \in L$)
como $\alpha_i \in L$, então $\alpha_i = \sum_{j=1}^{m} \beta_{ij} v_j$. Logo

$$x = \sum_{i=1}^{m} \Big(\sum_{j=1}^{m} \beta_{ij} v_j \Big) u_i = \sum_{i,j} \beta_{ij} v_j u_i$$

$$\begin{array}{c} \mathbb{Q}[\sqrt[3]{2}] \\ | \\ K \\ | \\ \mathbb{Q} \end{array} \qquad \begin{array}{l} [\mathbb{Q}[\sqrt[3]{2}] : K][K : \mathbb{Q}] = 3 \\ \therefore [\mathbb{Q}[\sqrt[3]{2}] : K] = 1 \\ \quad \text{ou} \\ [K : \mathbb{Q}] = 1 \end{array}$$

Rio, 13/6/78

1) Encontre o $Irr(\sqrt{3}+\sqrt{2}, \mathbb{Q})$

$$\begin{array}{ll} \mathbb{Q}[\sqrt{2}][\sqrt{3}] & \\ \quad | \, 2 & \sqrt{3}, 1 \qquad \sqrt{2}\sqrt{3} \\ \mathbb{Q}\sqrt{2} & \\ \quad | \, 2 & 1; \sqrt{2} \\ \mathbb{Q} & \end{array}$$

$[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$

$x^2-3 \in \mathbb{Q}[\sqrt{2}][x]$

Como raiz de 3 não é raiz de nenhum polinomio da forma $x+b$ $b \in \mathbb{Q}[\sqrt{2}]$ segue que $Irr(\sqrt{3}, \mathbb{Q}[\sqrt{2}]) = x^2-3$

$(\sqrt{3}+b = 0$, $b \in \mathbb{Q}[\sqrt{2}]$ então $\sqrt{3} \in \mathbb{Q}[\sqrt{2}]$

$\therefore \sqrt{3} = a + c\sqrt{2}$ onde $a, c \in \mathbb{Q}$ $\therefore \sqrt{3} - c\sqrt{3} \in \mathbb{Q}$ *

$[\mathbb{Q}[\sqrt{2}][\sqrt{3}] : \mathbb{Q}[\sqrt{2}]] = 2$

$[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}] : \mathbb{Q}] = 4$

$\sqrt{3}+\sqrt{2} \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$

$$\begin{array}{cc} & \mathbb{Q}[\sqrt{2}, \sqrt{3}] \\ & | \\ 4 & \mathbb{Q}[\sqrt{2}+\sqrt{3}] \\ & | \\ & \mathbb{Q} \end{array}$$

$[\mathbb{Q}[\sqrt{3}+\sqrt{2}] : \mathbb{Q}] = 2$ ou 4

$(\sqrt{2}+\sqrt{3})^2 = 5 + 2\sqrt{2}\sqrt{3}$

$(\sqrt{2}+\sqrt{3})^4 = 49 + 20\sqrt{2}\sqrt{3}$

$x^2 + ax + c$

$x^4 - 10x^2 + 1 = p(x) \in \mathbb{Q}[x]$

$p(\sqrt{2}+\sqrt{3}) = 0$

$+$ $\sqrt{2}, \sqrt{3} \in \mathbb{Q}[\sqrt{2}+\sqrt{3}]$

$\underbrace{(\sqrt{2}+\sqrt{3})^2}_{5+2\sqrt{2}\sqrt{3}} \in \mathbb{Q}[\sqrt{2}+\sqrt{3}]$

Se eu subtrair 5 de 2 continuo dentro

$\sqrt{2}\sqrt{3} \in \mathbb{Q}[\sqrt{2}+\sqrt{3}]$

$(\sqrt{2}+\sqrt{3})\sqrt{2}\sqrt{3} = 2\sqrt{3} + 3\sqrt{2} \in \mathbb{Q}[\sqrt{2}+\sqrt{3}]$

$2(\sqrt{2}+\sqrt{3}) = 2\sqrt{3} + \frac{2\sqrt{2}}{\sqrt{2}} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$

$\sqrt{3} = (\sqrt{2}+\sqrt{3}) - \sqrt{2} \in \mathbb{Q}[\sqrt{2}+\sqrt{3}]$

Conclusão

$\mathbb{Q}[\sqrt{2}+\sqrt{3}] = \mathbb{Q}[\sqrt{2},\sqrt{3}]$

e portanto $[\mathbb{Q}[\sqrt{2}+\sqrt{3}]:\mathbb{Q}] = 4$

$\therefore \ \partial\, \mathrm{Irr}(\sqrt{2}+\sqrt{3}, \mathbb{Q}) = 4$

$\therefore \ \mathrm{Irr}(\sqrt{2}+\sqrt{3}, \mathbb{Q}) = x^4 - 10x^2 + 1$

Teorema

a) $\overline{\mathbb{Q}}_{\mathbb{R}} = \{\alpha \in \mathbb{R} \,/\, \alpha$ algébrico sobre $\mathbb{Q}\}$
é um subcorpo de $\mathbb{R}$ que é uma ext infinita de $\mathbb{Q}$

b) $\overline{\mathbb{Q}}_{\mathbb{C}} = \{\alpha \in \mathbb{C} \,/\, \alpha$ é algébrico sobre $\mathbb{Q}\}$
é um subcorpo de $\mathbb{C}$ que é uma extensão infinita de $\mathbb{Q}$

dem: como $\overline{\mathbb{Q}}_{\mathbb{R}} = \overline{\mathbb{Q}}_{\mathbb{C}} \cap \mathbb{R}$, basta mostrar que $\overline{\mathbb{Q}}_{\mathbb{C}}$ é um corpo

Sejam $\alpha, \beta \in \mathbb{C}$ algébrico sobre $\mathbb{Q}$

então $[\mathbb{Q}[\alpha,\beta]:\mathbb{Q}] = [\mathbb{Q}[\alpha][\beta]:\mathbb{Q}(\alpha)]$
$[\mathbb{Q}[\alpha]:\mathbb{Q}]$

pois α é alg sobre $\mathbb{Q}$ e β é alg sobre $\mathbb{Q}[\alpha]$

$$\begin{array}{c} \mathbb{Q}[\alpha](\beta) \\ \| \\ \mathbb{Q}[\alpha,\beta] \\ \| \\ \mathbb{Q}[\alpha] \\ | \\ \mathbb{Q} \end{array} \qquad \begin{array}{l} < \infty \\ \\ \\ \\ < \infty \end{array}$$

$\mathbb{Q}[\alpha,\beta]$ extensão finita de $\mathbb{Q} \Rightarrow$

$\mathbb{Q}[\alpha,\beta]$ é uma extensão algébrica sobre $\mathbb{Q}$

Logo, como $\alpha \pm \beta$, $\alpha \cdot \beta$ e $\alpha\beta^{-1}$ (se $\beta \neq 0$)
então $\mathbb{Q}[\alpha,\beta]$ eles são algébricos sobre $\mathbb{Q}$, i.e estão em $\overline{\mathbb{Q}}_{\mathbb{C}}$

$\mathbb{Q}[\sqrt{2}] \text{---} \mathbb{Q}[\sqrt[3]{2}]$

$\bigcup_{i=1}^{\infty} \mathbb{Q}[\sqrt[i]{2}] \subset \overline{\mathbb{Q}}_{\mathbb{R}}$

Se $[\overline{\mathbb{Q}}_{\mathbb{R}}:\mathbb{Q}] = n < \infty$ então $[\mathbb{Q}\sqrt[i]{2}:\mathbb{Q}]$
$\leq n \qquad i = 1, 2, \ldots$ absurdo

Logo $\overline{\mathbb{Q}}_{\mathbb{R}}$ é 1 extensão infinita de $\mathbb{Q}$
como $\overline{\mathbb{Q}}_{\mathbb{R}} \subset \overline{\mathbb{Q}}_{\mathbb{C}}$, $\overline{\mathbb{Q}}_{\mathbb{C}}$ é tb uma extensão infinita sobre $\mathbb{Q}$

(4) Seja $\alpha = \sqrt[3]{2} \in \mathbb{R}$, $\beta = \sqrt[3]{2}\left(-\frac{1}{2} + \frac{\sqrt{3}}{2} i\right) \in \mathbb{Q}$

Prove que

(a) $\mathbb{Q}[\alpha] \simeq \mathbb{Q}[\beta]$
α é alg sobre $\mathbb{Q}$ e

$\mathrm{Irr}(\alpha,\mathbb{Q}) = \mathrm{Irr}(\beta,\mathbb{Q}) = x^3 - 2$

$\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + a_2\alpha^2 \,/\, b_i \in \mathbb{Q}\}$

$c_0 + c_1\alpha + c_2\alpha^2 \longrightarrow c_0 + c_1\beta + c_2\beta^2$

sobre
é biunívoca (injetivo)

Preserva (homomorfismo)

(b) $|\underbrace{\text{aut }[\mathbb{Q}\sqrt[3]{2}]}_{\text{not de nº de elementos}}| = 1$

AUT $\mathbb{Q}[\alpha]$ de $\mathbb{Q}[\alpha]$ = conj dos $\underbrace{\text{automorfismo}}$ isomorf de um corpo ou anel nele mesmo

Quero mostrar que há um único automorfismo: a identidade

Seja $\phi: \mathbb{Q}[\alpha] \to \mathbb{Q}[\alpha]$ um isomorf.

$\phi(\alpha^3) = \phi(\alpha)^3 = \phi(2) = 2 \Rightarrow \phi(\alpha)$ é raiz de x^3-2, $\phi(\alpha)$ é raiz de x^3-2. $\phi(\alpha) \in \mathbb{Q}[\alpha]$

$\alpha = \sqrt[3]{2}$

$\phi(1.1) = \phi[1).\phi(1)$ (cortou pq é injetivo e $\phi(0)=0$

$\phi(1) \Rightarrow \mathbb{Q}(1) = 1$

$\phi(2) = \phi(1+1) = \phi(1) + \phi(1) = 2$

$\phi(\alpha) = \alpha$ ou B ou $\overline{B}$

mas B e $\overline{B} \notin \mathbb{Q}[\alpha]$, logo $\phi(\alpha) = \alpha$

Se $y \in \mathbb{Q}[\alpha]$, $y = a_0 + a_1\alpha + a_2\alpha^2$ onde $a_i \in \mathbb{Q}$

Demostre que fixa os racionais

$\phi\left(\frac{n}{m}\right) = \phi(n) \cdot \phi\left(\frac{1}{m}\right) = \phi(n) \cdot \frac{1}{\phi(m)} = \frac{n}{m}$

$= \mathbb{Q}(1) = \phi\left(\frac{1}{m} \cdot m\right) = \phi\left(\frac{1}{m}\right)\phi(m)$

Logo

$\phi(y) = \phi(a_0) + \phi(a_1)\phi(\alpha) + \phi(a_2)\phi(2)^2$

$= a_0 + a_1\alpha + a_2\alpha^2 = y$

Logo ϕ é a identidade

Neste caso um automorfismo permuta raizes

$\mathbb{Q}[\alpha, B] \xrightarrow{\phi} \mathbb{Q}[\alpha, B]$

$\phi(\alpha) = \alpha$ ou B ou $\overline{B}$

$\phi(B) = \alpha$ ou B ou $\overline{B}$

$\phi(\overline{B}) = \alpha$ ou B ou $\overline{B}$

$Id = \begin{pmatrix} \alpha & B & \overline{B} \\ \alpha & B & \overline{B} \end{pmatrix}$

$\begin{pmatrix} \alpha & B & \overline{B} \\ B & \alpha & \overline{B} \end{pmatrix}$

$\begin{pmatrix} \alpha & B & \overline{B} \\ \overline{B} & \alpha & B \end{pmatrix}$

c) $Gal(x^3-2, \mathbb{Q}) = \mathbb{Q}[\alpha, B] = \mathbb{Q}[\alpha, \overline{B}] =$
$= \mathbb{Q}[B, \overline{B}]$

ex: $\sqrt[3]{2}\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)$

$\sqrt[3]{2}\left(-\frac{1}{2}\mp\frac{\sqrt{3}}{2}i\right)$

(a) $L = gal(x^3-2, \mathbb{Q})$

então $|aut\ L| = 6$

2º Questão

$a + b\alpha \qquad a, b \in \mathbb{Z}_7$

$\mathbb{Z}_7 \times \mathbb{Z}_7 \qquad \mathbb{Z}_7[\alpha]$

(a, b)

$$\begin{array}{c} \mathbb{Z}_7[\alpha] \\ | \\ \mathbb{Z}_7 \end{array} \Big\} 2$$

$gal(f(x); \mathbb{Q}) = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$

$gal(f(x), \mathbb{Q}[\sqrt{2}]) = \mathbb{Q}[\sqrt{2}][\sqrt{3}]$

$gal(f(x), \mathbb{R}) = \mathbb{R} / (x+\sqrt{2})(x-\sqrt{2})(x+\sqrt{3})$
$(x-\sqrt{3})$

$gal(x^5-1, \mathbb{Q}) = \mathbb{Q}[\alpha]$

$\alpha = |1 \quad \alpha^5 = 1$

$x^5 - 1 = (x-1)\, g(x)$

critério de Eisenstein 13/3/78

Seja $f(x) = a_0 + a_1x + \ldots a_nx^n \in \mathbb{Z}[x]$

e suponhamos que exista um nº primo p. 1
tal que

(i) $p \nmid a_n$

(ii) $p \mid a_0, a_1, \ldots a_{n-1}$

(iii) $p^2 \nmid a_0$

Então $f(x)$ é irredutível sobre $\mathbb{Q}$

~ // ~

Exemplo 1

Se p é um nº primo então $x^n - p$ é irredutível sobre $\mathbb{Q}$ $\forall n \geq 1$

Exemplo 2

$x^7 + 10x^4 - 15x^2 - 25x + 15$

~ // ~

* Seja p um nº primo ≥ 2 e seja

$g(x) = x^{p-1} + x^{p-2} + \ldots x + 1$

então $g(x)$ é irredutível sobre $\mathbb{Q}$.

Exercício

Seja K um corpo e $K[x] \xrightarrow{\varphi} K[x]$
$f(x) \to f(x+a)$

onde $a \in K$

mostre que φ é um isomorfismo

$\Psi(f \cdot g) = f \cdot g(x+a) = f(x+a)\, g(x+a)$.

$\Psi(f+g) = (f+g)(x+a) = f(x+a) + g(x+a)$

É biunívoca.
sejam $f, g \in K[x]$

$\Psi(f) = \Psi(g) \Rightarrow$
$\to f(x+a) = g(x+a) \to$
$f((x-a)+a) = g((x-a)+a)) \Rightarrow f(x) = g(x)$ é biunívoca

Ψ é sobre. seja $g(x) \in K[x]$. Queremos mostrar que $g(x) = \Psi(f)$ para algum $f \in K[x]$

seja $f(x) = g(x-a)$

Então $\Psi(f) = f(x+a)$
$= g((x+a)-a) = g(x)$
$x \quad -a$

consequência

Seja K um corpo e $a \in K$. Então $f(x) \in K[x]$ é irredutível sobre $K \Rightarrow f(x+a)$ é irredutível

dem. $f(x) = g(x)\, h(x) \Leftrightarrow f(x+a) = g(x+a)\, h(x+a)$ sobre K.

* $(p=3)$ $x^3 + x^2 + x + 1$ é irredutível sobre $\mathbb{Q}$

$f(x)$ irred sobre $\mathbb{Q} \Rightarrow f(x+a)$ é irred sobre $\mathbb{Q}$
seja $a=1$ $\quad a \in \mathbb{Q}$

$f(x+1) = (x+1)^3 + (x+1)^2 + x+1+1$
é falso

3×1

$-3x^2 +$

$p=3$ $\quad 2x$
$q(x) = x^2 + x + 1$

$q(x+1) = (x+1)^2 + (x+1) + 1 \quad = x^2 + 3x + 3$

3×1, $\quad 3/3 \quad 3/3 \quad 9 \times 3$

se $q(x+1)$ é irred $\Rightarrow q(x)$ tb é

Pode ser aplicado o critério de Eisenstein em $q(x+1)$ com nº primo p.

demost p/ casa

—//—

se $f(x) \in \mathbb{Q}[x]$ é tq $f(\alpha) = 0$ ($\alpha \in \mathbb{C} \supset \mathbb{Q}$), encontre um polinomio $g(x) \in \mathbb{Q}[x]$ tq $g(1/\alpha) = 0$

$0 = \frac{1}{\alpha^n} \cdot f(\alpha) = a_0 (1/\alpha)^n + a_1 \left(\frac{1}{\alpha}\right)^{n-1} \ldots$

—//—

$f(x) = x^2 - 2 \quad ; f(\alpha) = 0$

$g(x) = -2x^2 + 1 \quad g\left(\frac{1}{\sqrt{2}}\right) = 0$

—//—

calcule

$[\mathbb{Q}[\sqrt{2}, i] : \mathbb{Q}] = 2^2 = 4$ $\quad \mathbb{Q}[\sqrt{2}][i] \quad$ $\mathrm{Irr}(i, \mathbb{Q}\sqrt{2}) = x^2+1$

$\mathbb{Q}[\sqrt{2}][i]$ — $1, i$
$\mathbb{Q}[\sqrt{2}]$ — 2 — $1, \sqrt{2}$
$\mathbb{Q}$

base de $\mathbb{Q}[\sqrt{2}, i]$ sobre $\mathbb{Q}$ $\quad 1, \sqrt{2}i, i, \sqrt{2}$
=

calcule $[\mathbb{Q}[\sqrt{2}, \sqrt[3]{2}] : \mathbb{Q}] = 8$

$\mathbb{Q}[\sqrt{2}][\sqrt[3]{2}]$ $\to$ 4 $\quad x^4 - 2 \quad$ 2
$\mathbb{Q}[\sqrt{2}]$
$\mathbb{Q}$ $\quad$ 2 $\quad x^2 - 2 =$ $\quad \mathrm{Irr}(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$

Base de $\mathbb{Q}[\sqrt{2}][\sqrt[8]{2}]$ sobre $\mathbb{Q}$ $1, \sqrt[8]{2}, (\sqrt[8]{2})^2, \dots (\sqrt[8]{2})^7$

Rio, 26/6/78

irredutível sobre $\mathbb{Z} \Rightarrow$ irredutível sobre $\mathbb{Q}$

$x^4 + 8x^2 + 2x + 5 + x^2$ é irredutível sobre $\mathbb{Q}$?

$x^4 + x^2 + 1 = (x^2 + bx + 1)(x^2 + dx + 1)$ é irred sobre $\mathbb{Z}_2$?

$ce \equiv 1 \pmod 2$
$btd \equiv 0 \pmod 2$ $\Rightarrow$ $b = 1$, $d = 1$
$bd \equiv 1 \pmod 2$

$\Rightarrow (x^2 + x + 1)(x^2 + x + 1)$

é irredutível sobre $\mathbb{Q}$?

$x^4 + 8x^3 + x^2 + 2x + 5$

2) $f(x) = \sum_{i=0}^{n} \alpha_i x^i$

$f'(x) = \sum_{i=0}^{n-1} \alpha_i x^{i-1}$

$\mathbb{Z}_p[x]$ onde $p \neq 0$ $x^p + c$
$p x^{p-1} = 0$

$\underbrace{x^p + x^{p-1} + \dots x^0}_{P(x)} \in \mathbb{Z}[x]$ é irredutível sobre $\mathbb{Q}$
p - primo

dem: aplicar eisenstein ao pol $p(x+1)$

$-[gal(x^2 - (3+\sqrt{2})x + 3\sqrt{2}, \mathbb{Q}) : \mathbb{Q}]$

$[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$

$J = \{f(x) \in \mathbb{Q}[x] \mid f(3) = f(2) = 0\}$

$f(x) \in J \Rightarrow f(x)$ é divisível por $(x-2)(x-3)$

$J = (x-2)(x-3) \cdot \mathbb{Q}[x]$
é um ideal não é maximal

— —

mostre que $\overbrace{x^3 + x + \bar{1}}^{f(x)} \overset{= gh}{} \in \mathbb{Z}_5[x]$ é irred sobre $\mathbb{Z}_5$

dem: sup que $f(x)$ não é irred sobre $\mathbb{Z}_5$

Então $f(\bar{x}) = h(\bar{x})\, g(\bar{x})$, $h, g \in \mathbb{Z}_5[x]$ não ctes

Como $\partial f = \partial h + \partial g$ podemos supor $\partial g = 1$; $\partial g = 2$

Logo f tem uma raiz em $\mathbb{Z}_5$

tem 1 raiz $\Rightarrow$ redutível

basta mostrar que ñ tem nenhuma raiz $\Rightarrow$ irredutível

Prove que os corpos $\mathbb{Q}\sqrt{2}$ e $\mathbb{Q}[\sqrt{3}]$ não são isomorfos

sup que $\varphi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}\sqrt{3}$ é um isomorfismo
então: $\varphi(a) = a \quad \forall a \in \mathbb{Z}$
Logo, $\varphi(\sqrt{2})^2 = \varphi(\sqrt{2})\,\varphi(\sqrt{2}) = \varphi(\sqrt{2} \cdot \sqrt{2}) = \varphi(2) = 2$

Portanto:
$\mathbb{Q}[\sqrt{3}] \ni \varphi(\sqrt{2}) = \pm\sqrt{2}$

i.e. $\sqrt{2} = a + b\sqrt{3}$ onde $a, b \in \mathbb{Q}$ e $a \neq 0$ ou $b \neq 0$
$a \neq 0 \Rightarrow b = \sqrt{2}/\sqrt{3}$ contradição $*$
$a = 0 \Rightarrow$ contradição

— —

Calcule $Aut(\mathbb{Q}[\sqrt[4]{2}]) = \{\varphi : \mathbb{Q}[\sqrt[4]{2}] \to \mathbb{Q}\sqrt[4]{2} \mid \varphi$ isomorfismo

seja $\varphi : \mathbb{Q}[\sqrt[4]{2}] \to \mathbb{Q}[\sqrt[4]{2}]$ um isomorfismo
$y \in \mathbb{Q}[\sqrt[4]{2}]$, $y = a + b\sqrt[4]{2} + c(\sqrt[4]{2})^2 + d(\sqrt[4]{2})^3$

$$\varphi(y) = \varphi(a) + \varphi(b) + \varphi(\sqrt[4]{2}) + \varphi(c)\varphi(\sqrt[4]{3})^2 + \varphi(d) \cdot \varphi(\sqrt[4]{3})^3$$

$$= a + b\varphi(\sqrt[4]{2}) + c\varphi(\sqrt[4]{2})^2 + d\varphi(\sqrt[4]{2})^3$$

$$\varphi(\sqrt[4]{2})^4 = \varphi\{(\sqrt[4]{2})\}^4 = \varphi(2) = 2$$

$\therefore \sqrt[4]{2}$ é uma raiz de $x^4 - 2$

$\varphi(\sqrt[4]{2}) = \sqrt[4]{2}$ ou $-\sqrt[4]{2}$ ~~ou~~ α, β $\quad \alpha, \beta \in \mathbb{C}$

α, β não são reais $\quad \alpha, \beta \notin \mathbb{R}$

$aut(\mathbb{Q}[\sqrt[4]{2}]) = \{$identidade$, \varphi\}$

onde $\varphi(\sqrt[4]{3}) = -\sqrt[4]{2}$

Seja p um nº primo $p \geq 2$. Prove que

(a) $gal(x^p - 1, \mathbb{Q}) = \mathbb{Q}[\alpha]$ onde $\alpha^p = 1, \alpha \neq 1$

(b) $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + \dots a_{p-1}\alpha^{p-2} \mid a_i \in \mathbb{Q}\}$

c) se $L = gal(x^p - 1, \mathbb{Q})$ então $|aut\, L| = p - 1$

raízes de $x^p - 1$

$$\cos\frac{2\pi k}{p} + i\,\operatorname{sen}\frac{2\pi k}{p}, \quad k = 0, 1, 2 \dots p-1$$

p/ $k = 0 \quad \alpha_0 = 1$

p/ $k = 1 \quad \alpha_1 = \cos\frac{2\pi}{p} + i\operatorname{sen}\frac{2\pi}{p}$

p/ $k = 2 \quad \alpha_2 = \alpha_1^2$

p/ $k = p-1 \quad \Rightarrow \alpha_{p-1} = \alpha_1^{p-1}$

(a) $gal(x^p - 1, \mathbb{Q}) = \mathbb{Q}[\alpha_0, \alpha_1, \alpha_2 \dots \alpha_{p-1}] = \mathbb{Q}[\alpha_1]$

$\alpha_1^p = 1 \quad , \alpha_1 \neq 1$

(b) $\mathbb{Q}[\alpha] = ?$

$Irr(\alpha, \mathbb{Q}) = ?$

$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \dots x + 1)$

algebra II 1º sem/1978

PROJETO RONDON
integrar para não entregar

Estudante Brasileiro
Unido ao projeto Rondon.

$x^{p-1} + x^{p-2} + \dots x + 1$ é irredutível sobre $\mathbb{Q}$

$Irr(\alpha, \mathbb{Q}) =$

(c) $L = \mathbb{Q}[\alpha]$: $a_0 + \alpha_1 a_1 + \dots a_{p-1} \alpha^{p-2}$

$\varphi(\alpha)^{p-1} + \varphi(\alpha)^{p-2} + \varphi(\alpha) + \varphi(1) = \varphi(\alpha^{p-1} + \alpha^{p-2} + \alpha + 1)$

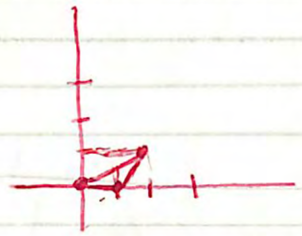
$= \varphi(0) = 0$

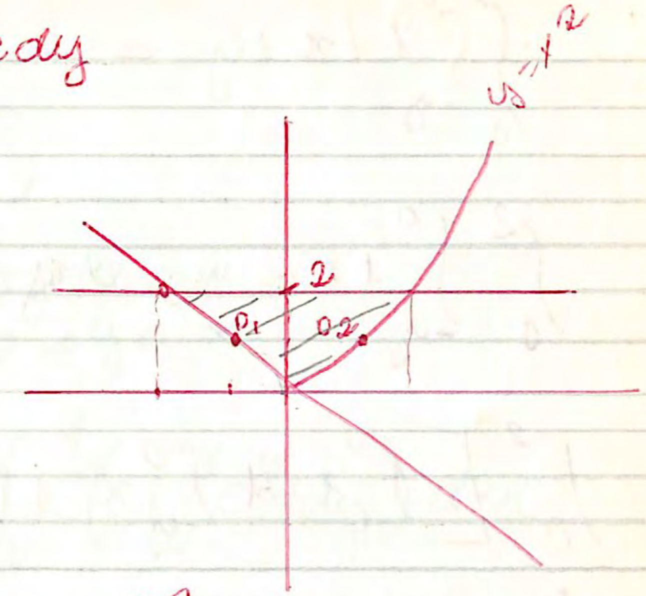
$\mathbb{Q}[\sqrt{2}, i] = \mathbb{Q}[u]$ $\qquad u \in \mathbb{Q}[\sqrt{2}, i]$

$\mathbb{Q}[\sqrt{2}i] \ni (\sqrt{2} + i)^2 = \cancel{2} + 2\sqrt{2}i - \cancel{1}$

~~somo 1~~
somo -2
divido po 2

massa = $\iint_R f(x,y)\,dx\,dy$





$y = -x$, $y = 2$

$x = \sqrt{y}$

$-y < x \leq \sqrt{y}$

$0 < y \leq 2$

$0 < y < 2$

$-y < x_1 < 0$

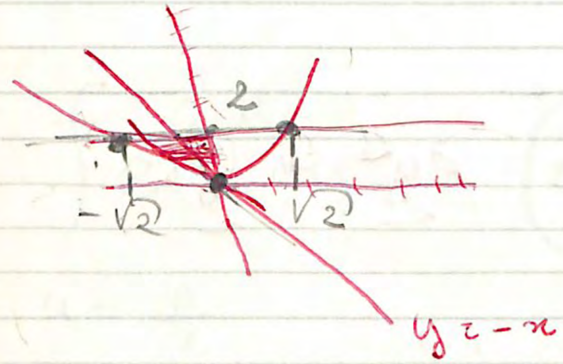
$0 < x_2 < \sqrt{y}$

$1 + x + y = 0$

$y = -x$

$x = \sqrt{y}$

//



$1 + x + 2 = 0$

$x = -3$

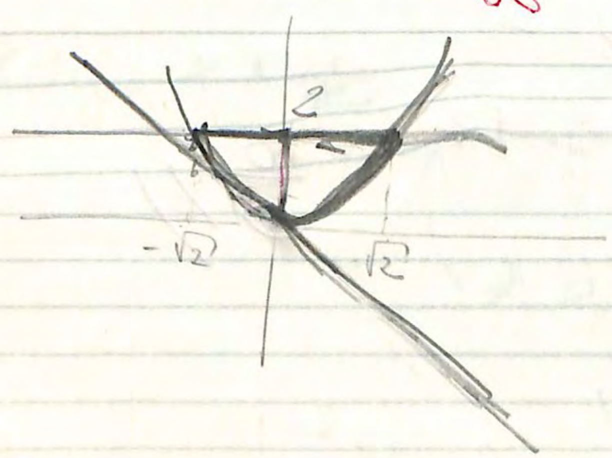
$y = -\sqrt{y}$

$y = -x$

$x = \sqrt{y}$

$y = 2$

$x = \pm\sqrt{2}$



y

$x = \sqrt{y}$

$x^2 = y$

$$\int_0^2\int_{-y}^{\sqrt{y}} 1+x+y =$$

$$\int_0^2\int_{-y}^{0} 1+x+y \; dy\,dx =$$

$$\int_0^2\left[\int_{-y}^{0} 1 + \int_{-y}^{0} x + \int_{-y}^{0} y\right) =$$

$$\left[x\right]_{-y}^{0} + \left[\frac{x^2}{2}\right]_{-y}^{0} + \left[yx\right]_{0}^{-y} =$$

$$y - \frac{y^2}{2} + y^2$$

$$\frac{2y}{2} - \frac{y^2}{2} + \frac{2y^2}{2} = \frac{2y^2}{2} + \frac{2y}{2}$$

$$\int_0^2 \frac{y^2}{2} + y = \frac{1}{2}\int_0^2 y^2 + \int_0^2 y = dy$$

$$\frac{1}{2}\left[\frac{y^3}{3}\right]_0^2 + \left[\frac{y^2}{2}\right]_0^2 =$$

$$\frac{1}{2}\cdot\frac{8}{3} + 2 = \frac{8}{6} = \frac{4}{3} + 2 = \frac{10}{3}$$

$$\frac{2\cdot\sqrt[2]{2^3}}{3} = \frac{2\cdot 2\sqrt{2}}{3} \quad \frac{4\sqrt{2}}{3}$$

$$\iint e^{\frac{y}{x}}$$

$y = x$

$y = 0$

$x = 1$

$0 < x < 1$

$0 < y < x$

$$\int_0^1\int_0^x e^{\frac{y}{x}}\, dy\, dx = \int_0^1\left(\int_0^x e^{\frac{y}{x}} dy\right) dx$$

$$* = \int_0^1 \left[x\cdot e^{\frac{y}{x}}\right]_0^x = \int_0^1 x\cdot e \, dx = e\int_0^1 x$$

$$= e\left[\frac{x^2}{2}\right]_0^1 =$$

$$\boxed{\frac{1}{2}e}$$

$$\int e^{\frac{y}{x}} dy$$

$e^y \cdot e^x$ $\quad$ e^{x+y} $\quad$ $e^{x\cdot y}$ $\quad$ e^x

$u = \frac{y}{x}$

$du = \frac{-y}{x^2} dy$

$du = \frac{1}{x} dy$

$x\,dy = x\,du$

$$\int x\, e^u \, du$$

$$x\int e^u \, d$$

$$* = x\cdot e^{\frac{y}{x}}$$

$$\left(e^{-1+y}\right)^2 \quad \left(e^{-2+y}\right)$$

$$e - e^{-3} - e - e^{-2}$$

$$\int_0^2\int_{-y}^{\sqrt{y}} 1+x+y =$$

$$\int_0^2\int_{-y}^{0} 1+x+y \; d\cancel{y}\, dx =$$

$$\int_0^2 \left[\int_{-y}^{0} 1 + \int_{-y}^{0} x + \int_{-y}^{0} y\right) =$$

$$\left[x\right]_{-y}^{0} + \left[\frac{x^2}{2}\right]_{-y}^{0} + \left[yx\right]_{0}^{-y} =$$

$$y - \frac{y^2}{2} + y^2$$

$$\frac{2y}{2} - \frac{y^2}{2} + \frac{+2y^2}{2} = \frac{2y^2}{2} + \frac{2y}{2}$$

$$\int_0^2 \frac{y^2}{2} + y = \frac{1}{2}\int_0^2 y^2 + \int_0^2 y = dy$$

$$\frac{1}{2}\left[\frac{y^3}{3}\right]_0^2 + \left[\frac{y^2}{2}\right]_0^2 =$$

$$\frac{1}{2}\cdot\frac{8}{3} + 2 = \frac{8}{6} = \frac{4}{3} + 2 = \frac{10}{3}$$

$$\frac{2\cdot\sqrt[2]{2^3}}{3} = 2\cdot 2\sqrt{2} \quad \frac{4\sqrt{2}}{3}\; 3$$

$$\iint e^{\frac{y}{x}}$$

$y = x$

$y = 0$

$x = 1$

$0 < x < 1$

$0 < y < x$

$$\int_0^1\int_0^x e^{\left(\frac{y}{x}\right)^u} \; d\cancel{y}\; dy = \int_0^1 \left(\int_0^x e^{\frac{y}{x}} dy\right) dx$$

$$* = \int_0^1 \left[x\cdot e^{\frac{y}{x}}\right]_0^x = \int_0^1 x\cdot e \, dx = e\int_0^1 x$$

$$= e\left[\frac{x^2}{2}\right]_0^1 =$$

$$\int e^{\left(\frac{y}{x}\right)^u} dy$$

$e^y \cdot \cancel{e^x}$ $\quad$ $\cancel{e^{x+y}}$ $\quad$ $\cancel{e^{x\cdot y}}$ $\quad$ e^x

$$\boxed{\frac{1}{2}e}$$

$u = \frac{y}{x}$

$du = \cancel{x\cdot 0}\; \frac{-y}{x^2} \, dy$

$du = \frac{1}{x} dy$

$\cancel{x}\, dy = x \frac{\cancel{x}du}{\cancel{x}}$

$$\int x \frac{e^u}{\cancel{x}} du$$

$$x\int e^u \, d$$

$$* = x\cdot \frac{y}{x}$$

$\iint e^{x+y}$

$x = -1$

$yx = 1$

$-y = -1$

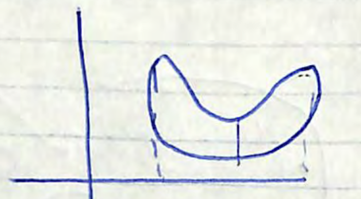
$(-1,-1)$

$x = -1$

$x = \frac{1}{y}$

$\int_{-1}^{-1}\int_{-1}^{1/y}$

$\iint e^{x+y}$

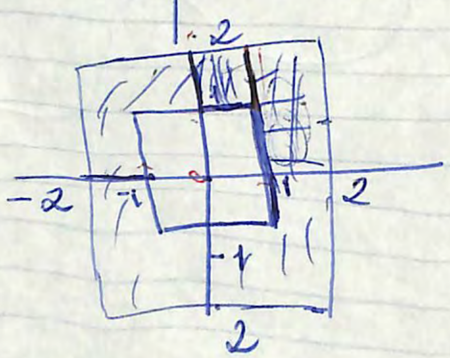


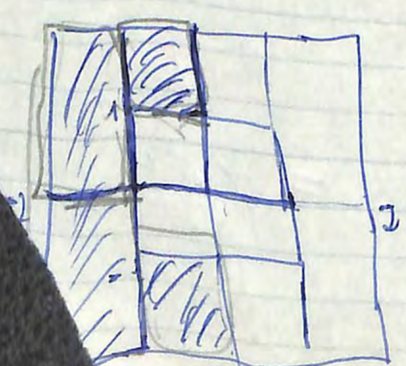
$x = -1$

$yx = 1$

$x = -1$

$x = \frac{1}{y}$





$\int_{-2}^{2y}\int_{-2x}^{-1x} e^{x+y} + \int_{-1x}^{1x}\int_{1y}^{2y} e^{x+y} + \int_{x=-1}^{x=1}\int_{-1-y}^{-2y} e^{x+y} +$

$\int_{-2y}^{2y}\int_{2}^{1} e^{x+y}$

$\int_{-2}^{2}\int_{-2}^{-1} e^{x+y}$

$\int_{-2}^{-1} e^{x+y}\,dx = \int_{-2}^{-1} e^{u}\,du = e^{u}$

$u = x+y$

$du = dx$

$\left[e^{x+y}\right]_{-2}^{-1} = e^{-1+y} - e^{-2+y}$

$\frac{e^{-3}-e^{1}}{2} = \frac{e^{-e}}{2}$

$\int e^{-1+y} - e^{-2+y}$

$\frac{1}{2}e^{-3} - \frac{1}{2}e^{1}$

$\int e^{-1+y} - \int e^{-2+y}$

$\frac{e^{-3}-e}{2}$

$u = -1+y$

$du = 2\,dx$

$dx = \frac{du}{2}$

$\frac{1}{2}\int e^{u}\,du =$

$\frac{1}{2} e^{-1+y}$

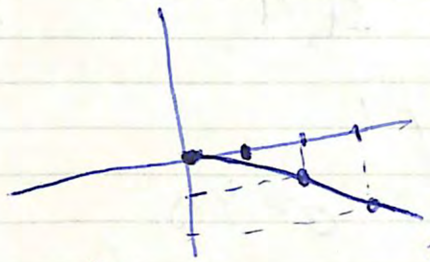
$\left(e^{-1+y}\right)^{2}_{-2} - \left(e^{-2+y}\right)$

$e - e^{-3} - e - e^{-4}$

$x=0$, $y=0$ $x+y+z=1$ $z=0$

$x = 1-y$

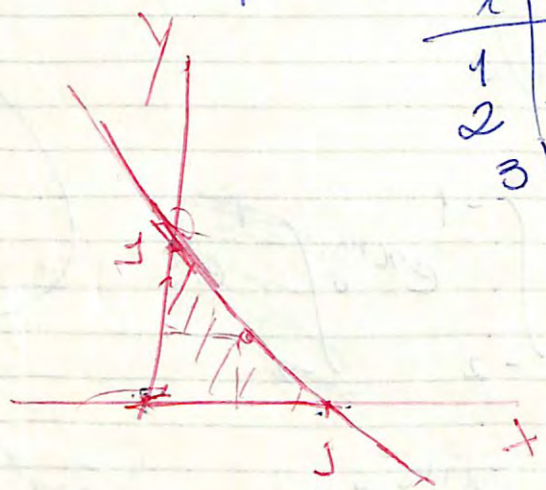
$0<x<1-y$
$0<y<1$



$x+y=1$
$1+y=1$
$y=1-$

x	y
1	0
2	-1
3	-2

$$\int_0^1 \int_0^{1-y} dx\, dy$$



$$\int_0^1 \left[x\right]_0^{1-y}$$

$$\int_0^1 1-y =$$

$$\left[y\right]_0^1 - \left[\frac{y^2}{2}\right]_0^1$$

$$y - \frac{y^2}{2} \quad 1-\frac{1}{2} = \boxed{\frac{1}{2}} \qquad -(x+y)^{-1}$$

$$-\frac{1}{(x+y)} \qquad -1.1$$

$y = 2-x^2$ $y = x$

$$\int_0^1 \int_1^2 (x^2+y^2)\, dx\, dy =$$

$$\int_0^1 \int_1^2 x^2 dx + \int_1^2 y^2 dx = \int_0^1 \left[\frac{x^3}{3}\right]_1^2 + \left[xy^2\right]_1^2 =$$

$$= \cancel{2}\ \frac{8}{3} - \frac{1}{3} \quad + \quad 2y^2 - y^2 =$$

$$= \frac{7}{3} + y^2$$

$$\int_0^1 \frac{7}{3} + y^2\, dy = \int_0^1 \frac{7}{3} dy + \int_0^1 y^2 dy =$$

$$\left[\frac{7}{3}y\right]_0^1 + \left[\frac{y^3}{3}\right]_1^0 = \frac{7}{3} + \frac{1}{3} = \boxed{\frac{8}{3}}$$

$$\int_3^4 \int_1^2 \frac{dy\, dx}{(x+y)^2} = \int_3^4 \int_1^2 \frac{1}{(x+y)^2}\, dy\, dx =$$

$$\int_3^4 \int_1^2 (x+y)^{-2}\, dy\, dx = \int_3^4 \left[-(x+y)^{-1}\right]_1^2$$

$$\int_3^4 \left[-(x+2)^{-1} - (x+1)^{-1}\right] = \int_3^4 \left[-\frac{1}{x+2} - \frac{1}{x+1}\right] =$$

$$\int_1^2\int_x^{x\sqrt{3}} xy\,dx/dy = \int_1^2 \left[\frac{x^2}{2}y\right]_x^{(x\sqrt{3})^2} dy$$

$$= \int_1^2 \left[\frac{3x^2}{2}y - \frac{x^2y}{2}\right] dy =$$

2 $\quad \log x+2 = \frac{1}{\ }$

$$\int_1^2 x^2y\,dy = \frac{x^2y^2}{2}\Big]_1^2$$

$-(x+2)^{-1}$

$\cancel{2}x$ / x^2

$$\int_1^2\int_x^{x\sqrt{3}} xy\,dy\,dx$$

$\cancel{\frac{x^2y}{2}} = -\cancel{x^2y^0}$

$DN'-ND'$

$\cancel{\frac{2\cdot 2xy}{4}}$

$$\int_1^2\left(\int_x^{x\sqrt{3}} xy\,dy\right)dx$$

$$\int_1^2\left[\frac{xy^2}{2}\right]_x^{x\sqrt{3}} = \int_1^2\left[\frac{x\cdot x^2 3}{2} - \frac{x^3}{2}\right] =$$

$$\int_1^2 \frac{3x^3}{2} - \frac{x^3}{2} = \int_1^2 \frac{\cancel{2}x^3}{\cancel{2}} = \int_1^2 x^3\,dx =$$

$$\left[\frac{x^4}{4}\right]_1^2 = \frac{16}{4} - \frac{1}{4} = \boxed{\frac{15}{4}}$$

$$\int_3^4 \frac{1}{x+2} - \int_3^4 \frac{1}{x+1}$$

$$\left[-\log x+2\right]_3^4 - \left[\log x+1\right]_3^4$$

$$-\log 6 + \cancel{\log 5} - [\cancel{\log 5} - \log 4]$$

$$\log 6 - \log 4 = \boxed{\log\frac{6}{4}}$$

$$\int_1^2\int_x^{x\sqrt{3}} xy\,dx\,dy = \int_1^2\left[\int_x^{x\sqrt{3}} xy\,dx\right]dy$$

$$= \int_1^2\left[\left[\frac{x^2}{2}y\right]_x^{x\sqrt{3}}\right]dy = \int_1^2\left[\frac{3x^2}{2}y - \frac{x^2}{2}y\right]$$

$$\int_1^2 \frac{3}{2}x^2y - \frac{1}{2}x^2y \qquad \frac{3}{2}\int_1^2 x^2y - \frac{1}{2}\int x^2y$$

$$\frac{3}{2}\left[\frac{x^2y^2}{2}\right]_1^2 - \frac{1}{2}\left[\frac{x^2y^2}{2}\right]_1^2 =$$

$$\frac{3}{2}\cdot 2x^2 - \frac{1}{2}\,2x^2 = 3x^2 - x^2 = 2x^2$$

$x = 2 \quad x = 3 \quad y = 1 \quad y = 5$

$2 < x < 3 \quad 1 < y < 5$

$y = 0$
$y = 1 - x^2$

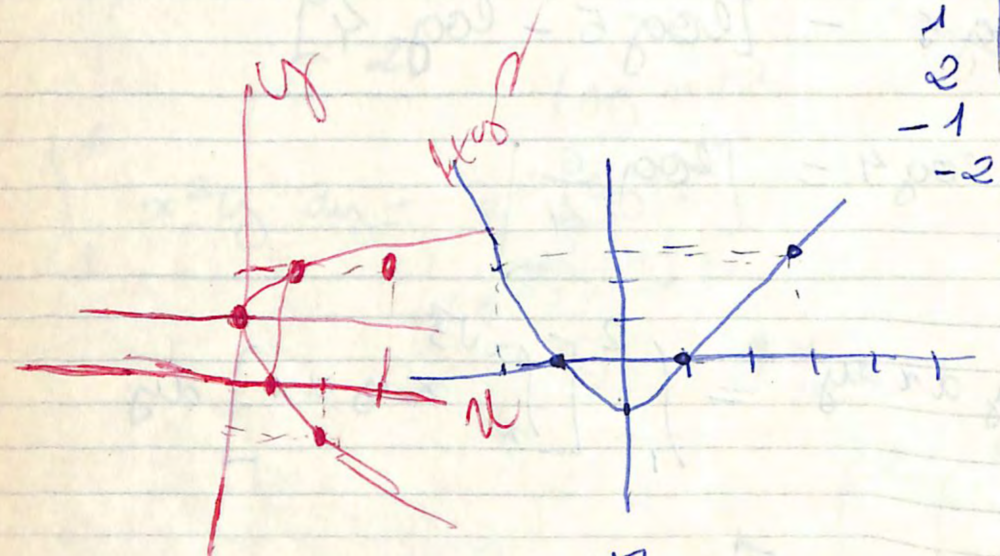
$y = -x^2$ $\quad (-1, -1)$ $\quad 0 = 1 - x^2$

$-1 = -x^2$

$y = 1$

$$\int_{1}^{-1} \int_{0}^{1-x^2}$$

x	y
1	0
2	3
−1	0
−2	3



$$\int_0^1 \int_{x^3}^{\sqrt{x}} f(x,y)\, dy\, dx$$

$y = 1$
$y = 0$

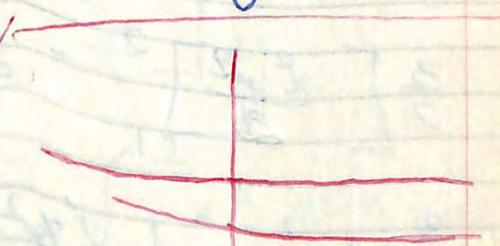
$x = 1$
$x = 0$

$y = \sqrt{x} \Rightarrow x = y^2$

$y = x^3 \quad x = \sqrt[3]{y}$

$$\int_0^1 \int_{\sqrt[3]{y}}^{y^2}$$

$$\int_0^1 \int_{-\sqrt{1-y^2}}^{1-y} dx\, dy$$



x	y
0	1
2	2
3	2

$y = 0$
$y = 1 -$
$y =$

1 -

1 - Eu +
2 - Fernando +
3 - ana +
4 - Levana
5 - augusto
6 - Regina
7 - galope +
8 - márcia +
9 - mininho +
10 - magda +
11 - Inês
12 - Beatriz
13 - mário
14 - tunico +
15 - companhia +
16 - mirna
17 - namorado da mirna.

1 - ~~Eu~~ +
2 - ~~Fernando~~ +
3 - ana
4 - ~~galope~~ +
5 - ~~márcia~~ +
6 - ~~magda~~ +
7 - ~~Tunico~~ +
8 - ~~Colega márcia~~ +
9 - ~~mininho~~ +
10 - Levana
11 - augusto
12 - Regina
13 - Kekén !
14 - mirna +
15 - augusto +
16 - Beth

11 - 5

1 - Eu
2 - Fernando
3 - minho
4 - Galope
5 - marcia
6 - Tunico
7 - colega tunico
8 - magda
9 - Kekeu

nmo

Λ