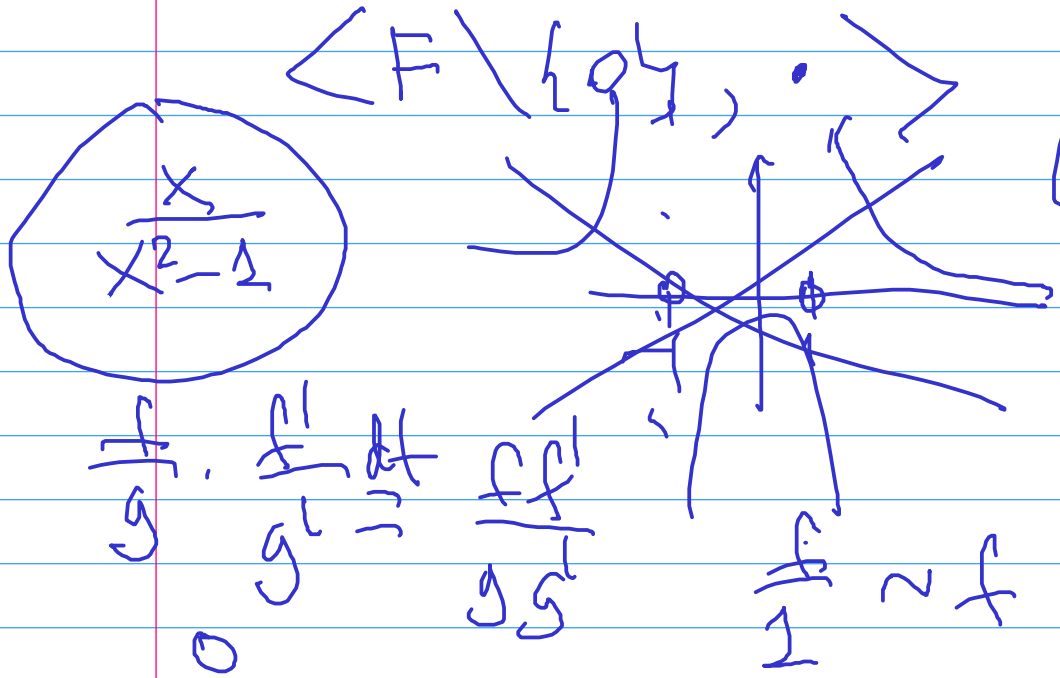
F F^* — multiplicative group of F

$F^* = \langle F \setminus \{0\}, \cdot \rangle$



$R \to R_f$

$f: R \to S$

$R/\ker f \simeq \operatorname{Im} f$

$\xi: \mathbb{R}[x] \to \mathbb{C}$ отображение

$f \mapsto f(i)$

$ev_i|_{\mathbb{R}[x]}$

$f(x) = (x-i)(x+i)g(x) = (x^2+1)g(x)$, $g(x) \in \mathbb{R}[x]$

$\deg = a_3 x$

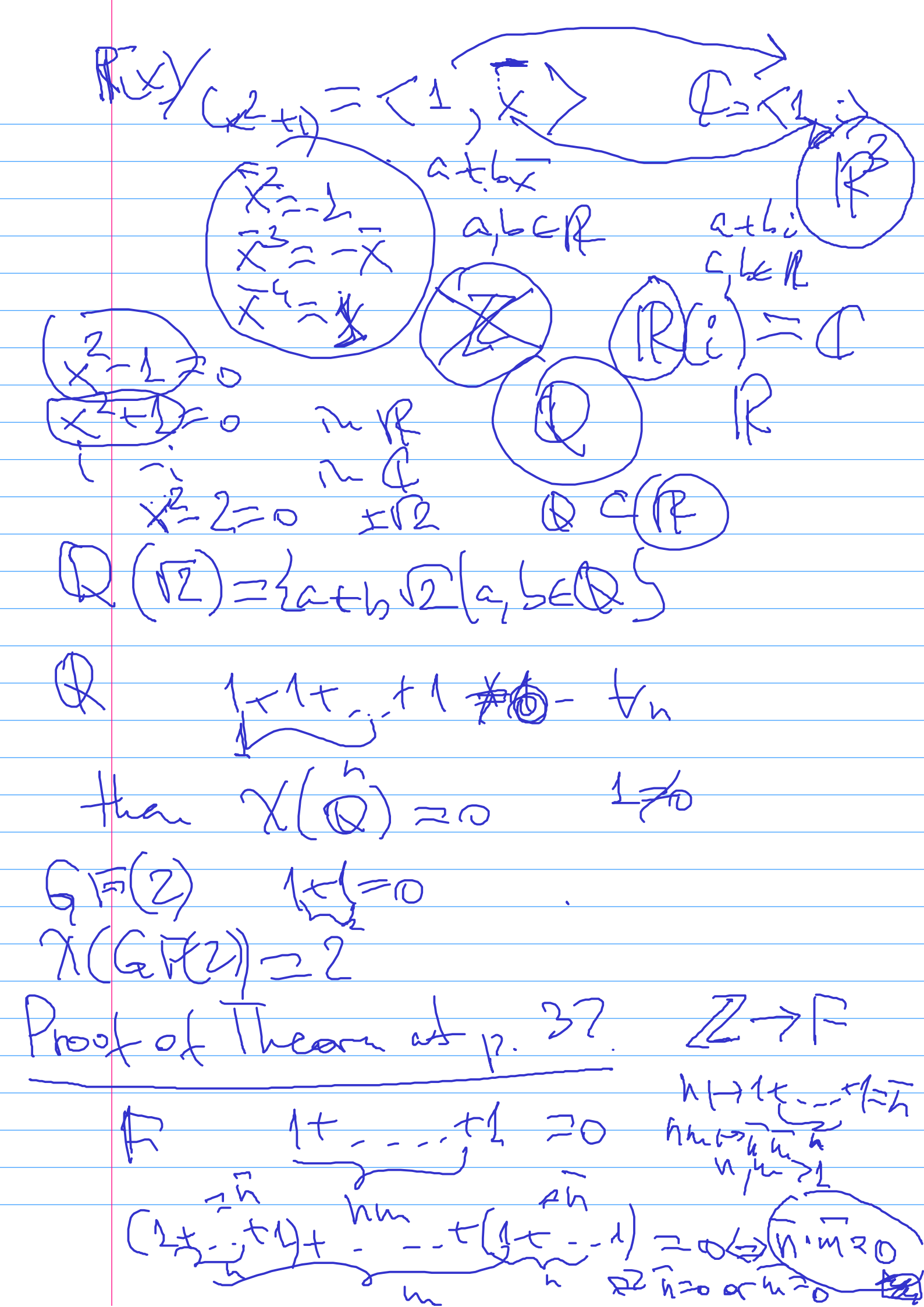
$\ker \xi = (x^2+1)$

$\mathbb{R}[x]/\ker \xi \simeq \mathbb{C}$

$\ker \xi = \{f \in \mathbb{R}[x] \mid f(i) = 0\}$

отображение: $(x-a)(x-b)$

$a = b$: $f(x) = (x-\alpha)(x-\alpha)\ldots(x-\alpha)$


$\mathbb{R}(x)/(x^2+1) = \langle 1, x \rangle$
$a+bx$
$a,b \in \mathbb{R}$
$x^2 = -1$
$x^3 = -x$
$x^4 = 1$
$\mathbb{C} = \langle 1, i \rangle$
$a+bi$
$a,b \in \mathbb{R}$
$\mathbb{R}(i) = \mathbb{C}$
$\mathbb{R}$
$x^2-1=0$
$(x+1)=0$
$x^2-2=0$
in $\mathbb{R}$
in $\mathbb{C}$
$\pm\sqrt{2}$
$\mathbb{Q} \subset \mathbb{R}$
$\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$
$\mathbb{Q}$
$1+1+\ldots+1 \neq 0 \quad \forall n$
1
then $\chi(\mathbb{Q}) = 0$
$1 \neq 0$
$\mathbb{G}\mathbb{F}(2)$
$1+1=0$
$\chi(\mathbb{G}\mathbb{F}(2)) = 2$
Proof of Theorem at p. 37
$\mathbb{Z} \to \mathbb{F}$
$\mathbb{F}$
$1+\ldots+1 = 0$
$n \mapsto 1+\ldots+1 = n$
$n \cdot m \mapsto n \cdot m$
$n, m > 1$
$(1+\ldots+1)+\ldots+(1+\ldots+1) = 0 \Leftrightarrow n \cdot m = 0$
$\Rightarrow n = 0$ or $m = 0$

GF(q) GF(2) = {0, 1}

Galois $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$

$\mathbb{Z}/4\mathbb{Z}$ $n = 0$

$\bar{2} \cdot \bar{3} = \overline{2+3} = \bar{5} = \bar{1}$

$\bar{2} \cdot \bar{3} = \overline{2 \cdot 3} = \bar{6} = \bar{2}$

$n = n_1 n_2$ $\bar{n}_1 \cdot \bar{n}_2 = \bar{0}$

$n_1, n_2 > 1$

$\mathbb{Z} \to F$

$\mathbb{Z}/p\mathbb{Z}$ is a field = GF(p) $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, $n \mapsto \bar{n}$

$\{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{p-1}\}$

$\mathbb{Z}$ | n inv in $\mathbb{Z}$? a, b: $an + bm = GCD(n, m)$

$0 \le n \le p-1$ $GCD(n, p) = 1$

$n = p$ $\bar{a}\bar{n} + \bar{b}\bar{p} = \bar{1}$

$\forall \bar{n} \in \mathbb{Z}/p\mathbb{Z} \; \exists \bar{a} \in \mathbb{Z}/p\mathbb{Z}$: $\bar{a}\bar{n} = \bar{1}$

$\bar{n}^{-1}$

GF(3) = {0, 1, 2} $\bar{1} + \bar{2} = \bar{0}$

GF(4)

$GF(q) \supset GF(p)$

$f: \mathbb{Z} \to F$

$n \mapsto 1 + \dots + 1$

$f(\mathbb{Z}) \subset F$ — prime subfield

prime subfield

$p > 0$ $GF(p)$

$p = 0$ $\mathbb{Q}$

$1 + 1 + \dots + 1$

$\bar{n} \cdot \bar{m} = \overline{nm}$

$\mathbb{Z}$

$\frac{n}{m}$ $m \neq 0$

$\mathbb{Q}$

$GF(p)(\alpha_1, \dots, \alpha_n) \simeq GF(q)$

$\alpha \in GF(q)$ $\quad x = \lambda_1 \alpha_1 + \dots + \lambda_n \alpha_n$

$\alpha \in GF(p)$ $\quad \lambda_i \in GF(p)$

$\dim_{GF(p)} GF(q) = n$ $\quad p^n$

$|GF(q)| = p^n$ $\quad q = p^n$.

$GF(4) = \{0, 1, \alpha, \alpha+1\}$ $\quad GF(p)$

$GF(2)$ $\quad p = 2$

$\alpha + (\alpha+1) = 1$

$(\alpha+1) + (\alpha+1) = 0$

$GF(2)$

$\alpha^2 = \alpha + 1$

$\alpha \neq 1$.

$(\alpha+1)^2 = \alpha^2 + 2\alpha + 1 = \alpha + 1 = 0$

$GF(p) \simeq \mathbb{Z}/p\mathbb{Z} = (\mathbb{Z}/n\mathbb{Z}, +, \cdot)$