Ch 1

$\boxed{\text{Density theorems}}$

arche-type : $\boxed{\text{Dirichlet density}}$

Thm: $m \in \mathbb{N}$ $\quad (a, m) = 1$

set of primes p : $p \equiv a \bmod m$
has density $\dfrac{1}{\varphi(m)}$

- $f(t) \in \mathbb{Z}[t]$ with leading coeff 1
how to determine $f(t)$ irred by reducing mod p?

Ex: $f = X^4 + 3X^2 + 7X + 4$

mod 2 : $f \equiv X(X^3 + X + 1)$
decomposition $1, 3$

mod 11 : $f \equiv (X^2 + 5X - 1)(X^2 - 5X - 4)$
decomposition $2, 2$

$\Rightarrow$ f must be irreducible.

? Can check irreducibility by looking at SINGLE prime ?

i.e. $\exists ?\, p$: $f \bmod p$ has decomp 4 ?

$f \in \mathbb{Z}[t]$ leading coeff 1

disc $\Delta(f) \neq 0$ i.e. f has distinct zeros $\subset \overline{\mathbb{Q}}$

$\deg(f) = n$

$\{\alpha_1, \ldots, \alpha_n\}$ roots

$K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ is Galois / $\mathbb{Q}$

$\mathrm{Gal}(K/\mathbb{Q})$ = $\mathbb{Q}$-autos of K

each σ permutes the roots α_i

$\mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow S_n$

$\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \Rightarrow$ write σ in cycle-form including 1-cycles.

and call this <u>cycle-pattern of σ</u>

partition of n

p prime $p \nmid \Delta(f)$

f mod p decomposes in distinct irreducible factors

call their degrees the <u>decomposition pattern</u> of f mod p

partition of n

Frobenius density

Thm: $\{$primes p : decomposition pattern of f mod p is $n_1, n_2, \dots, n_t\}$

has density

$$\frac{1}{\# \mathrm{Gal}} \left(\# \{ \sigma \in G \mid \text{cycle type}(\sigma) = n_1, n_2, \dots, n_t \} \right)$$

(Consequence: $\#\{$irred factors of f over $\mathbb{Q}\}$ = average of zeroes in $\mathbb{F}_p$ of f mod p over all primes.)

Frobenius - substitution

prime p fixed $\quad \overline{\mathbb{F}}_p$ alg closure of $\mathbb{F}_p$

$\mathrm{Frob}: \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p \quad \alpha \mapsto \alpha^p \quad$ Frobenius auto

Galois theory for finite fields

$(!=)$ cycle pattern of Frob as permutation on the zeroes of f = decomposition type of f over $\mathbb{F}_p$

for all $f \in \mathbb{F}_p[t]$ without repeated factors.
so also for all F for $p \nmid \Delta(f)$

(Ch 4

Frobenius-substitution σ_p is auto of
$K = \mathbb{Q}(\alpha_1, \to \alpha_n)$

How to relate K with $\overline{\mathbb{F}}_p[t]/(f(t))$

Dfn **place** of K over p is map
$$\psi : K \longrightarrow \overline{\mathbb{F}}_p \cup \{\infty\}$$

- ① $\psi^{-1}(\overline{\mathbb{F}}_p)$ is subring of K and
$$\psi : \psi^{-1}(\overline{\mathbb{F}}_p) \longrightarrow \overline{\mathbb{F}}_p \text{ is homomorph}$$
② $\psi(x) = \infty$ if and only if $\psi(x^{-1}) = 0$
$\forall x \in K^*$

- $\boxed{\text{FACTS}}$

Ⓐ $\forall$ prime p $\exists$ place of K over p

Ⓑ If ψ, ψ' are two places over p
$\Rightarrow \psi' = \psi \circ \tau$ for some $\tau \in \mathrm{Gal}(K/\mathbb{Q})$

Ⓒ If $p \nmid \Delta(f)$ then τ is uniquely determined by ψ and ψ'.

(ii)

$p \nmid \Delta(f)$

ψ place of K over p

$\Rightarrow \{\psi(\alpha_1), \ldots, \psi(\alpha_n)\}$ are zeros of $f \bmod p$ in $\overline{\mathbb{F}}_p$

$\psi' = \mathrm{Frob} \circ \psi$ is another place of K over p

$\Rightarrow \exists!$ ~~Φ_p~~ $\mathrm{Frob}_\psi \in \mathrm{Gal}(K/\mathbb{Q})$ s.t.

$$\psi \circ \mathrm{Frob}_\psi = \mathrm{Frob} \circ \psi$$

Frob_ψ is the Frobenius substitution.

characteristic feature:

$$\psi(\mathrm{Frob}_\psi(x)) = \mathrm{Frob}(\psi(x)) \quad \forall x \in K.$$

<u>So</u> Frob_ψ permutes $\alpha_1, \ldots, \alpha_n$ in same way as Frob permutes zeroes $\psi(\alpha_1), \ldots, \psi(\alpha_n)$ of $f \bmod p$

but Frob_ψ depends on choice of ψ

If $\mathfrak{P}$ ranges over places for fixed prime p

$\Rightarrow$ $\mathrm{Frob}_{\mathfrak{P}}$ ranges over conjugacy class of $\mathrm{Gal}(K/\mathbb{Q})$

$\underline{\underline{\sigma_p}}$ is typical element of this conjugacy class

CHEBOTAREV DENSITY

- f poly $\mathbb{Z}[t]$ leading coeff 1
  $\Delta(f) \neq 0$

  C conjugacy class of $\mathrm{Gal}(K/\mathbb{Q})$

  $K = \mathbb{Q}(\underbrace{\alpha_1, \ldots \alpha_n}_{\text{roots of } f})$

- $\{\text{primes } p \nmid \Delta(f) \text{ s.t. } \sigma_p \in C\}$

has density $\dfrac{\# C}{\# \mathrm{Gal}(K/\mathbb{Q})}$

no nilpotents

+ no additive torsion.

F1

AIM. classify reduced finite rank $\mathbb{Z}$-rings with Frobenius lifts

AKA: what is the Galois site of $\mathbb{F}_1$?

EXAMPLES:

① $\mathbb{Z}[\mu_n] = \dfrac{\mathbb{Z}[X]}{(X^n - 1)}$ with FL $X \mapsto X^p$

$\simeq \mathbb{F}_1 \subset \mathbb{F}_{1^n}$

② $R(G)$ G finite gp with FL = Adams oper.

③ $Z(G) = Z(\mathbb{Q}G)$ center of finite gp alg.

with FL induced by $e_g \mapsto e_{g^n}$

④ $\dfrac{\mathbb{Z}[X]}{f(X)}$ $f(X)$ separable poly

with λ-structure.

Discriminants

$$R = \bigoplus_{i=1}^{n} \mathbb{Z}\,\omega_i$$ then discriminant is $\mathbb{Z}$-ideal generated by

$$\Delta(R) = \det\left(\mathrm{Tr}_{R/\mathbb{Z}}(\omega_i\omega_j)\right)_{i,j}$$

<u>eigenschap</u> $p \nmid \Delta(R) \iff R/pR$ is "étale" over $\mathbb{F}_p$

$\iff p$ unramified

$\iff R/pR$ geen nilpotenten

i.e. $R/pR \cong \mathbb{F}_{p^{a_1}} \times \dots \times \mathbb{F}_{p^{a_e}}$

<u>Vbn:</u>

1) $\Delta(\mathbb{Z}[\mu_n]) = n$

2) $$\Delta(R(G)) = \frac{(\#G)^{\#\text{conj klass}}}{\prod_{\text{conjug } C} \#C}$$

3) $$\Delta(Z(G)) = \frac{(\#G)^{\#\text{conj}} \prod_{\text{conj } C} \#C}{\prod_{\text{irred}} (\dim_{\mathbb{C}} S_i)^2}$$

4) $$\Delta\left(\frac{\mathbb{Z}[x]}{f(x)}\right) = \operatorname{discr} f = \prod_{i<j} (\alpha_i - \alpha_j)^2$$

α_i wortels van f

vgl R(6) $\square$ ○

F3

<u>Stelling 1</u> : $p \nmid \Delta(R)$

$\Rightarrow \psi^p$ is automorfisme van R en is de <u>unieke</u> lift van $\mathrm{Frob}_p : R/pR \to R/pR$

Bewijs

$$p \nmid \Delta(R) \Rightarrow R/pR = \overbrace{\mathbb{F}_{p^{a_1}} \times \dots \times \mathbb{F}_{p^{a_k}}}^{\text{étale } \mathbb{F}_p\text{-alg.}}$$

dus $\mathrm{Frob}_p : x \mapsto x^p$ is auto on R/pR

$\exists$ category equivalence between

$$\{\hat{\mathbb{Z}}_p\text{-étale algebras}\} \qquad \{\mathbb{F}_p\text{-étale alg.}\}$$

$$A \longmapsto A \otimes_{\hat{\mathbb{Z}}_p} \mathbb{F}_p$$

ψ^p is endo-lift of Frob_p but

— on $A = R \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}_p$

~~vo~~ $\psi^p \otimes 1$ is unique lift of Frob_p and is auto of finite order

$\Rightarrow \psi^p : R \to R$ is auto and unique lift of Frob_p

$\boxtimes$

algemene $\mathbb{C}$-<u>étale</u> A is vd von

$$A = \frac{\mathbb{C}[x_1, \dots, x_n]}{(f_1, \dots, f_n)} \quad \text{met} \quad \det \mathrm{Jac}\left(\frac{\partial f_i}{\partial x_j}\right) \in A^*$$

$$\Delta(R(S_3)) = \frac{6^3}{1.2.3} = 36$$

Galois theory à la Grothendieck

$K = R \otimes_{\mathbb{Z}} \mathbb{Q}$ is finite étale $\mathbb{Q}$-algebra

$\cong L_1 \times \dots \times L_k$ $\quad [L_i : \mathbb{Q}]$ sep finite field exten

$S = \mathrm{Hom}_{\mathbb{Q}\text{-alg}}(K, \overline{\mathbb{Q}})$ is finite set

with $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action.

$$\begin{tikzcd}
K \arrow[r, "s"] \arrow[dr, "\sigma \circ s = \sigma \circ s"'] & \overline{\mathbb{Q}} \arrow[d, "\sigma"] \\
& \overline{\mathbb{Q}}
\end{tikzcd}$$

<u>? what is S ?</u>

$$K = \frac{\mathbb{Q}[x]}{(f_1(x))} \times \frac{\mathbb{Q}[x]}{(f_2(x))} \dots \times \frac{\mathbb{Q}[x]}{(f_k(x))}$$

en $(f_i, f_j) = 1$

$$K = \frac{\mathbb{Q}[x]}{(f_1(x) f_2(x) \dots f_k(x))}$$

$s \in \mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$ volledig bepaald door $s(X)$

Maar $s(X)$ moet nul zijn van $f_1(X) f_2(X) \cdots f_k(X)$

__Dus__ $S = \mathrm{Roots}\,(f_1(X) f_2(X) \cdots f_k(X))$

en actie is gewone Galois actie op $\overline{\mathbb{Q}}$

Grothendieck - Galois

$\exists$ category equivalence

$$\boxed{\mathbb{Q}\text{-étale algebras}} \longleftrightarrow \boxed{\text{finite } \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\text{ subsets of } \overline{\mathbb{Q}}}$$

$$K \longmapsto \mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$$

$$K = \mathbb{Q}(\alpha_1) \times \cdots \times \mathbb{Q}(\alpha_k) \longmapsto S = \mathcal{O}(\alpha_1) \sqcup \cdots \sqcup \mathcal{O}(\alpha_k)$$

diff orbits

extra info as R Frob lifts hold

$\Rightarrow \psi^n : K = R \otimes \mathbb{Q} \longrightarrow K = R \otimes \mathbb{Q}$
endos ~~autos~~ of $\mathbb{Q}$-algebras.

Monoid $\mathbb{N}_\times = \{1, 2, 3, \ldots\}$ with multiplicative structure

<u>So</u> If R has Frob-lifts then

$S = \mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$ is finite

$\underset{\text{left act}}{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})} \times \underset{\text{right action.}}{\mathbb{N}_\times}$ set

$$\begin{tikzcd} K \arrow[r, "s"] & \overline{\mathbb{Q}} \\ K \arrow[u, "\psi^n"'] \arrow[ur, dashed] & \end{tikzcd} \qquad s \circ n = s \circ \psi^n$$

$\boxed{\text{Back to R!}}$

$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on left on $S = \mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$

$\Rightarrow$ groepmorphism

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \cancel{\mathrm{Aut}}(S, S) \subset \mathrm{Map}(S, S)$$

Als kern $= N \triangleleft \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

dan is $\overline{\mathbb{Q}}^N = L$ finite Galois

extn of $\mathbb{Q}$ with Gal gp $\overline{G} = \mathrm{Gal}/N$

wat is die L?

$\{\alpha_1, \ldots, \alpha_e\}$ wortels $= S$

$\Rightarrow L = \mathbb{Q}(\alpha_1, \ldots, \alpha_e)$

dus alle factoren $R \otimes \mathbb{Q} = K = L_1 \times \ldots \times L_e$

zijn deellichamen van L en dus

elke $\sigma \in \overline{G}$ geeft auto ~~naar~~ L_i

Neem nu $\mathcal{O}_L$ is ~~[illegible]~~ integrale sluiting van $\mathbb{Z}$ in L dan hebben we

$$S = \mathrm{Hom}_{\mathbb{Q}}(K, \bar{\mathbb{Q}}) = \mathrm{Hom}_{\mathbb{Q}}(K, L)$$

$$= \mathrm{Hom}_{\mathbb{Z}}(R, \mathcal{O}_L)$$

waarop werkt $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \times \mathbb{N}_{\times}$ op S

$$\begin{tikzcd}
R \arrow[r, "s"] \arrow[dr, dashed, "\sigma \circ s" near end] & \mathcal{O}_L \arrow[d, "\sigma"] \\
R \arrow[u, "\psi^n"] \arrow[ur, dashed, "s \circ \psi^n" near end] & \mathcal{O}_L
\end{tikzcd}$$

Neem $\sigma \in \mathrm{Gal}(L/\mathbb{Q}) = \bar{G}$

<u>CHEBOTAREV</u> says $\exists$ ∞ many primes p s.t. $\exists$ ~~[illegible]~~ $\underline{P} \lhd \mathcal{O}_L$ lying over p with σ lift of $\mathrm{Frob}_p : \mathcal{O}_L/\underline{P} \to \mathcal{O}_L/\underline{P}$

$$x \mapsto x^p$$

volgen so veel mogen onderstelle $p \nmid \Delta(R)$

But then restriction of σ to R via embedding s is equal to ψ^p as there is a unique lift of the Frobenius. That is we have

$$\sigma \circ s = s \circ \psi^p \quad \text{on } R$$

This was for fixed $\sigma \in Gal(L/\mathbb{Q})$

<u>So have</u>:

Image

$$Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow Auto(S,S) \subset Map(S,S)$$

is contained in image

$$\mathbb{N}_X \longrightarrow Map(S,S)$$

$$n \mapsto - \circ \psi^n$$

$\mathbb{N}_\alpha$ is Abelian monoid

$\Rightarrow$ image in $\mathrm{Map}(S,S)$ is abelian monoid

$\Rightarrow$ image $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(S,S)$ is abelian gp

so $\mathrm{Gal}(L/\mathbb{Q})$ is Abelian !

$\boxed{\text{THM : KRONECKER-WEBER}}$

$L/\mathbb{Q}$ Abelian $\Rightarrow$

$L \subset \mathbb{Q}(\mu_c)$ met

c enkel deelbaar door priemgetallen die ramifiëren in L (i.e. die $\Delta(L)$ delen).

omdat L de gemeenschappelijke Galois uitbreiding is van componenten van

$R \otimes \mathbb{Q} = K = L_1 \times \cdots \times L_n$

ramifiëren deze priemen ook in R.

F11

We weten:

$$\mathrm{Gal}(\mathbb{Q}(\mu_c)/\mathbb{Q}) = (\mathbb{Z}/c\mathbb{Z})^*$$

en weten ook Frobenius lifts c dit geval

$$\forall p \nmid c : \quad p \bmod c \in (\mathbb{Z}/c\mathbb{Z})^*$$

is Frobenius element of any prime in extension $\mathbb{Q} \subset \mathbb{Q}(\mu_c)$.

$\boxed{\text{SAMENVATTEND}}$

$\exists\, c \in \mathbb{N}$ met enkel priemdelers van $\Delta(R)$ s.t. $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-actie op $S = \mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$

$$= \mathrm{Hom}_{\mathbb{Z}}(R, \mathcal{O}_L)$$

factoriseert via cyclotoom character

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow (\mathbb{Z}/c\mathbb{Z})^* = \mathrm{Gal}(\mathbb{Q}(\mu_c)/\mathbb{Q})$$

en $\forall\, p \nmid \Delta(R)$ geldt dat actie van $p \in \mathbb{N}_\times$ op S gelijk is aan actie van $p \bmod c \in \mathrm{Gal}(\mathbb{Q}(\mu_c)/\mathbb{Q})$

en $R \subset \mathbb{Z}[\mu_c] \times \dots \times \mathbb{Z}[\mu_c]$

We hebben nu al actie van

$Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \times \mathbb{N}_\times$ op S gefactoriseerd

via $\hat{\mathbb{Z}}^* \times \mathbb{N}_\times$ en willen nu verder

factoriseren via $\hat{\mathbb{Z}}_\times$ (multiplicative monoid van profinite integers $\hat{\mathbb{Z}}$)

$\boxed{\text{uitlaten: definitie van } \hat{\mathbb{Z}} \quad \text{lemma profinite Fib}}$

$\underline{\forall d \in \mathbb{N}_\times}$: $\psi^d(R)$ is sub λ-ring of R

so satisfies foreporg so met corresp. [illegible] $= d.S$

$\exists c_d$: $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ action on dS

factorises through $(\mathbb{Z}/c_d\mathbb{Z})^*$ and

action of one n s.t. $\boxed{nd.S = d.S}$ is

same as action of $n \bmod c_d$

such n's are products of primes unramified in $\psi^d(R)$.

F13

Define a_p smallest $\in \mathbb{N}$ s.t.

$$p^{a_p+1} \cdot S = p^{a_p} \cdot S$$

$\Rightarrow \forall p \nmid \Delta(R) : a_p = 0$

So only finitely many p's with $a_p > 0$

$$r_0 = \prod_p p^{a_p} \in \mathbb{N}$$

en $\forall n : \quad n \cdot S = \gcd(n, r_0) \cdot S$

Define $\quad r = \operatorname{lcm}(d \cdot c_d \mid d \mid r_0)$

CLAIM: acting factorises through $(\mathbb{Z}/r\mathbb{Z})^\times$

T.B. $\quad d_1 \equiv d_2 \bmod r \Rightarrow d_1 \cdot$ en $d_2 \cdot$ werken 't zelfde op S

$r_0 \mid r \Rightarrow \gcd(d_1, r_0) = \gcd(d_2, r_0) = d$

$\Rightarrow d_1 \cdot S = \underline{d} \cdot S = d_2 \cdot S$

$d'_i \cdot dS = dS$

$d_1 = d\, d'_1$ en dus $(d'_1, c_d) = 1 = (d'_2, c_d)$

(F14

~~03 235 05 06~~ holy 2

$d_1 = d d'_1 \equiv d d'_2 = d_2 \mod d c_d$

$\Rightarrow d'_1 \equiv d'_2 \mod c_d$ en dus werken

ze 't zelfde op d. S

maar dan werken d_1 en d_2 'tzelfde

op S $\boxtimes$

(1) <u>Conclusie</u>: $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \times N_x$ action factors through $\hat{\mathbb{Z}}_x$ en dus correspondence

$(\mathbb{F}_1\text{-étale site}) \longleftrightarrow (\hat{\mathbb{Z}}_x\text{ - finite sets})$

en $\mathrm{Gal}(\overline{\mathbb{F}}_1/\mathbb{F}_1)$ - monoid $= \hat{\mathbb{Z}}_x$

dus $\mathbb{Q}(\mu_\infty) =$ "alg closure of $\mathbb{F}_1$"

F15

(2) $\hat{\mathbb{Z}}_X$ heeft element

(-1) zodat $(-1)^2 = 1$

dus: op R is involutie

in geval $R = R(G)$ is deze involutie

$\chi_V \to \chi_{V^*}$

heeft ook $0 \in \hat{\mathbb{Z}}_X$ en dus is $0.S$ is

factor $\mathbb{Q}$ in $\mathbb{Q} \otimes_{\mathbb{Z}} R$

dus $\nexists$ lichamen met ~~deelbare R λ-ring~~

projectie: $S \to 0.S$

$\mathbb{Q} \otimes R \to \mathbb{Q}$

in geval $R(G)$

$\chi_V \to \dim(V)$

F16

③ $\mathbb{F}_1$ - subschemes of $\mathbb{P}^1_{\mathbb{Z}}$

$\updownarrow$

$\mathbb{Z}[t]/f(t)$ roots of $f(t)$ inv order $t \to t^p$

$\Rightarrow$ bestaan enkel uit roots of unity

$\Rightarrow$ $[n] = \mathbb{V}(\Phi_n(x))$ basis bouwstenen