2.1 Rings

Ring: Commutative, unital

Homomorphism: $\varphi: R \to S$:

$\varphi(r+r') = \varphi(r) + \varphi(r')$ $\quad \varphi(0)=0 \quad \varphi(-r) = -\varphi(r)$

$\varphi(rr') = \varphi(r)\varphi(r')$ $\quad \varphi(1) = 1$

Subring:
- $S \subseteq R$ and $0, 1 \in S$
- Closed under $+, \cdot$ and $-$

$\{0\}$ is ~~not~~ a Subring unless $1=0$!

e.g. inclusion $\iota: S \to R$ is a homomorphism.

Ex 2.1.2 $\cap$ of subrings is a subring.

Exm 2.1.3 $\exists!$ homo $\mathbb{Z} \to \mathbb{R}$

Ideal $I \trianglelefteq R$, $\exists$ $can_I : R \to R/I$, $a \mapsto aI$.
↳ Surjective and $\ker(can) = I$.

Universal property: ring S and homo $\varphi: R \to S$ with $I \subseteq \ker\varphi$, $\exists! \bar{\varphi}: R/I \to S$:

$$\begin{tikzcd} R \arrow[r, "can"] \arrow[dr, "\varphi"'] & R/I \arrow[d, "\exists!\bar{\varphi}"] \\ & S \end{tikzcd}$$

Integral domain: R s.t $0_R \neq 1_R$ and $\forall\, r, r' \in R$, $rr' = 0 \Rightarrow r = 0$ or $r' = 0$.

Ideal generated by $T \subseteq R$: $\langle T \rangle :=$ smallest ideal containing R.

$\langle r_1, \dots, r_n \rangle = \{ a_1 r_1 + \dots + a_n r_n : a_1, \dots, a_n \in R \}$

Principal ideal: $\langle r \rangle$.

Principal ideal domain = integral domain that has only principal ideals.

r divides s: $r \mid s \iff \exists\, a \in R$ s.t $s = ar$.
$\iff s \in \langle r \rangle$
$\iff \langle s \rangle \subseteq \langle r \rangle$.

unit: $u \in R$ if $\exists\, u^{-1}$ s.t $u^{-1}u = uu^{-1} = 1$
$\iff \langle u \rangle = R$.

Coprime: $r, s \in R$ if for $a \in R$,
$a \mid s$ and $a \mid r \Rightarrow a$ is a unit.

Prop 2.1.12: R a principal ideal domain, $r, s \in R$.
r, s coprime $\iff ar + bs = 1$, $(\exists\, a, b \in R)$.

2.2. Fields

Field = ring K w/ $0 \neq 1$ and $\forall\, r \in K$, r is a unit.

Lem 2.2.2: Homo between fields is injective.

Characteristic of R:

$$\operatorname{Char} R = \begin{cases} \text{least } n > 0 \text{ s.t } n \cdot 1_R = 0 & \text{if } \exists\, n \\ 0 & \text{otherwise} \end{cases}$$

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ have char $= 0$
- $\mathbb{F}_p$ has char p.

Lem 2.2.5: Char of an int. dom. is either 0 or prime.

Lem 2.2.6: $\varphi: K \to L$ homo of fields. Then $\operatorname{char} K = \operatorname{Char} L$.

Subfield: Subring of field that is a field.

prime subfield: of K is the intersection of all subfields:

$$\left\{ \frac{m \cdot 1_K}{n \cdot 1_K} : m, n \in \mathbb{Z} \text{ with } n \cdot 1_K \neq 0 \right\}$$

Lem 2.2.10: Let K be a field
1) if $\operatorname{Char} K = 0$, then prime subfield of K is $\mathbb{Q}$.
2) if $\operatorname{char} K = p$, then prime subfield of K is $\mathbb{F}_p$.

Lem 2.2.11: Every finite field has positive char.

Irreducible: $r \in R$ if $r \neq 0$, r not a unit, and if $a, b \in R$, $r = ab \Rightarrow a$ or b a unit.

Prop 2.2.14: R a principal ideal domain, and $0 \neq r \in R$. Then
r is irreducible $\iff R/\langle r \rangle$ is a field.

Exm 2.2.15: $\mathbb{F}_p$ a field $\iff p$ is prime

3.1 Ring of Polynomials

Dfn 3.1.1: R a ring. Poly over R is a tuple $(a_0, a_1, \dots)$ s.t $\{i : a_i \neq 0\}$ is finite.

Forms ring: $(a_0, a_1, \dots) + (b_0, b_1, \dots) = (a_0 + b_0, \dots)$

$(a_0, a_1, \dots) \cdot (b_0, b_1, \dots) = (c_0, c_1, \dots)$

$1 = (1, 0, 0, \dots)$. $\quad c_k = \sum_{i+j=k} a_i b_j$

Rephrasing: $p = (a_0, a_1, \dots) = a_0 + a_1 r + \dots + a_n r^n$.

Lem 3.1.5 (Universal property of poly ring)

R, B rings. $\forall$ homo $\varphi : R \to B$, $b \in B$, $\exists!\ \theta : R[t] \to B$ such that $\theta(a) = \varphi(a)\ \forall a \in R$, $\theta(t) = b$

Dfn 3.1.6: $\varphi : R \to S$ a ring homo. "Induced homo" $\varphi_* : R[t] \to S[t]$ is ! and $\varphi_*(a) = \varphi(a)$ $\forall a \in R$, $\varphi_*(t) = t$.

Substitution: $t \mapsto t + c$ is invertible.

Dfn 3.1.8: $\deg(f) =$ largest $n \in \mathbb{N}$ s.t $a_n \neq 0$

Convention: $\deg(0) = -\infty$.

Lem 3.1.10: R an integral domain. Then

(i) $\deg(fg) = \deg(f) + \deg(g)$

(ii) $R[t]$ is an integral domain

(iii) units in $R[t]$ = nonzero constant polys

(iv) Poly over R is irreducible iff has $\deg > 0$ and cannot be expressed as product of two polynomials of $\deg > 0$.

3.2 Factorizing Polynomials

Prop 3.2.1: K a field and $f, g \in K[t]$, s.t $f = qg + r$ and $\deg(r) < \deg(g)$

Prop 3.2.2: K a field. Then $K[t] =$ PID.

Cor 3.2.5: K a field and let $0 \neq f \in K[t]$.
$\Rightarrow f$ is irreducible $\Leftrightarrow$ $K[t]/\langle f \rangle$ is a field.

Lem 3.2.6: K a field and $f(t) \in K[t]$, $\deg f > 0$
Then $f(t)$ is divis by some irreducible in $K[t]$.

Lem 3.2.7: K a field and $f, g, h \in K[t]$. Suppose f is irreducible and $f \mid gh$. Then $f \mid g$ or $f \mid h$.

Thm 3.28: K a field and $0 \neq f \in K[t]$. Then

$$f = a f_1 f_2 \cdots f_n$$

for some $n \geq 0$, $a \in K$ and monic irreducibles $f_1, \dots, f_n \in K[t]$. These guys are ! (up to reordering)

Lem 3.29: $f(t) \in K[t]$, $a \in K$: $f(a) = 0 \Leftrightarrow (t-a) \mid f(t)$

Dfn 3.2.10: K a field, $0 \neq f(t) \in K[t]$, and $a \in K$ a root of f. The multiplicity of a: $!\, m \in \mathbb{Z}$ s.t. $(t-a)^m \mid f(t)$ but $(t-a)^{m+1} \nmid f(t)$.

Prop 3.2.13: K a field and $0 \neq f \in K[t]$. Write $\alpha_1, \dots, \alpha_k$ for any distinct roots in K of f, and $m_1, \dots, m_k$ for their multiplicities. Then

$$f(t) = (t - a_1)^{m_1} \dots (t - a_k)^{m_k} g(t)$$

For some $g(t) \in K[t]$ that has no roots in K.

Cor 3.2.14: K a field and $f \in K[t]$. Suppose f has k distinct roots with multiplicities $m_1, \dots, m_k$.
Then $m_1 + \dots + m_k \leq \deg(f)$.

Algebraically closed: every nonconstant poly has at least one root in K.

Cor 3.2.15: K algebraically closed.

$$f(t) = c(t - a_1)^{m_1} \dots (t - a_k)^{m_k}$$

3.3 Irreducible Polynomials

Lem 3.3.1: k a field, $f \in k[t]$.

(i) f constant $\Rightarrow$ f not irreducible

(ii) $\deg f = 1 \Rightarrow f$ irreducible

(iii) $\deg f \geq 2$, f has root $\Rightarrow$ f reducible

(iv) $\deg f \in \{2,3\}$, f no root $\Rightarrow$ f irreducible.

Dfn 3.3.5: primitive: poly whose coeffs have no common divisor except ± 1.

Lem 3.3.6: $f(t) \in \mathbb{Q}[t]$. $\exists$ primitive poly $F(t) \in \mathbb{Z}[t]$, $\alpha \in \mathbb{Q}$ s.t $f = \alpha F$.

f irreducible "over k"

Lem 3.3.7 (Gauss)

1. prim x prim = prim over $\mathbb{Z}$
2. irreducible over $\mathbb{Z}$ $\Rightarrow$ irreducible over $\mathbb{Q}$.

Prop 3.3.8 (Mod p method): $f(t) = a_0 + \ldots + a_n t^n \in \mathbb{Z}[t]$.
If $\exists$ prime p s.t $p \nmid a_n$ and $\bar{f} \in \mathbb{F}_p[t]$ irreducible over $\mathbb{F}_p$, then f irreducible over $\mathbb{Q}$.

Prop 3.3.12: (Eisenstein's Criterion)
If $\exists$ prime p s.t $p \nmid a_n$, $p \mid a_i \; \forall i \in \{0, \ldots, n-1\}$, and $p^2 \nmid a_0$, then f irreducible over $\mathbb{Q}$.

Lem 3.3.16: p prime and $0 < i < p$. Then $p \mid \binom{p}{i}$

Exm 3.3.17: p^{th} cyclotomic polynomial:

$$\Phi_p(t) = 1 + t + \ldots + t^{p-1} = \frac{t^p - 1}{t - 1}$$

is irreducible over $\mathbb{Q}$.

4.1 Dfn of Field Extensions

Dfn 4.1.1: $M:K$: M, K fields + homo $\iota: K \to M$

$K(t)$ = field of rational expressions over K

$K(t):K$

Dfn 4.1.10: $M:K$ and $Y \subseteq M$. $K(Y)$:= subfield of M generated by $K \cup Y$: "K with Y adjoined".

4.2 Algebraic and Transcendental Elements.

Dfn 4.2.1: $M:K$, $\alpha \in M$. α is called

- *algebraic*: if $\exists\, 0 \neq f \in K[t]$ s.t $f(\alpha) = 0$
- *transcendental* : otherwise.

$\bar{\mathbb{Q}} = \{$ algebraic numbers over $\mathbb{Q}\}$

Annihilating poly: of $\alpha \in M$ is an $f \in K[t]$ s.t $f(\alpha) = 0$.

Algebraic $\Leftrightarrow$ $\exists$ nonzero annihilating poly.

Dfn 4.2.6: $\alpha \in M$ algebraic over K. The minimal polynomial of α is the ! monic poly m satisfying

$\langle m \rangle = \{$ annihilating polys of $\alpha \}$

Lem 4.2.8: $M:K$, $\alpha \in M$ alg/K, $m \in K[t]$ monic.

- m is min. poly of α over K,

$\Leftrightarrow$ • $m(\alpha) = 0$ and $m \mid f$ $\forall$ ann. poly f of α

$\Leftrightarrow$ • $m(\alpha) = 0$, $\deg(m) \leq \deg(f)$ $\forall$

$\Leftrightarrow$ • $m(\alpha) = 0$ and m irreducible over K.

4.3 Simple Extensions

Dfn 4.3.1 A field extension is simple if $\exists\ \alpha \in M$ such that $M = K(\alpha)$.

Lem 4.3.4: m monic, irred. poly over K. Then $\left(K[t]/\langle m \rangle\right) : K$ is a simple extension generated by α, and the minimal poly of α over K is m.

Dfn 4.3.5: K a field, $\iota: K \to M$, $\iota': K \to M'$ extensions of K. $\varphi: M \to M'$ is a homomorphism over K if this commutes:

$$\begin{tikzcd} M \arrow[rr, "\varphi"] & & M' \\ & K \arrow[ul, "\iota"] \arrow[ur, "\iota'"'] & \end{tikzcd}$$

iso if φ invertible

Thm 4.3.7 (Classification of simple extensions)

(i) $m \in K[t]$ monic, irr. poly. Then $\exists$ $M:K$ and $\alpha \in M$ algebraic such that $M = K(\alpha)$ and α has min poly m over K.

↳ if (M, α), (M', α') are two such pairs, there is an isomorphism $\varphi: M \to M'$ over K s.t $\varphi(\alpha) = \alpha'$.

(ii) $\exists$ $M:K$ and a transcendental element $\alpha \in M$ such that $M = K(\alpha)$

↳ if (M, α), (M', α') are two such pairs, then $\exists$ an iso $\varphi: M \to M'$ over K such that $\varphi(\alpha) = \alpha'$.

5.1 Degrees of Extensions and Polynomials

Dfn 5.1.1: Degree $[M:K]$ = dimension of M as a vector space over K.

finite: $[M:K] < \infty$

Exm 5.1.3: $[M:K] \geq 1$
$[M:K] = 1 \Leftrightarrow M = K$
$[K(t):K] = \infty$

Thm 5.1.5: $K(\alpha):K$ a simple extension, with α algebraic over K. $m \in K[t]$ min. poly of α, $n = \deg(m)$. Then $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ is a basis of $K(\alpha)$ over K. So $[K(\alpha):K] = n$.

Cor 5.1.7: $M:K$, $\alpha \in M$. Then
$K(\alpha):K$ is finite $\Leftrightarrow$ α is algebraic over K.

$\deg_K(\alpha)$ $:= [K(\alpha):K]$.
α algebraic $\Leftrightarrow$ $\deg_K(\alpha) < \infty$

Cor 5.1.9:
(i) $M:L:K$, $\beta \in M$. $\Rightarrow$ $[L(\beta):L] \leq [K(\beta):K]$
(ii) $M:K$, $\alpha, \beta \in M \Rightarrow [K(\alpha,\beta):K(\alpha)] \leq [K(\beta):K]$.

Cor 5.1.11: $M:K$, $\alpha_1, \dots, \alpha_n \in M$, $\deg_K(\alpha_i) = d_i < \infty$.
$\forall\, \alpha \in K(\alpha_1, \dots, \alpha_m)$, can write α in terms of $\alpha_1, \dots, \alpha_n$:

$$\alpha = \sum_{r_1, \dots, r_n} c_{r_1 \dots r_n} \alpha_1^{r_1} \cdots \alpha_n^{r_n}$$

where r_i ranges over $0, \dots, d_i - 1$.

5.2. Tower Law

Thm 5.2.1 (Tower Law) $M:L:K$
① $(\alpha_i)_{i \in I}$ a basis of L over K and $(\beta_j)_{j \in J}$ a basis of M over L, then $(\alpha_i \beta_j)_{i \in I, j \in J}$ is a basis of M over K.
② $M:K$ is finite $\Leftrightarrow$ $M:L$ and $L:K$ are finite
③ $[M:K] = [M:L][L:K]$.

Cor 5.2.4: $M:L':L:K$. If $M:K$ is finite then $[L':L] \mid [M:K]$

Cor 5.2.6: $M:K$, $\alpha_1, \dots, \alpha_n \in M$. Then
$[K(\alpha_1, \dots, \alpha_n):K] \leq [K(\alpha_1):K] \cdots [K(\alpha_n):K]$.

5.3. Algebraic Extensions

Dfn 5.3.1: $M:K$ is "finitely generated" if $M = K(Y)$ for some finite subset $Y \subseteq M$.

Dfn 5.3.2: $M:K$ is "algebraic" if every element of M is algebraic over K.

Prop 5.3.4: $M:K$ is finite
$\Leftrightarrow$ $M:K$ is finitely generated and algebraic
$\Leftrightarrow$ $M = K(\alpha_1, \dots, \alpha_m)$ for some $\alpha_1, \dots, \alpha_n \in M$ algebraic over K.

Cor 5.3.6: $K(\alpha):K$ simple: $K(\alpha):K$ is finite
$\Leftrightarrow$ $K(\alpha):K$ is algebraic
$\Leftrightarrow$ α is algebraic over K.

Prop: $\overline{\mathbb{Q}}$ is a subfield of $\mathbb{C}$.

5.4 Ruler and Compass Constructions

A point C is ...

immediately constructible: from Σ if it is a point of intersection between two distinct lines or circles or both.

constructible: from Σ if there is a finite sequence $C_1, \dots, C_n = C$ of points such that C_i is immediately constructible from $\Sigma \cup \{C_1, \dots, C_{i-1}\}$ $\forall i$.

$K_\Sigma = \mathbb{Q}\left(\{\alpha \in \mathbb{R} : \alpha \text{ is a coordinate of a point in } \Sigma\}\right)$

Thm 5.4.2: $\Sigma \subseteq \mathbb{R}^2$ and $(x,y) \in \mathbb{R}^2$. If (x,y) is constructible from Σ, then there is an iterated quadratic extension of K_Σ containing x and y.

Cor 5.4.3: If (x,y) is constructible from Σ, then x and y are algebraic over K_Σ, and their degrees over K_Σ are powers of 2.

Lem 5.4.4: Let K be a subfield of $\mathbb{R}$ and $\alpha, \beta \in \mathbb{R}$. Suppose that α, β are each contained in some iterated quadratic extension of K. Then there is some iterated quadratic extension of K containing α and β.

Prop 5.4.6: θ not trisected by ruler and compass
Prop 5.4.7: cube not duplicated by ruler and compass
Prop 5.4.8: ○ not □ by ruler and compass

Reg. n-gon constructible $\Leftrightarrow$ $n = 2^r p_1 \dots p_k$ for p_i dist. Fermat primes

6.1 Extending Homomorphisms

Dfn: $\iota : K \to M$ and $\iota' : K' \to M'$ field extensions, Let $\psi : K \to K'$ be a field homo. We say a homomorphism $\varphi : M \to M'$ extends ψ iff $\varphi(a) = \psi(a) \quad \forall a \in K$.

Lem 6.1.2: $M : K$, $M' : K'$. Let $\psi : K \to K'$ be a homo, and φ extend ψ. Let $\alpha \in M$ and $f(t) \in K[t]$. Then

$$f(\alpha) = 0 \iff (\psi_* f)(\varphi(\alpha)) = 0$$

ψ injective/iso $\Rightarrow$ ψ_* injective / iso.

Lem: $M : K$, $M : K'$, $\varphi : M \to M'$ extends $\psi : K \to K'$. Let $\alpha \in M$ algebraic over K with min poly m. Then $\varphi(\alpha)$ algebraic over K' with min poly $\psi_*(m)$

Prop 6.1.5: $\psi : K \to K'$ iso, $K(\alpha) : K$ simple with min poly of α over K m, $K'(\alpha') : K'$ simple with min poly of α' over K' $\psi_*(m)$. Then $\exists !$ iso $\varphi : K(\alpha) \to K'(\alpha')$ extending ψ satisfying $\varphi(\alpha) = \alpha'$

6.2. ∃! Splitting Fields

Dfn 6.2.2: $f \in M[t]$. Then f splits in M if

$$f(t) = \beta(t - \alpha_1) \dots (t - \alpha_n)$$

for some $n \geq 0$ and $\beta, \alpha_1, \dots, \alpha_n \in M$.

Exm 6.2.3: (i) M algebraically closed if $\forall f \in M[t]$, f splits in M.

Dfn 6.2.4: $f \in K[t]$. A splitting field of f over K is an extension M of K such that

① f splits in M

② $M = K(\alpha_1, \dots, \alpha_n)$ where $\alpha_1, \dots, \alpha_n$ are the roots of f in M.

Lem 6.2.9: $f \in K[t]$. $\exists$ a splitting field M of f over K such that $[M : K] \leq \deg(f)!$

Prop 6.2.10: $\psi : K \to K'$ iso, $f \in K[t]$, M an s.f of f over K, and M' an s.f. of $\psi_*(f)$ over K'. Then:

① $\exists$ iso $\varphi : M : M'$ extending ψ

② there are at most $[M : K]$ such extensions φ.

Thm 6.2.12: $f \in K[t]$. Then

① $\exists$ a splitting field of f over K

② any two splitting fields of f are iso over K

③ when M is a splitting field of f over K, # of autos of M over K $\leq [M : K] \leq \deg(f)!$

Lem 6.2.13:

① $M : S : K$, $f \in K[t]$, $Y \subseteq M$. Let S be s.f of f over K. Then $S(Y)$ is the s.f of f over $K(Y)$

② $f \in K[t]$, L a subfield of $SF_K(f)$ containing K (i.e. $SF_K(f) : L : K$). Then $SF_K(f)$ is the s.f. of f over L.

6.3. The Galois Group

Dfn 6.3.1: $Gal(M : K) =$ group of automorphisms of M over K, with composition as the group operation.
↳ $\theta \in Gal(M : K)$ iff $\theta(a) = a \quad \forall a \in K$.

Dfn 6.3.5: $f \in K[t]$. $Gal_K(f) = Gal(SF_K(f) : f)$.

Thm 6.2.12 $\Rightarrow$ $|Gal_K(f)| \leq [SF_K(f) : K] \leq \deg(f)!$
↳ finite!

Rem $Gal_K(f)$ permutes the roots α_i of f

Lem 6.3.7: $f \in K[t]$. X be set of roots of f in $SF_K(f)$. Action of $Gal_K(f)$ on X defined by:

$$Gal_K(f) \times X \to X$$
$$(\theta, \alpha) \mapsto \theta(\alpha).$$

Dfn 6.3.9: $M : K$, $k \geq 0$, $(\alpha_1, \dots, \alpha_k), (\alpha_1', \dots, \alpha_k') \in M^k$. Then $(\alpha_1, \dots, \alpha_k)$, $(\alpha_1', \dots, \alpha_k')$ are conjugate over K if $\forall p \in K[t_1, \dots, t_k]$,

$$p(\alpha_1, \dots, \alpha_k) = 0 \iff p(\alpha_1', \dots, \alpha_k') = 0$$

Prop 6.3.10: $f \in K[t]$, with distinct roots $\alpha_1, \dots, \alpha_k$ in $SF_K(f)$. Def. group homo $\Gamma : Gal_K(f) \to S_k$ as $\theta \mapsto \sigma_\theta$, where $\theta(\alpha_i) = \alpha_{\sigma_\theta(i)}$. Then Γ is injective, and has image

$$\left\{ \sigma \in S_k : \begin{array}{l} (\alpha_1, \dots, \alpha_k) \text{ and } (\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(k)}) \\ \text{are conjugate over } K \end{array} \right\}$$

Cor 6.3.13: $L : K$, $f \in K[t]$. Then $Gal_L(f)$ embeds naturally as a subgroup of $Gal_K(f)$.

Cor 6.3.15: $f \in K[t]$, with k distinct roots in $SF_K(f)$. Then $|Gal_K(f)| \mid k!$

7.1 Normality

Dfn 7.1.1. Algebraic field extension $M:K$ is normal iff $\forall \alpha \in M$, the min. poly of α splits in M.

Lem 7.1.2: $M:K$ algebraic. $M:K$ is normal iff $\forall$ irreducible poly $f \in K[t]$, f splits in M, or f has no roots in M.

Thm 7.1.5: $M = SF_K(f)$ for some $f \in K[t]$ $\Leftrightarrow$ $M:K$ is finite and normal.

Cor 7.1.6: $M:L:K$. If $M:K$ is finite and normal, then so is $M:L$.

Prop 7.1.9: $M:K$ finite and normal, $\alpha, \alpha' \in M$.
Then α, α' are conjugate over K
$\Leftrightarrow$
$\alpha' = \varphi(\alpha)$ for some $\varphi \in Gal(M:K)$.

Cor 7.1.10: $f \in K[t]$ irreducible. Then the action of $Gal_K(f)$ on the roots of f in $SF_K(f)$ is *transitive*: $\forall \alpha, \alpha' \in SF_K(f)$, $\exists \varphi \in Gal_K(f)$ such that $\varphi(\alpha) = \alpha'$.

Thm 7.1.14: $M:L:K$, with $M:K$ finite, normal.
① $L:K$ is normal $\Leftrightarrow$ $\varphi L = L$ $\forall \varphi \in Gal(M:K)$
② $L:K$ normal $\Rightarrow$ $Gal(M:L)$ is a normal subgroup of $Gal(M:K)$ and

$$\frac{Gal(M:K)}{Gal(M:L)} \cong Gal(L:K)$$

7.2 Separability

Dfn 7.2.2: An irred. poly over a field is separable if it has no repeated roots in its splitting field.

Exm 7.2.4: irreducible polynomial that's inseparable: p prime, $K = \mathbb{F}_p(u)$ = field of rational expressions in u over $\mathbb{F}_p$, and let $f(t) = t^p - u$.
Let α be a root of f in $SF_K(f)$. Then

$$(t-\alpha)^p = \sum_{i=0}^{p} \binom{p}{i} t^i (-\alpha)^{p-i} = t^p - \alpha^p = f(t)$$

$\Rightarrow$ α is only root of f in $SF_K(f)$.

Dfn 7.2.7: Let K be a field and $f(t) = \sum_{i=0}^{n} a_i t^i$.
The formal derivative of f is

$$(Df)(t) = \sum_{i=0}^{n} i a_i t^{i-1} \in K[t]$$

Lem 7.2.8: $D(f+g) = Df + Dg$, $D(fg) = fDg + gDf$, $Da = 0$.

Lem 7.2.10: $0 \neq f \in K[t]$.
f has a repeated root in $SF_K(f)$;
$\Leftrightarrow$ f and Df have a common root in $SF_K(f)$;
$\Leftrightarrow$ f and Df have a nonconstant common factor in $K[t]$

Prop 7.2.11: $f \in K[t]$ irred. f is inseparable $\Leftrightarrow$ $Df = 0$

Cor 7.2.12:
- $\mathrm{char}\, K = 0$ $\Rightarrow$ every irred poly over K is sep.
- $\mathrm{char}\, K = p > 0$ $\Rightarrow$ irred poly $f \in K[t]$ is sep. iff $f(t) = b_0 + b_1 t^p + \dots b_r t^{rp}$.

Dfn 7.2.14: $M:K$ algebraic. $\alpha \in M$ is seperable if min poly m over K is sep. $M:K$ seperable $\Leftrightarrow$ $\forall \alpha \in M$ seperable.

For $M:L:K$:
Ex. 7.2.16 $M:K$ algebraic $\Rightarrow$ $M:L$, $L:K$ algebraic
Lem 7.2.17: $M:K$ separable $\Rightarrow$ $M:L$, $L:K$ separable

Thm 7.2.19: $|Gal(M:K)| = [M:K]$ $\forall$ finite, normal, separable extensions $M:K$.

7.3. Fixed Fields

Dfn 7.3.1: X, Y sets, $H \subseteq \{\text{functions } X \to Y\}$. Equalizer of H:

$$Eq(H) := \{ x \in X : f(x) = g(x)\ \forall f, g \in H \}$$

Lem 7.3.2: M, M' fields, $H \subseteq \{\text{Homo } M \to M'\}$. Then $Eq(H)$ is a subfield of M.

Dfn 7.3.3: M field, $H \subseteq Aut(M)$. Fixed field of H is

$$Fix(H) = \{ \alpha \in M : \varphi(\alpha) = \alpha\ \forall \varphi \in H \}$$

Lem 7.3.4: $Fix(H)$ is a subfield of M.

Thm 7.3.6: M field and $H \leq Aut(M)$ finite. Then $[M : Fix(H)] \leq |H|$.

Lem 7.3.10: M field, $H \leq Aut(M)$, $\varphi \in Aut(M)$.
Then $Fix(\varphi H \varphi^{-1}) = \varphi Fix(H)$.

Prop 7.3.11: $M:K$ field extension, H normal subgroup of $Gal(M:K)$. Think $Fix(H):K$ is normal.

8.1 Galois Correspondence

Intermediate field of $M:K$ = subfield of M containing K

$\mathscr{F} = \{$intermediate fields of $M:K\}$
$\mathscr{G} = \{$subgroups of $Gal(M:K)\}$

Gal(M:−) : $\mathscr{F} \to \mathscr{G}$
: $L \mapsto Gal(M:L)$

Fix : $\mathscr{G} \to \mathscr{F}$
: $H \mapsto Fix(H)$

Lem 8.1.2 :

1. $L_1, L_2 \in \mathscr{F}$, $L_1 \subseteq L_2 \Rightarrow Gal(M:L_1) \supseteq Gal(M:L_2)$
   $H_1, H_2 \in \mathscr{G}$, $H_1 \subseteq H_2 \Rightarrow Fix(H_1) \supseteq Fix(H_2)$
2. $L \in \mathscr{F}$, $H \in \mathscr{G}$,
   $L \subseteq Fix(H) \iff H \subseteq Gal(M:L)$
3. $\forall L \in \mathscr{F}$, $L \subseteq Fix(Gal(M:L))$
   $\forall H \in \mathscr{G}$, $H \subseteq Gal(M:Fix(H))$.

Galois correspondence : $\mathscr{F} \underset{Fix}{\overset{Gal(M,-)}{\rightleftarrows}} \mathscr{G}$

8.2: The Theorem

Thm 8.2.1 : (Fundamental Theorem of Galois Theory)

$M:K$ a finite, normal, separable extension.

1. The functions $\mathscr{F} \underset{Fix}{\overset{Gal(M,-)}{\rightleftarrows}} \mathscr{G}$ are **mutually inverse :**
   $L = Fix(Gal(M:L))$ and $H = Gal(M:Fix(H))$.

2. $|Gal(M:L)| = [M:L]$ $\forall L \in \mathscr{F}$, and
   $[M:Fix(H)] = |H|$ $\forall H \in \mathscr{G}$.

3. Let $L \in \mathscr{F}$. Then
   L is a normal extension of K
   $\iff Gal(M:L)$ is a normal subgroup of $Gal(M:K)$.
   and in that case,
   $$\frac{Gal(M:K)}{Gal(M:L)} \cong Gal(L:K)$$

Cor 8.2.6 : $M:K$ finite, normal, separable.
Then $\forall \alpha \in M \setminus K$, $\exists \varphi \in Aut(M)$ over K
such that $\varphi(\alpha) \neq \alpha$.

9.1 Radicals

Dfn 9.1.2: Let $\mathbb{Q}^{rad}$ be the smallest subfield of $\mathbb{C}$ s.t $\forall \alpha \in \mathbb{C}$, $\alpha^n \in \mathbb{Q}^{rad}, n \geq 1 \Rightarrow \alpha \in \mathbb{Q}^{rad}$. α "radical" if $\alpha \in \mathbb{Q}^{rad}$.

Dfn 9.1.5: poly over $\mathbb{Q}$ is "solvable by radicals if all it's complex roots are radical.

Lem 9.1.6: $n \geq 1$, $Gal_{\mathbb{Q}}(t^n - 1)$ is abelian

Lem 9.1.8: K a field, $n \geq 1$. Suppose $t^n - 1$ splits in K. Then $Gal_K(t^n - a)$ is abelian $\forall a \in K$

9.2. Solvability by Radicals

Dfn 9.2.1: $M:K$ finite, normal, separable. Then $M:K$ is solvable if $\exists\ r \geq 0$ and intermediate fields

$$K = L_0 \subseteq L_1 \subseteq \dots \subseteq L_r = M$$

s.t. $L_i : L_{i-1}$ is normal and $Gal(L_i : L_{i-1})$ is abelian.

Ex. 9.2.2: $N:M:K$ finite, normal, separable. If $N:M$ and $M:K$ are solvable, then so is $N:K$.

Ex 9.2.3: $SF_{\mathbb{Q}}(t^n - a):\mathbb{Q}$ is solvable

Lem 9.2.4: $M:K$ finite, normal, separable.

$$M:K \text{ is solvable} \iff Gal(M:K) \text{ is solvable.}$$

Lem 9.2.6: L, M subfields of $\mathbb{C}$ s.t $L:\mathbb{Q}$ and $M:\mathbb{Q}$ are finite, normal and solvable. Then $\exists$ subfield N of $\mathbb{C}$ s.t $L \cup M \subseteq N$ and $N:\mathbb{Q}$ is finite, normal and solvable.

$$\mathbb{Q}^{sol} := \left\{ \begin{array}{l} \alpha \in \mathbb{C} : \alpha \in L \text{ for some subfield } L \subseteq \mathbb{C} \\ \text{that is finite, normal and solvable over } \mathbb{Q} \end{array} \right\}$$

Prop 9.2.10: $\mathbb{Q}^{rad} \subseteq \mathbb{Q}^{sol}$

Thm 9.2.11: $f \in \mathbb{Q}[t]$. If f is solvable by radicals, then $Gal_{\mathbb{Q}}(f)$ is solvable

9.3 An unsolvable polynomial

Lem 9.3.1: f irred. poly. over K, with $SF_K(f):K$ separable. Then $\deg(f) \mid |Gal_K(f)|$

Lem 9.3.3: p prime, $f \in \mathbb{Q}[t]$ irred., $\deg(f) = p$, exactly $p-2$ real roots. Then $Gal_{\mathbb{Q}}(f) \cong S_p$

Thm 9.3.5: Not every polynomial over $\mathbb{Q}$ of degree 5 is solvable by radicals

e.g. $f(t) = t^5 - 6t + 3$.

10.1 p^{th} Roots in Characteristic p

Prop 10.1.1: p prime, R a ring with $\mathrm{Char}(R) = p$.
① $\theta: R \to R$, $r \mapsto r^p$ is homo — "Frobenius automorphism"
② R field $\Rightarrow$ θ injective
③ R finite $\Rightarrow$ θ automorphism

Rem: Char $= p \Rightarrow (r+s)^p = r^p + s^p$

Cor 10.1.4: p prime
① Field char p, every element has at most one p^{th} root
② finite field char p, every element has exactly one p^{th} root.

10.2 Classification of finite fields

Order of a finite field M = cardinality of M = $|M|$

WARNING: order $\neq$ degree of a field!

see 2.2.5, 2.2.10, 2.2.11.

Lem 10.2.2: Let M be a finite field. Then char $M = p$, and $|M| = p^n$ where $n = [M : \mathbb{F}_p] \geqslant 1$.

Lem 10.2.4: p prime, $n \geqslant 1$. Then the splitting field of $t^{p^n} - t$ over $\mathbb{F}_p$ has order p^n.

Lem 10.2.5: $|M| = q$, then $\alpha^q = \alpha \;\; \forall \alpha \in M$

Lem 10.2.7: $|M| = q$, then M is a splitting field of $t^q - t$ over $\mathbb{F}_p$.

Thm 10.2.8: (Classification of Finite Fields)

① Every finite field has order p^n for some prime p and $n \geqslant 1$.
② $\forall$ prime p and $n \geqslant 1$, $\exists!$ field of order p^n (up to iso). Has char $= p$ and is a splitting field for $t^{p^n} - t$ over $\mathbb{F}_p$.

10.3 Multiplicative Structure

Prop 10.3.1: Field K: every finite subgroup of $K^\times$ is cyclic. ($\Rightarrow$) K finite $\Rightarrow K^\times$ cyclic.

Cor 10.3.5: Every extension of one finite field over another is simple.

Cor 10.3.8: prime p, $n \geqslant 1$. $\exists$ an irred. poly over $\mathbb{F}_p$ of degree n.

10.4 Galois Groups for finite fields

Lem 10.4.2: $M : K$ field extension
① K finite $\Rightarrow$ $M : K$ separable
② M finite $\Rightarrow$ $M : K$ finite, normal.

Prop 10.4.3: p prime, $n \geqslant 1$. $\mathrm{Gal}(\mathbb{F}_{p^n} : \mathbb{F}_p)$ is cyclic and of order n, generated by the Frobenius auto of $\mathbb{F}_{p^n}$.

Prop 10.4.6: p prime, $n \geqslant 1$. $\mathbb{F}_{p^n}$ has exactly one subfield of order p^m for each divisor m of n, and no others: $= \{ \alpha \in \mathbb{F}_{p^n} : \alpha^{p^m} = \alpha \}$

$\mathrm{Gal}(\mathbb{F}_{p^n} : \mathbb{F}_p) = \langle \theta \rangle \cong C_n$
$\mathrm{Fix}\langle \theta \rangle = \mathbb{F}_p$

When $k \mid n$, $!$ subgroup of order k is $\langle \theta^{n/k} \rangle$.
$\mathrm{Fix}\langle \theta^{n/k} \rangle = \{ \alpha \in \mathbb{F}_{p^n} : \alpha^{p^{n/k}} = \alpha \}$

$\mathrm{Gal}(\mathbb{F}_{p^n} : \mathbb{F}_{p^m}) \cong C_{n/m}$