$a|b \Rightarrow b=ma$. a divides b

Ring - $\forall a,b,c \in R$, $(R,+)$ an abelian group, $(ab)c=a(bc)$, $a(b+c)=ab+ac$ and $(b+c)a=ba+ca$

↳ $a0=0a=0$, $a(-b)=(-a)b=-(ab)$, $(-a)(-b)=ab$, $a(b-c)=ab-ac$, $(b-c)a=ba-ca$.

Ring with unity - $\exists 1 \in R \ \forall a$ $a1=1a=a$, $(-1)a=-a$, $(-1)(-1)=1$, 1 is unique. If 1 has infinite order (under +), then $\mathrm{Char}R=0$. If 1 has order n, then $\mathrm{Char}R=n$.

Commutative ring - $\forall a,b \in R$ $ab=ba$, $b|a \Leftrightarrow b \neq 0, \exists c \in R: a=bc$.

Commutative ring with unity - $a \in R$ a unit if $\exists a^{-1} \in R$ s.t. $aa^{-1}=a^{-1}a=1$, $U(R)$ = set of units of R.

a^{-1} is unique for each a. - $\langle a \rangle \trianglelefteq R$ (is an ideal), $U(R)$ is a group wrt multiplication.

Integral domain - Commutative ring w/ unity and without **Zero-divisors** - zero divisor of $a \neq 0 \in R$ is $b \neq 0 \in R$ s.t. $ab=0$.

↳ $ab=0 \Rightarrow a=0 \vee b=0$, $ab=ac \Rightarrow b=c$, $\mathrm{Char}R=0$ or a prime.

Field - An integral domain where $F \setminus \{0\} = U(F)$, $U(F)$ is abelian group under multiplication. A finite integral domain always a field. → Finite fields have $\mathrm{Char}F \neq 0$. → only ideals of F are $\{0\}$ and F.

Subring - $S \subseteq R$ a subring if $\forall a,b \in S$: $a-b \in S$, $ab \in S$, $\{0\}$ is trivial subring.

Subfield - Subring of a field which is itself a field.

Ideal - A subring of R, $\forall r \in R \ \forall a \in A$ $ar \in A \wedge ra \in A$. To check if any $A \subseteq R$ is an ideal use ideal test 1) $a,b \in A \Rightarrow a-b \in A$.

2) $a \in A, r \in R \Rightarrow ar \in A, ra \in A$. $\{0\}, R$ both ideals of R. $\langle a_1,\dots,a_n \rangle = \{r_1a_1+\dots+r_na_n \mid r_1,\dots,r_n \in R\}$ = ideal generated by $a_1,\dots,a_n$.

Principal Ideal - $\langle a \rangle = \{ra \mid r \in R\}$, R commutative, $I \trianglelefteq R$, I principle if $\exists a \in R: I=\langle a \rangle$, **PID** - D integral domain, every $I \trianglelefteq D$ is principal. ↳ Every field is a PID

↳ if $x \in U(R) \cap I \Rightarrow I=R$.

Factor Rings - R ring, $A \trianglelefteq R$. Then $R/A = \{r+A \mid r \in R\}$ is a ring w/ $(s+A)+(t+A)=(s+t)+A$, $(s+A)(t+A)=st+A$.

Characteristic of a ring - $\mathrm{Char}R$ = least positive integer n s.t. $nx=\sum_{i=1}^{n} x=0 \ \forall x \in R$. If no n exists, then $\mathrm{Char}R=0$

↳ Finite ring always has $\mathrm{Char}R \neq 0$. $\mathrm{char}R$ = additive order of 1_R, if $\exists 1_R$.

$\Rightarrow R/A$ integral domain $\Leftrightarrow A$ is prime.

R a commutative ring w/ unity, $A \trianglelefteq R \Rightarrow R/A$ a field $\Leftrightarrow A$ is maximal.

↳ maximal $\Rightarrow$ prime, R/I is a field $\Rightarrow I$ is max and prime.

R a ring, $|R|$ prime $\Rightarrow$ R a field. Since $R/\{0\} \cong R$ and $\{0\}$ maximal in R, since only $\{0\}, R$ subgroup of R, since only $0 \mid |R| \wedge |R| \mid |R|$.

Ring Homomorphism - Map from R to S s.t. $\forall a,b \in R$, $\varphi(a+b)=\varphi(a)+\varphi(b)$, $\varphi(ab)=\varphi(a)\varphi(b)$.

↳ bijective ring homomorphism = **Isomorphism**. $\varphi: R \to R \wedge \varphi$ isomorphic $\Rightarrow \varphi$ **automorphic**. $\mathrm{Im}(\varphi) = \{\varphi(r): r \in R\}$

↳ φ $R \to S$ homomorphism, $A \subseteq R$ subring, $B \trianglelefteq S$. $\varphi(A) \to \{\varphi(a): a \in A\}$, $\varphi^{-1}(B) = \{r \in R \mid \varphi(r) \in B\}$, $\mathrm{Ker}(\varphi) = \{r \in R \mid \varphi(r)=0 \in S\}$

↳ $\forall r \in R, n \in \mathbb{N}$: $n\varphi(r)=\varphi(nr)$, $\varphi(r^n)=(\varphi(r))^n$, $\varphi(A)$ subring of S, $A \trianglelefteq R$, φ onto $\Rightarrow \varphi(A) \trianglelefteq S$, $\varphi^{-1}(B) \trianglelefteq R$, R commutative $\Rightarrow \varphi(R)$ commutative in S.

↳ $\exists 1_R, S \neq \{0\}$, φ onto $\Rightarrow \varphi(1_R)=1_S$, φ isomorphism $\Leftrightarrow \mathrm{Ker}\varphi=\{0\}$, φ onto. $\mathrm{Ker}(\varphi) \trianglelefteq R$. $\to R/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi)$ [1st Isomorphism thm]

[Kernels are ideals and ideals are kernels]

↳ $\varphi: R \to R/I$, $I \trianglelefteq R \Rightarrow \mathrm{Ker}\varphi = I$, $\exists 1_R$ $\varphi: \mathbb{Z} \to R$ $\varphi(n)=\sum_{i=1}^{n} 1_R$, φ ring homomorphism, so $\exists S \subseteq R$: $S \cong \mathbb{Z}_{\mathrm{Char}R}$ or $S \cong \mathbb{Z}$ if $\mathrm{Char}R=0$.

F is **Field of Quotients** of D (integral domain) contains subring $S \cong D$. $S=\{(a,b) \mid a,b \in D, b \neq 0\}$ $(a,b) \sim (c,d) \Leftrightarrow ad-bc=0$ $F=S/\sim$

$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$, $\frac{a}{b} \cdot \frac{c}{d}=\frac{ac}{bd}$

$\mathrm{Aut}(R)=\{\phi: \phi$ an automorphism of $R\}$ is a group, w/ operation as map composition.

Every ring homomorphism $\varphi: \mathbb{Z}_n \to \mathbb{Z}_n$ has form $\varphi(x)=ax$, $a \in \mathbb{Z}_n$ and $a^2=a$ (idempotent).

RINGS

Name	Cardinality	Unity	Units	Commutative	Integral domain	PID	Char	Subrings, Ideals (A)	(principal, maximal, prime, field) (B) (C) (D) (E)
$\mathbb{Z}$	∞	1	$\{1,-1\}$	Yes	Yes	Yes	0	$n\mathbb{Z}$, $n\in\mathbb{Z}$	(D)∧(C) $\Leftrightarrow$ n prime ; (A),(B)
$\mathbb{Z}_n$	n	1	$k: \gcd(k,n)=1$	Yes	Yes	Yes	n	$\mathbb{Z}_k$ $k\mid n$	(C) $\Leftrightarrow$ n prime
R a ring	R[x]	∞	1		iff R is ID	iff R a field			

$\mathbb{Q}[x]$, $\mathbb{C}[x]$, $\mathbb{Z}[x]$ → PID.

PATHOLOGICAL RINGS

- Commutative ring w/ a maximal ideal not prime ideal. $4\mathbb{Z} \lhd 2\mathbb{Z}$, but $4\mathbb{Z}$ maximal but not prime.
- Commutative ring w/o unity $2\mathbb{Z}$ (So has no zero-divisors but not an integral domain)
- Ring w/ unity, not commutative $\mathbb{M}_{2\times 2}(\mathbb{Z})$
- finite, noncommutative ring $\mathbb{M}_{2\times 2}(\mathbb{Z}_6)$
- Non commutative ring w/o unity $\mathbb{M}_{2\times 2}(2\mathbb{Z})$
- $\mathbb{Z}_n[x]$ infinitely large but Char $\neq 0$.
- $S=\{2n \mid n\in\mathbb{Z}_3\}$, $\mathbb{M}_{2\times 2}(S)$ finite, non commutative and without unity.
- ring $=\left\{\begin{pmatrix} a & b \\ c & d\end{pmatrix} a,b,c,d\in R\right\}$ identity is $\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $\leftarrow$ non commutative but subring $\left\{\begin{pmatrix} a & a \\ a & a\end{pmatrix} a\in R\right\}$ has identity $\begin{pmatrix}\frac{1}{2}&\frac{1}{2}\\\frac{1}{2}&\frac{1}{2}\end{pmatrix}$ and is commutative.
- $\mathbb{Z}\oplus 2\mathbb{Z}$ has no unity, but subring $\{(x,0): x\in\mathbb{Z}\}$ has unity $(1,0)$.
- finite commutative ring w/o unity $\langle 2\rangle \subset \mathbb{Z}_4$
- $\mathbb{Z}$ is an integral domain that is not a field, since $2\notin U(\mathbb{Z})$.

$f \in R[x]$, $f = a_n x^n + \cdots + a_1 x + a_0$, $a_n \neq 0 \Rightarrow \deg f = n$, leading coefficient of $f = a_n$, constant term $= a_0$, $\exists 1_R$ and $a_n = 1_R$, f monic

$f = a_0 \Rightarrow f$ is constant ($\deg f = 0$ if $f \neq 0$, u.d. o.w.). $R \subseteq R[x]$.

F field, $f, g \in F[x]$, $g \neq 0 \Rightarrow \exists! q, r \in F[x]$ s.t. $f = g \cdot q + r$, $r = 0 \vee \deg r < \deg g$.

Factors D int. domain, $f, g \in D[x]$, $g \neq 0$, $g \mid f \Leftrightarrow \exists h \in D[x] : f = gh$

Roots $a \in R$ root of $f(x) \in R[x] \Leftrightarrow f(a) = 0$. R field $(x-a)^k \mid f \wedge (x-a)^{k+1} \nmid f \Leftrightarrow$ root a has multiplicity $k \geq 1$.

↳ F field, $f(x) \in F[x]$, $a \in F$. $(x-a) \overline{)f(x)}$; remainder $= f(a) \rightarrow a$ root of $f(x) \Leftrightarrow (x-a) \mid f(x) \rightarrow n = \deg f \Rightarrow \#$ roots of $f \leq n$.

→ $f, g \in F[x]$ and $f(a) = g(a)$ $\forall a \in F$ but $f(x) \neq g(x)$ can only happen in finite field w/ $|F| < \deg f, g$

Factorization D int. domain, $f(x) \in D[x]$, $f(x) \neq 0$ not a unit. irreducible if $f(x) = g(x)h(x) \Rightarrow g(x)$ or $h(x)$ unit in $D[x]$.

Inverses for polynomials only exist in rings w/ zero-divisors.

Irreducibility tests → F Field $f(x) \in F[x]$, $\deg f(x) = 2$ or 3, f irreducible over $F \Leftrightarrow f(x)$ has no zeros in F.

→ $f(x) \in \mathbb{Z}[x]$ f reducible over $\mathbb{Q} \Leftrightarrow f$ reducible over $\mathbb{Z}$.

→ p prime, $f \in \mathbb{Z}_p[x]$, $\deg f \geq 1$. $\hat{f}(x) = f(x) \pmod p$, if $\deg \hat{f}(x) = \deg f(x)$, $\hat{f}(x)$ irreducible in $\mathbb{Z}_p \Rightarrow f(x)$ irreducible over $\mathbb{Q}$.

Eisenstein criteria – $f(x) \in \mathbb{Z}[x]$, $\deg f = n$, if $\exists p$ prime s.t. $p \nmid a_n$, $p \mid a_i$, $i = 0, 1, \ldots, n-1$, $p^2 \nmid a_0 \Rightarrow f(x)$ irreducible over $\mathbb{Q}$.

↳ apply to $\hat{f}(x) = x^{\deg f} \cdot f(\frac{1}{x}) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$ (reciprocal of f), or to $f(x+n)$, $n \in \mathbb{Z}$.

$p(x)$ irreducible over $F \Leftrightarrow \langle p(x) \rangle$ maximal ideal of F.

Unique Factorization – $F[x]$, F a field or $\mathbb{Z}$, $f(x) \in F[x]$, $\forall f(x) \in F[x]$, $f(x) \neq 0 \Rightarrow f(x) = b_1 \cdots b_s p_1(x) \cdots p_m(x)$, $\deg b_i = 0$, p_j irreducible and b_i, p_j unique, (any other representation differs only by $\pm$ unity)

Extension Fields E extension of $F \Rightarrow$ 1) $F \subseteq E$, 2) Operations on F are operations on E restricted to F.

use unique factorization on $f(x)$ to get $p(x)$

Fund. Thm. of Field Thy – F field, $f(x) \in F[x]$, $f(x)$ not constant, $\exists$ extension E of F s.t. $f(x)$ has a zero in E. ↳ $f(x)$ can be factored into linear polynomials only in $E[x]$.

the $E = F[x]/\langle p(x) \rangle$, $F = \{f + \langle p(x) \rangle, f \in F\} \subseteq E$.

root of $f(x)$ is $x + \langle p(x) \rangle = y$ ($p(y) = 0 \Rightarrow f(y) = 0$)

Splitting field – E extension of F, $f(x) \in F[x]$. $f(x)$ splits in E, but not any proper subfield of E.

↳ E extension of F, $a_1, \ldots, a_n \in E \Rightarrow F(a_1, \ldots, a_n)$ is minimal subfield of E containing F and $a_1, a_2, \ldots, a_n$.

$F(a) \cong F[x]/\langle p(x) \rangle$ F field, $p(x)$ irreducible over F and $p(a) = 0$ in some extension E. any $y \in F(a)$, $y = c_{n-1} a^{n-1} + \cdots + c_1 a + c_0$, $c_i \in F$, $\deg p(x) = n$. Use $\phi : F[x] \to F(a)$, $\phi(f(x)) = f(a)$, $\ker \phi = \langle p(x) \rangle$

Algebraic Extensions $a \in E$, extension of F. a algebraic over $F \Leftrightarrow \exists p \in F[x], p(a) = 0 \wedge p(x) \neq 0$. Not algebraic $\Leftrightarrow$ transcendental.

a transcendental $\Rightarrow F(a) \cong F(x)$ $\quad F(x) = \{f(x)/g(x) \mid f, g \in F[x], g \neq 0\}$

Algebraic Extension – every $a \in E$ algebraic over F. a algebraic $\Rightarrow F(a) \cong F[x]/\langle p(x) \rangle$, E field extension of F, $a \in E$.

Minimal polynomial – of algebraic a over field F is unique monic irreducible $p(x) \in F[x] : p(a) = 0$. (E has dimension) $\quad [\{1, x, \ldots, x^{n-1}\}$ a basis for $F(a)$ over $F]$.

Finite Extension – E extension of F, $[E:F] < \infty$. $F(a)$ finite extension of F and $\dim F(a) = \deg p(x)$, $y \in F(a) \Rightarrow y = c_0 1 + \cdots + c_{n-1} x^{n-1}$ ($c_i \in F$).

Finite Extension of $E \Rightarrow E$ Algebraic over F. K finite extension of E, E finite extension of $F \Rightarrow K$ finite extension of F $\wedge [K:F] = [K:E][E:F]$.

Steintz thm – F field $\wedge$ $\mathrm{Char} F = 0$, a, b algebraic over $F \Rightarrow \exists c \in F(a,b) : F(a,b) = F(c)$.

↳ chose $d \in F$ s.t. $\forall i \geq 1, j \geq 1$ $d \neq (a_i - a)(b - b_j)^{-1}$, a_i roots of min poly of a, $i \in \{1, 2, \ldots\}$; b_j roots of min poly of b, $j \in \{1, 2, \ldots\}$

↳ $c = a + bd$

Galois Groups - E extension of F, $Gal(E/F)$ is subgroup of $Aut(E)$ that fixes F. $\{\varphi \in Aut(E) \mid \varphi(x)=x, \forall x \in F\}$

- Fixed field of $H \leq Gal(E/F)$, $E_H = \{x \in E \mid \varphi(x)=x \ \forall \varphi \in H\}$

- Galois thm - F field, $\text{char}F=0$ or a finite field. E splitting field of polynomial $p(x) \in F[x] \Rightarrow K \to Gal(E/K) \leq Gal(E/F)$ for $F \leq K \leq E$ is a 1:1 correspondence. 1) $[E:K] = |Gal(E/K)|$, $[K:F] = |Gal(E/F) : Gal(E/K)| = |Gal(E/F)| / |Gal(E/K)|$

2) K splitting field, $p \in F[x]$, $Gal(E/K) \trianglelefteq Gal(E/F)$, $Gal(K/F) \cong Gal(E/F) / Gal(E/K)$ 3) $K = E_{Gal(E/K)}$

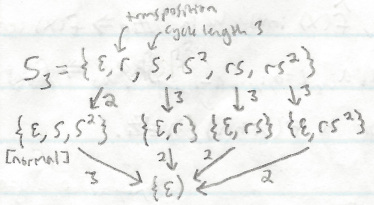
4) $H \leq Gal(E/F) \Rightarrow H = Gal(E/E_H)$

Solvability by Radicals let F field, $f(x) \in F[x]$. $f(x)=0$ solvable by radicals (over F) if $f(x)$ splits into linear factors in some $F(a_1, \dots, a_n)$ extension of F, s.t. $\exists k_1, \dots, k_n \in \mathbb{Z}^+ : a_1^{k_1} \in F$, $a_i^{k_i} \in F(a_1, \dots, a_{k_{i-1}})$ for $i = 2, \dots, n$.

Solvable group - A group G is solvable if G has series of subgroups $\{\varepsilon\} = H_0 \subset H_1 \subset \cdots \subset H_n = G$, for each $0 \leq i < n$ H_{i+1}/H_i abelian. $H_i \trianglelefteq H_{i+1}$ and

$x^n - a$ - F field, $\text{char}F=0$, $a \in F$. If E splitting field of $x^n - a$ (over F), then $Gal(E/F)$ solvable.

$N \trianglelefteq G$, G/N solvable $\Rightarrow G$ solvable.



$\{\varepsilon\} \trianglelefteq \{\varepsilon, s, s^2\} \trianglelefteq S_3$

$D_8 = \{\varepsilon, s, s^2, s^3, r, sr, s^2r, s^3r\}$

subgroups $= \{\varepsilon\}, \{\varepsilon, s^2\}, \{\varepsilon, r\}, \{\varepsilon, s^2r\}, \{\varepsilon, s^3r\}, \{\varepsilon, sr\}, \{\varepsilon, r, s^2, s^2r\}, \{\varepsilon, sr, s^2, s^3r\}, \{e, s, s^2, s^3\}, D_8$.

$\{\varepsilon\} \trianglelefteq \{\varepsilon, s^2\} \trianglelefteq \{\varepsilon, s, s^2, s^3\} \trianglelefteq D_8$

→ for any extension E of $\mathbb{Q}$, $[E:\mathbb{Q}] = |Gal(E/\mathbb{Q})|$, $\mathbb{Q} < E < L$, by Lagrange thm, $[L:\mathbb{Q}] = |Gal(L/\mathbb{Q})| = |Gal(E/\mathbb{Q})| \cdot [Gal(L/\mathbb{Q}) : Gal(E/\mathbb{Q})] \Rightarrow [E:\mathbb{Q}] = |Gal(L/\mathbb{Q})| / |Gal(E/\mathbb{Q})|$

→ any intermediate subfield E is a splitting field of $Gal(L/E)$ normal.

S_4 has $\{e\} \trianglelefteq \{e, (12)(34), (13)(24), (14)(23)\} \trianglelefteq A_4 \trianglelefteq S_4$. ($\trianglelefteq$ abelian)

$[E:F] = Gal(E/F)$

① 1) Find roots 2) And splitting field 3) Compute degree of splitting field 4) find basis for $[E:F]$ 5) Find $g \in Gal(E/F)$ $\Leftrightarrow$ g permutes roots and $g(p(x)) = 0$.

② - Not solvable by radicals: (1) Check $f(x)$ irreducible (2) Check deg $f(x) = p$ prime (3) $f(x)$ has exactly $p-2$ real roots, (and 2 complex conjugate roots).

→ Rolles thm → if derivative has k roots, function cannot have more than $k+1$ roots.

Irreducibility → F field, $f(x)\in F[x]$ & $\deg f(x)=2$ or 3; f no zeros in F $\Leftrightarrow$ f irreducible over F.

- $f(x)\in\mathbb{Z}[x]$ f reducible over $\mathbb{Q}\Leftrightarrow$ f reducible over $\mathbb{Z}_p$, p prime, $f\in\mathbb{Z}_p[x]$, $\deg f\geq 1$, $\hat{f}(x)=f(x) \pmod p$ if $\deg\hat{f}=\deg f$, $\hat{f}$ irreducible in $\mathbb{Z}_p\Rightarrow$ f irreducible in $\mathbb{Z}$.

Eisenstein Criteria - $f(x)\in\mathbb{Z}[x]$, $\deg f=n$, $\exists p$ s.t. $p\nmid a_n$, $p\mid a_i$, $i=0,\dots,n-1$, $p^2\nmid a_0\Rightarrow f(x)$ irreducible over $\mathbb{Q}$.
↳ apply to $\tilde{f}(x)=x^{\deg f}\cdot f(1/x)=a_0x^n+\dots+a_{n-1}x+a_n$ or to $f(x+n)$, $n\in\mathbb{Z}$.

Steinitz thm F field, $\mathrm{char}F=0$, a,b algebraic over F $\Rightarrow\exists c\in F(a,b)$ s.t. $F(a,b)=F(c)$.
↳ chose $d\in F$ s.t. $\forall i\geq 1, j\geq 1$ $d\neq(a_i-a)(b-b_j)^{-1}$, a_i roots of min poly of a, b_j roots of min poly of b.
$c=a+b\cdot d$

Galois Groups E extension of $\mathbb{Q}$, $\mathrm{Gal}(E/\mathbb{Q})=\{\varphi\in\mathrm{Aut}(E):\varphi(x)=x\ \forall x\in\mathbb{Q}\}<\mathrm{Aut}(E)$ [All automorphisms of E fixing F]

Fixed field of $H\leq\mathrm{Gal}(E/\mathbb{Q})$ is $E_H=\{x\in E\mid\varphi(x)=x\ \forall\varphi\in H\}$

Galois thm E splitting field of $p(x)\in\mathbb{Q}[x]$, $\mathbb{Q}\leq K\leq E$, $K\leftrightarrow\mathrm{Gal}(E/K)\leq\mathrm{Gal}(E/\mathbb{Q})$
1) $[E:K]=|\mathrm{Gal}(E/K)|$, $[K:\mathbb{Q}]=[\mathrm{Gal}(E/\mathbb{Q}):\mathrm{Gal}(E/K)]=|\mathrm{Gal}(E/\mathbb{Q})|/|\mathrm{Gal}(E/K)|$
2) K splitting field, $p\in\mathbb{Q}[x]$, $\mathrm{Gal}(E/K)\trianglelefteq\mathrm{Gal}(E/\mathbb{Q})$, $\mathrm{Gal}(K/\mathbb{Q})\cong\mathrm{Gal}(E/\mathbb{Q})/\mathrm{Gal}(E/K)$ 3) $K=E_{\mathrm{Gal}(E/K)}$
4) $H\leq\mathrm{Gal}(E/\mathbb{Q})\Rightarrow H=\mathrm{Gal}(E/E_H)$

To find Galois Group 1) Find roots of p(x) 2) find splitting field E 3) Compute degree of splitting field $[E:\mathbb{Q}]=|\mathrm{Gal}(E/\mathbb{Q})|$
4) find basis for E as vector space over $\mathbb{Q}$ w/ degree $[E:\mathbb{Q}]$. 5) find $g\in\mathrm{Gal}(E/\mathbb{Q})$ (g permutes roots and $g(p(x))=0$)
6) determine $\mathrm{Gal}(E/\mathbb{Q})\cong$? 7) for each $H<\mathrm{Gal}(E/\mathbb{Q})$, compute fixed field of H (L_H), note: $[L_H:\mathbb{Q}]=\frac{|\mathrm{Gal}(E/\mathbb{Q})|}{|H|}$
8) Show $\mathrm{Gal}(E/\mathbb{Q})$ solvable, that means find $\{e\}\subset H_1\subset\dots\subset H_n\subset G$ s.t. $H_i\trianglelefteq H_{i+1}$, H_{i+1}/H_i abelian,
↳ If $\mathrm{Gal}(E/\mathbb{Q})$ finite and commutative $\Rightarrow$ Solvable.
Note: Normal subgroup corresponds to a polynomial extension. Normal - $\forall g\in G$ $gH=Hg$ or $gHg^{-1}\subseteq H$, G cyclic $\Rightarrow$ G commutative $\Rightarrow$ all subgroups normal $\Rightarrow$ G solvable
$[G:H]=2\Rightarrow$ H normal in G.

roots x^n-a has roots $\{\omega^k\sqrt[n]{a}\}_{k=0}^{n}$, $\omega=e^{i2\pi k/n}$, min poly of ω is $x^{n-1}+\dots+x+1=\frac{1-x^n}{1-x}$

to get degree $\dim\mathbb{Q}(a)=\deg p(x)$, p(x) min poly of a [i.e. p(x) monic, irreducible over $\mathbb{Q}$ and $p(a)=0$]
$[E:\mathbb{Q}]=[E:K][K:\mathbb{Q}]$ (E extension of K, K extension of $\mathbb{Q}$)

finding $g\in\mathrm{Gal}(E/\mathbb{Q})$ g completely determined by action on a,b [$E=\mathbb{Q}(a,b)$], $g(p(x))=0$, $g(x^n-1)=g(x)^n-1=0$ ← to get $\omega\to$?

$\mathrm{Gal}(E/\mathbb{Q})\cong$??? Check Cayley table or compute cycles of elements, to get orders.

Galois Correspondence Subfields of degree K ($K<E$) $\leftrightarrow$ Subgroups of order $=\frac{|\mathrm{Gal}(E/\mathbb{Q})|}{K}$ ($\mathrm{Gal}(E/K)<\mathrm{Gal}(E/\mathbb{Q})$), K fixed field of $\mathrm{Gal}(E/K)$!

To show not Solvable (1) check f(x) irreducible (2) Check $\deg f(x)=p$ prime (3) f(x) has exactly $p-2$ roots (and 2 complex conjugate roots) [ie: Rolle's thm → If derivative has K roots, function cannot have more than K+1 roots.

Small Soluable Groups (Normal Subgroups Listed)

Klein 4-group $\mathbb{Z}_2 \times \mathbb{Z}_2$

	ε	a	b	c
ε	ε	a	b	c
a	a	ε	c	b
b	b	c	ε	a
c	c	b	a	ε

Subgroups $\{\varepsilon\}, \{\varepsilon, a\}, \{\varepsilon, b\}, \{\varepsilon, c\}, \{\varepsilon, a, b, c\}$ (all are normal)

* All elements have order 2 (except ε)
* Commutative ($\Rightarrow$ Soluable)

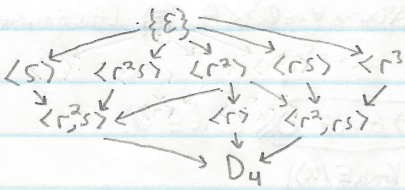
S_3

$\langle r, s \rangle = \{\varepsilon, r, r^2, s, rs, r^2s\}$ Subgroups $\{\varepsilon\}, \{\varepsilon, s\}, \{\varepsilon, rs\}, \{\varepsilon, r^2s\}, \{\varepsilon, r, r^2\}$

	ε	r	r^2	s	rs	r^2s
ε	ε	r	r^2	s	rs	r^2s
r	r	r^2	ε	rs	r^2s	s
r^2	r^2	ε	r	r^2s	s	rs
s	s	r^2s	rs	ε	r^2	r
rs	rs	s	r^2s	r	ε	r^2
r^2s	r^2s	rs	s	r^2	r	ε

* $D_{2n} = \{r^i s^j : r^n = id, s^2 = id, sr^k s = r^{n-k}\}$, $sr^k = r^{n-k}s$ ($S_3 = D_3$)
  ($r^k)^{-1}$
  $rsr = r(r^{n-1}s) = s$
* $\{\varepsilon\} \trianglelefteq \{\varepsilon, r, r^2\} \trianglelefteq S_3$ ($\Rightarrow$ Soluable)

D_4



* $\{\varepsilon\} \trianglelefteq \langle r^2 \rangle \trianglelefteq \langle r \rangle \trianglelefteq D_4$ ($\Rightarrow$ Soluable)

Q_8

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	j	$-j$
$-i$	$-i$	i	1	-1	$-k$	k	$-j$	j
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	i	$-i$	-1	1
$-k$	$-k$	k	$-j$	j	$-i$	i	-1	-1

* every subgroup is normal.