MATH 5032 MIDTERM

SOLUTIONS

(1) [2 pts] What does it mean for an algebraic field extension L/K to be normal?

$\forall \alpha \in L$, m_α splits over L

↑ minimal polynomial / K

(b) [2 pts] What is the splitting field of $x^4 - 2$ over $\mathbb{Q}$? Identify explicitly a non-normal subfield.

$\mathbb{Q}(i, \sqrt[4]{2})$

$\mathbb{Q}(\sqrt[4]{2})$ [since this is the fixed field of a $\mathbb{Z}_2 \leq D_4$, which is not a normal subgroup]

(c) [3 pts] What is the Galois group? Define "soluble" (for finite groups), and explicitly demonstrate its solubility.

$D_4 = \langle r, h \mid hrh = r^{-1}, r^4 = 1, h^2 = 1 \rangle$

G solvable $\iff \exists$ sgps. $\{1\} = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_1 = G$ w/ G_{i-1}/G_i abelian

$1 \trianglelefteq \mathbb{Z}_4 \cong \langle r \rangle \trianglelefteq D_4$ ← quotient $\cong \mathbb{Z}_2$

(2) [3 pts] The polynomials $P(x) = x^3 + x + 1$ and $Q(x) = x^3 + x^2 + 1$ are irreducible over $\mathbb{Z}_2$. Let K (resp. K') be a field obtained from $\mathbb{Z}_2$ by adjoining a root of P (resp. Q). Describe explicitly an isomorphism from K to K'.

$K \cong \mathbb{Z}_2[x]/(P(x)) \longrightarrow \mathbb{Z}_2[x]/(Q(x)) \cong K'$

$x \longmapsto x+1$

Check well-def'd. : $P(x) \longmapsto P(x+1) = (x+1)^3 + (x+1) + 1 = x^3 + x^2 + x + 1 + x + 1 + 1$

$= Q(x)$.

(3) [6 pts] Compute the Galois group of $f(x) := x^3 + 4x + 1$ over $\mathbb{Q}$, over $\mathbb{Z}_7$, and over $\mathbb{Z}_5$.

by formula on cover, $\Delta = -4(4)^3 - 27(1)^2 = -283$ (prime)

$\underline{\mathbb{Q}}$: $f' > 0$, $f(-1) < 0 < f(0)$ $\not\Rightarrow$ Gauss lemma $\Rightarrow$ no roots $\in \mathbb{Q}$

$\overset{\text{cubic}}{\Rightarrow}$ irred. $/\mathbb{Q}$

Δ * square

$\Rightarrow G \cong S_3$

$\underline{\mathbb{Z}_7}$: no roots $\Rightarrow$ irred.

$\Delta = -283 \underset{(7)}{\equiv} -3 \underset{(7)}{\equiv} 4 = 2^2$

$\Rightarrow G \cong \mathbb{Z}_3$

$\underline{\mathbb{Z}_5}$: $3 (\equiv -2)$ is a root (only one), $f \underset{(5)}{\equiv} (x+2)(x^2 - 2x + 3)$ (irred.)

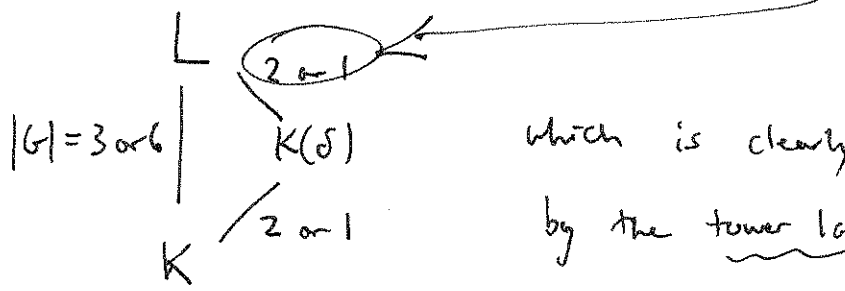
$\Rightarrow G \cong \mathbb{Z}_2$.

(4) [4 pts] Let f be an irreducible cubic polynomial over K with $\mathrm{char}(K) \neq 2$, and let δ be a square root of the discriminant of f. Show that f remains irreducible over $K(\delta)$.

$L :=$ SFE for f/K contains δ, hence also

$=$ SFE for $f/K(\delta)$

Suppose f reducible $/K(\delta)$. Then we have



which is clearly impossible by the tower law.

(5) (a) [8 pts] Use the Galois correspondence to find all subfields of $\mathbb{Q}(\zeta_7)$, and express them in the form $\mathbb{Q}(\alpha)$. Which are Galois over $\mathbb{Q}$?

$$\mathrm{Aut}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \cong \mathbb{Z}_7^* \cong \mathbb{Z}_6 \overset{\text{sgps.}}{\geq} \mathbb{Z}_2, \mathbb{Z}_3$$

$$\mathbb{Z}_7^* = \langle 3 \rangle \qquad \mathbb{Z}_2 = \langle -1 \rangle \qquad \mathbb{Z}_3 = \langle 2 \rangle$$

$\{\zeta_7, \zeta_7^2, \zeta_7^3, \zeta_7^4, \zeta_7^5, \zeta_7^6\}$ = basis of $\mathbb{Q}(\zeta_7)/\mathbb{Q}$

Basis of fixed fld. of $\mathbb{Z}_2$: $\zeta_7 + \zeta_7^6$, $\zeta_7^2 + \zeta_7^5$, $\zeta_7^3 + \zeta_7^4$

α (circled) $\qquad \alpha^2 - 2 \qquad \alpha^3 - 3\alpha$

$\Rightarrow$ fixed fld. is $\mathbb{Q}(\alpha)$.

Basis of fixed field of $\mathbb{Z}_3$: $\zeta_7 + \zeta_7^2 + \zeta_7^4$, $\zeta_7^3 + \zeta_7^6 + \zeta_7^5$

β (circled) $\qquad 1 - \beta \quad (\Leftarrow 1 + \zeta_7 + \cdots + \zeta_7^6 = 0)$

$\Rightarrow$ fixed field is $\mathbb{Q}(\beta)$

$\mathbb{Z}_7^*$ abelian $\Rightarrow$ all sgps. normal

$\Rightarrow$ all subfields of $\mathbb{Q}(\zeta_7)$ normal/$\mathbb{Q}$

$\Rightarrow$ " " " Galois/$\mathbb{Q}$

(b) [2 pts] Using a criterion from class, show that a regular 7-gon is not constructible with straightedge and compass.

$[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = 6$ which is not of the form 2^t.

(6) (a) [5 pts] Let K be a finite field, of order $q = p^m$. Show that K is a splitting field for $x^q - x$.

K^* grp., $|K^*| = q-1 \implies \alpha^{q-1} = 1 \quad \forall \alpha \in K^*$

$\implies \alpha^q - \alpha = 0 \quad \forall \alpha \in K.$

Repeatedly applying div. algorithm. gives

$$x^q - x = \prod_{\alpha \in K} (x - \alpha)$$

so that $x^q - x$ splits/K and K is generated by its roots.

$\implies$ K is SFE.

(b) [5 pts] Let $f \in K[x]$ be irreducible of degree $n > 1$. Use (a) to give a direct proof that f is separable. [Hint: given one root, what are the others?]

Let L be an SFE/K for f, $\sigma = \varphi^m$ the $(p^m = q^{th})$ power Frob map $\in Aut(L/K)$.

Since $x^q - x$ cannot have $> q$ distinct roots, and the q elements of K are all roots, K is precisely the fixed field of σ.

Now let $\alpha \in L$ be a root of f, and suppose $\sigma^k(\alpha) = \alpha$.

Then α is in the fixed fld. of σ^k, which has order $\leq p^{mk} = |K|^k$ hence degree $\leq k$ /K. Since $m_\alpha \in K[x]$ has degree n, $[K(\alpha) : K] = n$ and so $k \geq n$.

Hence the $\{\alpha, \sigma(\alpha), \sigma^2(\alpha), \ldots, \sigma^{n-1}(\alpha)\}$ are distinct, and by the freshmen's dream are also roots of f

$\implies$ f has no repeated roots.