Peize Liu
St. Peter's College
University of Oxford

Problem Sheet 4

B3.1: Galois Theory

A⁻ Great work! Well explained.
Just a few silly mistakes
I think.

1 January, 2020

In these problems K denotes an arbitrary field and $K[x]$ denotes the ring of polynomials in one variable x over K. If p is a prime number, then $\mathbb{F}_p$ denotes the field of integers modulo p.

Question 1

Find the Galois groups of the following polynomials over $\mathbb{Q}$:

(a) $x^5-2x^3-x^2+2$;

(b) x^5-2;

(c) x^5-4x+2.

Proof. (a) Note that $f(x):=x^5-2x^3-x^2+2$ has the factorisation over $\mathbb{Q}$:

$$x^5-2x^3-x^2+2=(x-1)(x^2-2)(x^2+x+1)$$

Hence the roots of f in $\mathbb{C}$ are 1, $\sqrt{2}$, $-\sqrt{2}$, ω, ω^2, where ω is a primitive third root of unity. Hence the splitting field of f over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2},\omega)$.

It is clear that $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$ and that $[\mathbb{Q}(\sqrt{2},\omega):\mathbb{Q}(\sqrt{2})]=2$. The latter is because $\omega\notin\mathbb{R}\supseteq\mathbb{Q}(\sqrt{2})$ and ω has minimal polynomial with degree 2 over $\mathbb{Q}$. Hence by tower law $[\mathbb{Q}(\omega,\sqrt{2}):\mathbb{Q}]=4$. Since $\mathbb{Q}$ is separable, this is a Galois extension. $|\mathrm{Gal}(f)|=4$. Consider $\sigma\in\mathrm{Gal}(f)$ that swaps ω wiuth ω^2 and fixes all other roots, and $\tau\in\mathrm{Gal}(f)$ that swaps $\sqrt{2}$ with $-\sqrt{2}$ fixes all other roots. σ and τ are of order 2 in $\mathrm{Gal}(f)$. Hence $\mathrm{Gal}(f)\cong V_4=\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. ✓

(b) The set of roots of x^5-2 in $\mathbb{C}$ are $\{2^{1/5}\zeta:\ \zeta^5=1\}$. Fix $\zeta\in\mathbb{C}$ to be a primitve fifth root of unity. Observe that $[\mathbb{Q}(\zeta):\mathbb{Q}]=4$ because the minimal polynomial of ζ over $\mathbb{Q}$ is $\Phi_5(x)=x^4+x^3+x^2+x+1$.

Next, f splits over $\mathbb{Q}(2^{1/5},\zeta)$, which is a Kummer extension over $\mathbb{Q}(\zeta)$. Therefore we have a (non-trivial) monomorphism $\mathrm{Gal}\left(\mathbb{Q}(2^{1/5},\zeta)\mid\mathbb{Q}(\zeta)\right)\to\mu_5(\mathbb{Q}(\zeta))\cong\mathbb{Z}/5\mathbb{Z}$. Since $\mathbb{Z}/5\mathbb{Z}$ is simple, we have $\mathrm{Gal}\left(\mathbb{Q}(2^{1/5},\zeta)\right)\cong\mathbb{Z}/5\mathbb{Z}$.

By Galois correspondence and tower law, we have

$$\left|\mathrm{Gal}\left(\mathbb{Q}(2^{1/5},\zeta)\mid\mathbb{Q}\right)\right|=[\mathbb{Q}(2^{1/5},\zeta):\mathbb{Q}]=[\mathbb{Q}(2^{1/5},\zeta):\mathbb{Q}(\zeta)][\mathbb{Q}(\zeta):\mathbb{Q}]=20$$

By the three Sylow theorems, $G:=\mathrm{Gal}\left(\mathbb{Q}(2^{1/5},\zeta)\mid\mathbb{Q}\right)$ has a unique Sylow 5-subgroup $\mathrm{Gal}\left(\mathbb{Q}(2^{1/5},\zeta)\mid\mathbb{Q}(\zeta)\right)$, which is normal. This subgroup is generated by the $\mathbb{Q}$-automorphism $\gamma\in G$ such that $\gamma(2^{1/5})=2^{1/5}\zeta$ and $\gamma(\zeta)=\zeta$.

Consider another $\mathbb{Q}$-automorphism $\beta\in G$ such that $\beta(2^{1/5})=2^{1/5}$ and $\beta(\zeta)=\zeta^2$. It is clear that $G=\langle\gamma\rangle\langle\beta\rangle$ and $\langle\gamma\rangle\cap\langle\beta\rangle=\{\mathrm{id}\}$. Therefore G is a semi-direct product: $G=\langle\gamma\rangle\rtimes_\varphi\langle\beta\rangle$ for some $\varphi:\langle\beta\rangle\to\mathrm{Aut}(\langle\gamma\rangle)$.

To determine φ, we simply note that $\gamma^2\circ\beta(2^{1/5})=\beta\circ\gamma(2^{1/5})=2^{1/5}\zeta^2$ and $\gamma^2\circ\beta(\zeta)=\beta\circ\gamma(\zeta)=\zeta^2$. Hence $\gamma^2=\beta\circ\gamma\circ\beta^{-1}$. Therefore $\varphi(\beta)$ is the inner automorphism of G that maps γ to γ^2.

We conclude that $\mathrm{Gal}(f)=\langle\gamma\rangle\rtimes\langle\beta\rangle\cong\mathbb{Z}/5\mathbb{Z}\rtimes_\varphi\mathbb{Z}/4\mathbb{Z}$, where $\varphi:\mathbb{Z}/5\mathbb{Z}\mapsto\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z})$ is given by $\varphi(\beta):\gamma\mapsto\gamma^2$. ✓

(c) We claim that $f(x):=x^5-4x+2$ has exactly 3 real roots. Then by Proposition 6.5 we have $\mathrm{Gal}(f)\cong S_5$.

Note that $f(-2)=-22$, $f(0)=2$, $f(1)=-1$, $f(2)=26$. By intermediate value theorem f has at least 3 real roots. The derivative of f is $f'(x)=5x^4-4$. It has exactly two real roots $\pm(4/5)^{1/4}$. f can change its monotonicity 2 times, and hence has at most 3 real roots. This proves the claim. ✓ Nice A $\square$

Question 2

In this exercise you will complete the characterization of finite fields. Let L be a finite field. Recall that there exists a prime number p, and a positive integer n such that $|L|=p^n$. Recall that $(L^*,\cdot)$ is a cyclic group.

(a) Show that there exists an irreducible polynomial $g(x)\in\mathbb{F}_p[x]$ such that $L\cong\mathbb{F}_p[x]/(g(x))$.

(b) Show that L is a Galois extension of $\mathbb{F}_p$.

(c) Show that, up to isomorphism, there exists a unique finite field of cardinality p^n. This finite field is denoted by $\mathbb{F}_{p^n}$.

(d) Show that the map $\varphi:\mathbb{F}_{p^n}\longrightarrow\mathbb{F}_{p^n}$ defined by $\varphi(y):=y^p$ is an automorphism of $\mathbb{F}_{p^n}$. This map is called the Frobenius automorphism.

(e) Show that $\Gamma\left(\mathbb{F}_{p^n} : \mathbb{F}_p\right) \cong (\mathbb{Z}/n\mathbb{Z}, +)$.

(f) Deduce that there is exactly one subfield of $\mathbb{F}_{p^n}$ for any divisor d of n.

(g) Let $f \in \mathbb{F}_p[x]$ be an irreducible polynomial. Show that f splits into linear factors in $\mathbb{F}_{p^{\deg(f)}}$.

Proof. (c) We know that $L^\times$ is a cyclic group of order $p^n - 1$. Hence any $\alpha \in L^\times$ satisfies $\alpha^{p^n-1} - 1 = 0$ and hence is a root of $f(x) := x^{p^n} - x \in \mathbb{F}_p[x]$. In addition, $0 \in L$ is also a root of f. Hence f splits over L and L is exactly the set of all roots of f. Hence L is the splitting field of f over $\mathbb{F}_p$. By Theorem 3.13, all splitting fields of f over $\mathbb{F}_p$ is isomorphic. Hence the finite field of cardinality p^n is unique up to isomorphism. ✓

(a) Since L is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p[x]$, by Question 2 of Sheet 3, there exists an element $\alpha \in L$ such that $L \cong \mathbb{F}_p(\alpha)$. Let $g \in \mathbb{F}_p[x]$ be the minimal polynomial of α. Then g is irreducible and $L \cong \mathbb{F}_p(\alpha) = \mathbb{F}_p[x]/\langle g(x)\rangle$. ✓

(b) L is the splitting extension of f over $\mathbb{F}_p$, and we know that f is separable. By Theorem 3.18 $L \mid \mathbb{F}_p$ is a Galois extension. ✓

(d) The proof that $\alpha \mapsto \alpha^p$ is an automorphism of $\mathbb{F}_{p^n}$ is essentially the same as the proof in Question 6 of Sheet 1.

For $\alpha, \beta \in \mathbb{F}_{p^n}$,

$$(\alpha\beta)^p = \alpha^p\beta^p, \qquad (\alpha+\beta)^p = \sum_{k=0}^{p} \frac{p!}{k!(p-k)!}\alpha^k\beta^{p-k} = \alpha^p + \beta^p$$

We have used the fact that $\dfrac{p!}{k!(p-k)!}$ is divisible by p for $1 \leqslant k \leqslant p-1$. Therefore φ is a ring homomorphism. Since and $0^p = 0$ $1^p = 1$, $\ker\varphi = \{0\}$. φ is faithful. Since $\mathbb{F}_{p^n}$ is finite, φ is bijective. We conclude that φ is an automorphism of $\mathbb{F}_{p^n}$. ✓

(e) First we note that the Frobenius automorphism fixes elements in $\mathbb{F}_p$, because $\mathbb{F}_p$ is the prime subfield of $\mathbb{F}_{p^n}$, and $\varphi(1) = 1$ implies that $\varphi(k) = k$ for all $k \in \mathbb{F}_p$. Hence $\varphi \in \mathrm{Gal}\left(\mathbb{F}_{p^n} \mid \mathbb{F}_p\right)$.

Second, we claim that φ has order n in $\mathrm{Gal}\left(\mathbb{F}_{p^n} \mid \mathbb{F}_p\right)$. For $\alpha \in \mathbb{F}_{p^n}$,

$$\varphi^n(\alpha) = \alpha^{p^n} = \alpha \implies \varphi^n = \mathrm{id}$$

In addition, if $\varphi^k = \mathrm{id}$ for some $k \leqslant n$, then $x^{p^k} - x$ has p^n distinct roots in $\mathbb{F}_{p^n}$, which is impossible.

Finally, by the fundamental theorem $|\mathrm{Gal}\left(\mathbb{F}_{p^n} \mid \mathbb{F}_p\right)| = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. We deduce that φ generates $\mathrm{Gal}\left(\mathbb{F}_{p^n} \mid \mathbb{F}_p\right)$ and hence $\mathrm{Gal}\left(\mathbb{F}_{p^n} \mid \mathbb{F}_p\right) \cong \mathbb{Z}/n\mathbb{Z}$. ✓

(f) For any d with $d \mid n$, $\mathbb{Z}/n\mathbb{Z}$ has a unique subgroup of order d. By the Galois correspondence, there is a unique subfield M of $\mathbb{F}_{p^n}$ such that $[\mathbb{F}_{p^n} : M] = d$. ✓

(g) Let $n = \deg f$. Let α be a root of f in its splitting field. Then f is the minimal polynomial of α over $\mathbb{F}_p$ and $\mathbb{F}_{p^n} \cong \mathbb{F}_p(\alpha)$. Using the Frobenius automorphism, we find that $\alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{n-1}}$ are also roots of f. Since $\deg f = n$, we have in fact

$$f(x) = \prod_{i=0}^{n-1}(x - \alpha^{p^i})$$

in $\mathbb{F}_{p^n}$. Hence f splits over $\mathbb{F}_{p^n}$, ✓ Great A □

Question 3

Let p be an odd prime, $K = \mathbb{F}_p(t)$, and $f = x^4 - t \in K[x]$.

(a) Find the splitting field E of f distinguishing the cases $p \equiv 1 \bmod 4$ and $p \equiv 3 \bmod 4$.

(Hint: if α is a root of f, find $c \in E$ such that $c\alpha$ is a root of f)

(b) Write down a set of generators for $\Gamma(E : K)$ distinguishing the cases $p \equiv 1 \bmod 4$ and $p \equiv 3 \bmod 4$.

(c) In the case $p \equiv 1 \bmod 4$ write down the Galois correspondence for $E : K$ and $\Gamma(E : K)$.

Proof. (a) In the splitting field of f, we have

$$f(x) = (x - t^{1/4})(x - \omega t^{1/4})(x - \omega^2 t^{1/4})(x - \omega^3 t^{1/4})$$

where ω is a primitive fourth root of unity.

When $p \equiv 1 \bmod 4$, $\mathbb{F}_p^\times$ is a cyclic group whose order is divisible by 4. Hence K contains all fourth roots of unity. The splitting field of f over K is $K(t^{1/4})$, which is degree 4 over K. ✓

When $p \equiv 3 \bmod 4$, the order of $\mathbb{F}_p^\times$ is divisible by 2 but not 4. Then the splitting field of $x^4 - 1$ is $K(\omega)$, which is a quadratic extension K. The splitting field of f over K is $K(t^{1/4}, \omega)$, which is degree 8 over K. ✓

(b) When $p \equiv 1 \bmod 4$, $E \mid K$ is a Kummer extension. By Lemma 5.6 there exists a group monomorphism $\mathrm{Gal}(E \mid K) \to \mu_4(K)$. Since $|\mathrm{Gal}(E \mid K)| = 4$, we deduce that $\mathrm{Gal}(E \mid K) \cong \mu_4(K) \cong \mathbb{Z}/4\mathbb{Z}$. $\mathrm{Gal}(E \mid K)$ is generated by the K-automorphism given by $\gamma : t^{1/4} \mapsto t^{1/2}$. ? you mean $t^{1/4} \mapsto \omega t^{1/4}$

When $p \equiv 1 \bmod 3$, $E \mid K(\omega)$ is a Kummer extension. It is easy to observe that $\mathrm{Gal}(E \mid K)$ is generated by γ and σ, where γ maps $t^{1/4}$ to $t^{1/2}$ and fixes ω, and σ maps ω to ω^3 and fixes $t^{1/4}$. We have $\mathrm{Gal}(E \mid K) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

same mistake here

should be D_8, which is non-abelian, as $\sigma\tau \neq \tau\sigma$

(c) $\mathrm{Gal}(E \mid K) \cong \mu_4(K) \cong \mathbb{Z}/4\mathbb{Z}$ has a unique non-trivial proper subgroup, and hence $E \mid K$ has a unique intermediate field. The Galois correspondence is given by

$$\begin{array}{ccccc} K & \subseteq & K(t^{1/2}) & \subseteq & K(t^{1/4}) \\ \updownarrow & & \updownarrow & & \updownarrow \\ \langle\gamma\rangle & \supseteq & \langle\gamma^2\rangle & \supseteq & \{\mathrm{id}\} \end{array}$$

✓ Good work

AB

□

Question 4

Let L/K be a finite separable extension of field. Define a *Galois Closure* M of L/K as a minimal degree extension of L for which M/K is Galois. Show that the Galois Closure of L/K exists and is unique up to isomorphism. Show that the set of K invariant embeddings $\hom_K(L, M)$ of L in M is in natural bijection with the set of right cosets of $\Gamma(M : L)$ in $\Gamma(M : K)$.

Proof. By primitive element theorem, $L \mid K$ is a simple extension. There exists $\alpha \in L$ such that $L = K(\alpha)$. Let $f \in K[x]$ be the minimal polynomial of α. By definition f is separable. Let M be the splitting field of f over K. By Theorem 3.18 $M \mid K$ is a Galois extension. We claim that M is a the Galois closure of $L \mid K$.

Since M is the splitting field of the minimal polynomial of α, then $\alpha \in M$. Hence $L = K(\alpha) \subseteq M$. Suppose that F is an extension of L such that $F \mid K$ is a Galois extension. By Theorem 3.18, $F \mid K$ is a normal extension. $\alpha \in L \subseteq F$ implies that f splits over F. Hence F contains a splitting field of f over K. As all splitting fields of f are K-isomorphic, we deduce that M is an extension of L of minimal degree such that $M \mid K$ is a Galois extension. Finally, since all Galois closures of $L \mid K$ are splitting fields of f, they are K-isomorphic. ✓

The notation $\mathrm{Hom}_K(L, M)$ *seems ambiguous, since it normally refers to the set of all K-linear maps from L to M.*

I think the notation is just invented for the Qn

First we fix an embedding $\iota : L \hookrightarrow M$. For $\gamma \in \mathrm{Gal}(M \mid K)$, we define $\Phi(\gamma) := \gamma \circ \iota \in \mathrm{Hom}_K(L, M)$. We claim that Φ is a bijective from the set of right cosets of $\mathrm{Gal}(M \mid L)$ in $\mathrm{Gal}(M \mid K)$ to $\mathrm{Hom}_K(L, M)$.

- For $\gamma, \beta \in \mathrm{Gal}(M \mid K)$,

$$\begin{aligned} \gamma \circ \iota = \beta \circ \iota &\iff \gamma \circ \iota(\alpha) = \beta \circ \iota(\alpha) \\ &\iff \beta^{-1} \circ \gamma \circ \iota(\alpha) = \iota(\alpha) \\ &\iff \beta^{-1} \circ \gamma \text{ fixes } \iota(L) \\ &\iff \beta^{-1} \circ \gamma \in \mathrm{Gal}(M \mid L) \\ &\iff \mathrm{Gal}(M \mid L)\beta = \mathrm{Gal}(M \mid L)\gamma \end{aligned}$$

  Hence Φ is well-defined and injective.

- For $\sigma \in \mathrm{Hom}_K(L, M)$, the assignment $\iota(\alpha) \mapsto \sigma(\alpha)$ extends to a K-isomorphism $\gamma \in \mathrm{Gal}(M \mid K)$ with $\gamma \circ \iota(\alpha) = \sigma(\alpha)$. Since $L = K(\alpha)$, then $\sigma = \gamma \circ \iota = \Phi(\gamma)$. Hence Φ is surjective. ✓ □

A

Question 5

Let ℓ be a positive integer, p be a prime number, and $f_\ell = x^{2^\ell} + 1 \in \mathbb{F}_p[x]$. If $N > 1$ is an integer, we denote by $U(\mathbb{Z}/N\mathbb{Z})$ the set of invertible elements of the ring $\mathbb{Z}/N\mathbb{Z}$. Recall that $(U(\mathbb{Z}/N\mathbb{Z}), \cdot)$ is a multiplicative group.

(a) Show that any polynomial of degree 2 in $\mathbb{F}_p[x]$ splits in $\mathbb{F}_{p^2}[x]$.

(b) Show that for $p = 3$ the polynomial f_1 is irreducible in $\mathbb{F}_3[x]$ and give a construction of the field $\mathbb{F}_{3^2}$.

(c) Show that the splitting field of f_ℓ is isomorphic to the splitting field of $x^{2^{\ell+1}} - 1 \in \mathbb{F}_p[x]$.

(d) Prove that for $p = 5$ the polynomial $f_2 \in \mathbb{F}_5[x]$ is reducible.

(e) Show that there exists an integer ℓ such that for any prime number p, the polynomial f_ℓ is reducible in $\mathbb{F}_p[x]$.

(Hint: show first that $(U(\mathbb{Z}/2^n\mathbb{Z}), \cdot)$ is not a cyclic group if $n \geqslant 3$).

Proof. (a) Let $f \in \mathbb{F}_p[x]$ with $\deg f = 2$. If f is irreducible, then f splits over $\mathbb{F}_{p^2}$ by Question 2.(g). If f is reducible, then f already splits over $\mathbb{F}_p$. Since $\mathbb{F}_p \subseteq \mathbb{F}_{p^2}$, f also splits over $\mathbb{F}_{p^2}$.

(b) $f_1(x) = x^2 + 1 \in \mathbb{F}_3[x]$. Since $f_1(0) = 1$, $f_1(1) = 2$, $f_1(2) = 2$, then f_1 has no roots in $\mathbb{F}_3$. Hence f_1 is irreducible in $\mathbb{F}_3[x]$. The splitting field of f_1 over $\mathbb{F}_3$ is $\mathbb{F}_3[x]/\langle x^2+1\rangle \cong \mathbb{F}_{3^2}$, also as a result of Question 2.(g).

(c) Note that

$$x^{2^{\ell+1}} - 1 = (x-1)\prod_{i=0}^{\ell}\left(x^{2^i}+1\right) = (x-1)\prod_{i=0}^{\ell} f_i(x)$$

For simplicity consider the algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$. The set of roots of f_i in $\overline{\mathbb{F}_p}$ is exactly

If $u^2 = -1$ does $u^4 = -1$?

$$G_i := \left\{u \in \overline{\mathbb{F}_p} :\ u^{2^i} = -1\right\}$$

Observe that $G_i \subseteq G_{i+1}$ for each $i \in \mathbb{N}$. We find that f_ℓ and $x^{2^{\ell+1}} - 1$ has the same set of roots in $\overline{\mathbb{F}_p}$. Hence their splitting fields are isomorphic.

We have $G_i = G_{i+1}^2 = \{x^2 : x \in G_{i+1}\} \Rightarrow$ all roots of $x^{2^{\ell+1}} - 1$ in spl field of f_ℓ

(d) In $\mathbb{F}_5[x]$, we have

$$f_2(x) = x^4 + 1 = (x^2+2)(x^2+3)$$

Hence $f_2 \in \mathbb{F}_5[x]$ is reducible.

(e) In Question 3.(b) of Sheet 3 we have proven that $24 \mid p^2 - 1$ for all primes $p > 3$. Hence $8 \mid p^2 - 1$ for all odd primes. Since $\mathbb{F}_{p^2}^\times \cong \mathbb{Z}/(p^2-1)\mathbb{Z}$, then $\mathbb{F}_{p^2}$ contains all eighth roots of unity. Hence $x^8 - 1$ splits in $\mathbb{F}_{p^2}[x]$. By part (c), $f_2(x) = x^4 + 1$ also splits in $\mathbb{F}_{p^2}[x]$. Suppose that f_2 is irreducible in $\mathbb{F}_p[x]$. Then for any root α of f_2 we have $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \deg f_2 = 4$. But $[\mathbb{F}_{p^2} : \mathbb{F}_p] = 2$, which is a contradiction. Therefore f_2 is reducible in $\mathbb{F}_p[x]$ for all odd primes p. Finally, $f_2(x) = (x^2-1)^2 \in \mathbb{F}_2[x]$. Hence f_2 is reducible in $\mathbb{F}_2[x]$. We deduce that f_2 is reducible in every $\mathbb{F}_p[x]$. □

AB