Title

D. Zack Garza

Monday 10th August, 2020

Contents

1 Fields and Galois Theory

1.1 ⋆ Fall 2016 #5

How many monic irreducible polynomials over $\mathbb{F}_p$ of prime degree ℓ are there? Justify your answer.

1.2 ⋆ Fall 2013 #7

Let $F = \mathbb{F}_2$ and let $\overline{F}$ denote its algebraic closure.

a. Show that $\overline{F}$ is not a finite extension of F.

b. Suppose that $\alpha \in \overline{F}$ satisfies $\alpha^{17} = 1$ and $\alpha \neq 1$. Show that $F(\alpha)/F$ has degree 8.

1.3 Spring 2020 #3

Let E be an extension field of F and $\alpha \in E$ be algebraic of odd degree over F.

a. Show that $F(\alpha) = F(\alpha^2)$.

b. Prove that α^{2020} is algebraic of odd degree over F.

1.4 Spring 2020 #4

Let $f(x) = x^4 - 2 \in \mathbb{Q}[x]$.

a. Define what it means for a finite extension field E of a field F to be a Galois extension.

b. Determine the Galois group $\mathrm{Gal}(E/\mathbb{Q})$ for the polynomial $f(x)$, and justify your answer carefully.

c. Exhibit a subfield K in (b) such that $\mathbb{Q} \leq K \leq E$ with K not a Galois extension over $\mathbb{Q}$. Explain.

1.5 Fall 2019 #4 ⋈

Let F be a finite field with q elements.

Let n be a positive integer relatively prime to q and let ω be a primitive nth root of unity in an extension field of F.

Let $E = F[\omega]$ and let $k = [E : F]$.

(a) Prove that n divides $q^k - 1$.

(b) Let m be the order of q in $\mathbb{Z}/n\mathbb{Z}^\times$. Prove that m divides k.

(c) Prove that $m = k$.

Solution.
Concepts used:

- Theorem: $F^\times$ is always cyclic for F a field

Solution:

1.5.1 a

- Since $|F| = q$ and $[E : F] = k$, we have $|E| = q^k$ and $|E^\times| = q^k - 1$.
- Noting that $\zeta \in E^\times$ we must have $n = o(\zeta) \,\Big|\, |E^\times| = q^k - 1$ by Lagrange's theorem.

1.5.2 b

- Rephrasing (a), we have

$$\begin{aligned} n \,\Big|\, q^k - 1 &\iff q^k - 1 \cong 0 \mod n \\ &\iff q^k \cong 1 \mod n \\ &\iff m := o(q) \,\Big|\, k. \end{aligned}$$

1.5.3 c

- Since $m \,\Big|\, k \iff k = \ell m$, (**claim**) there is an intermediate subfield M such that

$$E \leq M \leq F \quad k = [F : E] = [F : M][M : E] = \ell m,$$

  so M is a degree m extension of E.
- Now consider $M^\times$.
- By the argument in (a), n divides $q^m - 1 = |M^\times|$, and $M^\times$ is cyclic, so it contains a cyclic subgroup H of order n.

- But then $x \in H \implies p(x) := x^n - 1 = 0$, and since $p(x)$ has at most n roots in a field.
- So $H = \left\{ x \in M \mid x^n - 1 = 0 \right\}$, i.e. H contains all solutions to $x^n - 1$ in $E[x]$.
- But ζ is one such solution, so $\zeta \in H \subset M^\times \subset M$.
- Since $F[\zeta]$ is the smallest field extension containing ζ, we must have $F = M$, so $\ell = 1$, and $k = m$.

Revisit. Tricky!

1.6 Fall 2019 #7 ⋈

Let ζ_n denote a primitive nth root of $1 \in \mathbb{Q}$. You may assume the roots of the minimal polynomial $p_n(x)$ of ζ_n are exactly the primitive nth roots of 1.

Show that the field extension $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is Galois and prove its Galois group is $(\mathbb{Z}/n\mathbb{Z})^\times$.

How many subfields are there of $\mathbb{Q}(\zeta_{20})$?

Solution.
Concepts Used:

- **Galois** = normal + separable.
- **Separable**: Minimal polynomial of every element has distinct roots.
- **Normal (if separable)**: Splitting field of an irreducible polynomial.
- Definition: ζ is a primitive root of unity iff $o(\zeta) = n$ in $F^\times$.
- $\varphi(p^k) = p^{k-1}(p-1)$
- The lattice:

Solution:
Let $K = \mathbb{Q}(\zeta)$. Then K is the splitting field of $f(x) = x^n - 1$, which is irreducible over $\mathbb{Q}$, so $K/\mathbb{Q}$ is normal. We also have $f'(x) = nx^{n-1}$ and $\gcd(f, f') = 1$ since they can not share any roots.

Or equivalently, f splits into distinct linear factors $f(x) = \prod_{k \leq n} (x - \zeta^k)$.

Since it is a Galois extension, $|\mathrm{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = \varphi(n)$ for the totient function.
We can now define maps

$$\begin{aligned} \tau_j : K &\longrightarrow K \\ \zeta &\mapsto \zeta^j \end{aligned}$$

and if we restrict to j such that $\gcd(n, j) = 1$, this yields $\varphi(n)$ maps. Noting that if ζ is a primitive root, then $(n, j) = 1$ implies that that ζ^j is also a primitive root, and hence another root of $\min(\zeta, \mathbb{Q})$, and so these are in fact automorphisms of K that fix $\mathbb{Q}$ and thus elements of $\mathrm{Gal}(K/\mathbb{Q})$.
So define a map

$$\begin{aligned} \theta : \mathbb{Z}_n^\times &\longrightarrow K \\ [j]_n &\mapsto \tau_j. \end{aligned}$$

from the *multiplicative* group of units to the Galois group.
The claim is that this is a surjective homomorphism, and since both groups are the same size, an isomorphism.
Surjectivity:

Letting $\sigma \in K$ be arbitrary, noting that $[K : \mathbb{Q}]$ has a basis $\left\{1, \zeta, \zeta^2, \cdots, \zeta^{n-1}\right\}$, it suffices to specify $\sigma(\zeta)$ to fully determine the automorphism. (Since $\sigma(\zeta^k) = \sigma(\zeta)^k$.)
In particular, $\sigma(\zeta)$ satisfies the polynomial $x^n - 1$, since $\sigma(\zeta)^n = \sigma(\zeta^n) = \sigma(1) = 1$, which means $\sigma(\zeta)$ is another root of unity and $\sigma(\zeta) = \zeta^k$ for some $1 \leq k \leq n$.
Moreover, since $o(\zeta) = n \in K^\times$, we must have $o(\zeta^k) = n \in K^\times$ as well. Noting that $\left\{\zeta^i\right\}$ forms a cyclic subgroup $H \leq K^\times$, then $o(\zeta^k) = n \iff (n, k) = 1$ (by general theory of cyclic groups).
Thus θ is surjective.
Homomorphism:

$$\tau_j \circ \tau_k(\zeta) = \tau_j(\zeta^k) = \zeta^{jk} \implies \tau_{jk} = \theta(jk) = \tau_j \circ \tau_k.$$

Part 2:
We have $K \cong \mathbb{Z}_{20}^\times$ and $\varphi(20) = 8$, so $K \cong \mathbb{Z}_8$, so we have the following subgroups and corresponding intermediate fields:

- $0 \sim \mathbb{Q}(\zeta_{20})$
- $\mathbb{Z}_2 \sim \mathbb{Q}(\omega_1)$
- $\mathbb{Z}_4 \sim \mathbb{Q}(\omega_2)$
- $\mathbb{Z}_8 \sim \mathbb{Q}$

For some elements ω_i which exist by the primitive element theorem.

1.7 Spring 2019 #2 $\bowtie$

Let $F = \mathbb{F}_p$, where p is a prime number.

(a) Show that if $\pi(x) \in F[x]$ is irreducible of degree d, then $\pi(x)$ divides $x^{p^d} - x$.

(b) Show that if $\pi(x) \in F[x]$ is an irreducible polynomial that divides $x^{p^n} - x$, then $\deg \pi(x)$ divides n.

Solution.

1.7.1 (a)

Go to a field extension. Orders of multiplicative groups for finite fields are known.

We can consider the quotient $K = \dfrac{\mathbb{F}_p[x]}{\langle \pi(x) \rangle}$, which since $\pi(x)$ is irreducible is an extension of $\mathbb{F}_p$ of degree d and thus a field of size p^d with a natural quotient map of rings $\rho : \mathbb{F}_p[x] \longrightarrow K$.
Since $K^\times$ is a group of size $p^d - 1$, we know that for any $y \in K^\times$, we have by Lagrange's theorem that the order of y divides $p^d - 1$ and so $y^{p^d} = y$.
So every element in K is a root of $q(x) = x^{p^d} - x$.
Since ρ is a ring morphism, we have

$$
\begin{aligned}
\rho(q(x)) = \rho(x^{p^d} - x) = \rho(x)^{p^d} - \rho(x) = 0 \in K \\
&\iff q(x) \in \ker \rho \\
&\iff q(x) \in \langle \pi(x) \rangle \\
&\iff \pi(x) \,\Big|\, q(x) = x^{p^d} - x \quad \text{"to contain is to divide".}
\end{aligned}
$$

$\blacksquare$

1.7.2 (b)

Some potentially useful facts:

- $\mathbb{GF}(p^n)$ is the splitting field of $x^{p^n} - x \in \mathbb{F}_p[x]$.
- $x^{p^d} - x \,\Big|\, x^{p^n} - x \iff d \,\Big|\, n$
- $\mathbb{GF}(p^d) \leq \mathbb{GF}(p^n) \iff d \,\Big|\, n$
- $x^{p^n} - x = \prod f_i(x)$ over all irreducible monic f_i of degree d dividing n.

Claim: $\pi(x)$ divides $x^{p^n} - x \iff \deg \pi$ divides n.
$\implies$: Let $L \cong \mathbb{GF}(p^n)$ be the splitting field of $\varphi_n(x) := x^{p^n} - x$; then since $\pi \,\Big|\, \varphi_n$ by assumption, π splits in L. Let $\alpha \in L$ be any root of π; then there is a tower of extensions $\mathbb{F}_p \leq \mathbb{F}_p(\alpha) \leq L$.
Then $\mathbb{F}_p \leq \mathbb{F}_p(\alpha) \leq L$, and so

$$
\begin{aligned}
n &= [L : \mathbb{F}_p] \\
&= [L : \mathbb{F}_p(\alpha)]\ [\mathbb{F}_p(\alpha) : \mathbb{F}_p] \\
&= \ell d,
\end{aligned}
$$

for some $\ell \in \mathbb{Z}^{\geq 1}$, so d divides n.
$\impliedby$: If $d \,\Big|\, n$, use the fact (claim) that $x^{p^n} - x = \prod f_i(x)$ over all irreducible monic f_i of degree d dividing n. So $f = f_i$ for some i.

1.8 Spring 2019 #8 $\bowtie$

Let $\zeta = e^{2\pi i/8}$.

(a) What is the degree of $\mathbb{Q}(\zeta)/\mathbb{Q}$?

(b) How many quadratic subfields of $\mathbb{Q}(\zeta)$ are there?

(c) What is the degree of $\mathbb{Q}(\zeta, \sqrt[4]{2})$ over $\mathbb{Q}$?

Solution.
Concepts used:

- $\zeta_n := e^{\frac{2\pi i}{n}}$, and ζ_n^k is a primitive nth root of unity $\iff \gcd(n,k) = 1$
  - In general, ζ_n^k is a primitive $\dfrac{n}{\gcd(n,k)}$th root of unity.

- $\deg \Phi_n(x) = \varphi(n)$
- $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$ (proof: for a nontrivial gcd, the possibilities are $p, 2p, 3p, 4p, \cdots, p^{k-2}p, p^{k-1}p$.)
- $\operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \mathbb{Z}/(n)^\times$

Solution:
Let $K = \mathbb{Q}(\zeta)$

1.8.1 a

- $\zeta := e^{2\pi i/8}$ is a primitive 8th root of unity
- The minimal polynomial of an nth root of unity is the nth cyclotomic polynomial Φ_n
- The degree of the field extension is the degree of Φ_8, which is

$$\varphi(8) = \varphi(2^3) = 2^{3-1} \cdot (2-1) = 4.$$

- So $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$.

1.8.2 b

- $\operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \mathbb{Z}/(8)^\times \cong \mathbb{Z}/(4)$ by general theory
- $\mathbb{Z}/(4)$ has exactly one subgroup of index 2.
- Thus there is exactly **one** intermediate field of degree 2 (a quadratic extension).

1.8.3 c

- Let $L = \mathbb{Q}(\zeta, \sqrt[4]{2})$.
- Note $\mathbb{Q}(\zeta) = \mathbb{Q}(i, \sqrt{2})$
  - $\mathbb{Q}(i, \sqrt{2}) \subseteq \mathbb{Q}(\zeta)$
    * $\zeta_8^2 = i$, and $\zeta_8 = \sqrt{2}^{-1} + i\sqrt{2}^{-1}$ so $\zeta_8 + \zeta_8^{-1} = 2/\sqrt{2} = \sqrt{2}$.
  - $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(i, \sqrt{2})$:
    * $\zeta = e^{2\pi i/8} = \sin(\pi/4) + i\cos(\pi/4) = \dfrac{\sqrt{2}}{2}(1+i)$.
- Thus $L = \mathbb{Q}(i, \sqrt{2})(\sqrt[4]{2}) = \mathbb{Q}(i, \sqrt{2}, \sqrt[4]{2}) = \mathbb{Q}(i, \sqrt[4]{2})$.
  - Uses the fact that $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$ since $\sqrt[4]{2}^2 = \sqrt{2}$
- Conclude

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[4]{2})]\ [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2 \cdot 4 = 8$$

  using the fact that the minimal polynomial of i over any subfield of $\mathbb{R}$ is always x^2+1, so $\min_{\mathbb{Q}(\sqrt[4]{2})}(i) = x^2 + 1$ which is degree 2.

1.9 Fall 2018 #3 ⋈

Let $F \subset K \subset L$ be finite degree field extensions. For each of the following assertions, give a proof or a counterexample.

(a) If L/F is Galois, then so is K/F.

(b) If L/F is Galois, then so is L/K.

(c) If K/F and L/K are both Galois, then so is L/F.

Solution.
Let $L/K/F$.

1.9.1 a

False: Take $L/K/F = \mathbb{Q}(\zeta_2, \sqrt[3]{2}) \longrightarrow \mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{Q}$.
Then L/F is Galois, since it is the splitting field of $x^3 - 2$ and $\mathbb{Q}$ has characteristic zero.
But K/F is not Galois, since it is not the splitting field of any irreducible polynomial.

1.9.2 b

True: If L/F is Galois, then L/K is normal and separable:

- L/K is normal, since if $\sigma : L \hookrightarrow \overline{K}$ lifts the identity on K and fixes L, i-t also lifts the identity on F and fixes L (and $\overline{K} = \overline{F}$).
- L/K is separable, since $F[x] \subseteq K[x]$, and so if $\alpha \in L$ where $f(x) \coloneqq \min(\alpha, F)$ has no repeated factors, then $f'(x) \coloneqq \min(\alpha, K)$ divides f and thus can not have repeated factors.

1.9.3 c

False: Use the fact that every quadratic extension is Galois, and take $L/K/F = \mathbb{Q}(\sqrt[4]{2}) \longrightarrow \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}$.
Then each successive extension is quadratic (thus Galois) but $\mathbb{Q}(\sqrt[4]{2})$ is not the splitting field of any polynomial (noting that it does not split $x^4 - 2$ completely.)

1.10 Spring 2018 #2 ⋈

Let $f(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$.

(a) Find the splitting field K of f, and compute $[K : \mathbb{Q}]$.

(b) Find the Galois group G of f, both as an explicit group of automorphisms, and as a familiar abstract group to which it is isomorphic.

(c) Exhibit explicitly the correspondence between subgroups of G and intermediate fields between $\mathbb{Q}$ and k.

Not the nicest proof! Would be better to replace the ad-hoc computations at the end.

Solution.

1.10.1 a

Note that $g(x) = x^2 - 4x + 2$ has roots $\beta = 2 \pm \sqrt{2}$, and so f has roots

$$\begin{aligned}
\alpha_1 &= \sqrt{2 + \sqrt{2}} \\
\alpha_2 &= \sqrt{2 - \sqrt{2}} \\
\alpha_3 &= -\alpha_1 \\
\alpha_4 &= -\alpha_2.
\end{aligned}$$

and splitting field $K = \mathbb{Q}(\{\alpha_i\})$.

1.10.2 b

K is the splitting field of a separable polynomial and thus Galois over $\mathbb{Q}$. Moreover, Since f is irreducible by Eisenstein with $p = 2$, the Galois group is a transitive subgroup of S^4, so the possibilities are:

- S_4
- A_4
- D_4
- $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$
- $\mathbb{Z}/(4)$

We can note that g splits over $L := \mathbb{Q}(\sqrt{2})$, an extension of degree 2.
We can now note that $\min(\alpha, L)$ is given by $p(x) = x^2 - (2 + \sqrt{2})$, and so $[K : L] = 2$.
We then have

$$[K : \mathbb{Q}] = [K : L][L : \mathbb{Q}] = (2)(2) = 4.$$

This $|\mathrm{Gal}(K/\mathbb{Q})| = 4$, which leaves only two possibilities:

- $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$
- $\mathbb{Z}/(4)$

We can next check orders of elements. Take

$$\begin{aligned}
\sigma &\in \mathrm{Gal}(K/\mathbb{Q}) \\
\alpha_1 &\mapsto \alpha_2.
\end{aligned}$$

Computations show that

- $\alpha_1^2 \alpha_2^2 = 2$, so $\alpha_1 \alpha_2 = \sqrt{2}$
- $\alpha_1^2 = 2 + \sqrt{2} \implies \sqrt{2} = \alpha_1^2 - 2$

and thus

$$\begin{aligned}
\sigma^2(\alpha_1) &= \sigma(\alpha_2) \\
&= \sigma\left(\frac{\sqrt{2}}{\alpha_1}\right) \\
&= \frac{\sigma(\sqrt{2})}{\sigma(\alpha_1)} \\
&= \frac{\sigma(\alpha_1^2 - 2)}{\alpha_2} \\
&= \frac{\alpha_2^2 - 2}{\alpha_2} \\
&= \alpha_2 - 2\alpha_2^{-1} \\
&= \alpha_2 - \frac{2\alpha_1}{\sqrt{2}} \\
&= \alpha_2 - \alpha_1\sqrt{2} \\
&\neq \alpha_1,
\end{aligned}$$

and so the order of σ is strictly greater than 2, and thus 4, and thus $\mathrm{Gal}(K/\mathbb{Q}) = \left\{\sigma^k \;\middle|\; 1 \leq k \leq 4\right\} \cong \mathbb{Z}/(4)$.

1.10.3 c

?? The subgroup of index 2 $\left\langle \sigma^2 \right\rangle$ corresponds to the field extension $Q(\sqrt{2})/\mathbb{Q}$.

1.11 Spring 2018 #3 ⋈

Let K be a Galois extension of $\mathbb{Q}$ with Galois group G, and let E_1, E_2 be intermediate fields of K which are the splitting fields of irreducible $f_i(x) \in \mathbb{Q}[x]$.

Let $E = E_1E_2 \subset K$.

Let $H_i = \mathrm{Gal}(K/E_i)$ and $H = \mathrm{Gal}(K/E)$.

(a) Show that $H = H_1 \cap H_2$.

(b) Show that H_1H_2 is a subgroup of G.

(c) Show that

$$\mathrm{Gal}(K/(E_1 \cap E_2)) = H_1H_2.$$

Solution.

Moral: $H_1 \bigcap H_2 \iff E_1E_2,\ H_1H_2 \iff E_1 \bigcap E_2$.

1.11.1 a

By the Galois correspondence, it suffices to show that the fixed field of $H_1 \bigcap H_2$ is E_1E_2.

Let $\sigma \in H_1 \bigcap H_2$; then $\sigma \in \mathrm{Aut}(K)$ fixes both E_1 and E_2.

Not sure if this works – compositum is not literally product..?

Writing $x \in E_1 E_2$ as $x = e_1 e_2$, we have

$$\sigma(x) = \sigma(e_1 e_2) = \sigma(e_1)\sigma(e_2) = e_1 e_2 = x,$$

so σ fixes $E_1 E_2$.

1.11.2 b

That $H_1 H_2 \subseteq G$ is clear, since if $\sigma = \tau_1 \tau_2 \in H_1 H_2$, then each τ_i is an automorphism of K that fixes $E_i \supseteq \mathbb{Q}$, so each τ_i fixes $\mathbb{Q}$ and thus σ fixes $\mathbb{Q}$.
That it is a subgroup follows from the fact that elements commute. (?)
To see this, let $\sigma = \sigma_1 \sigma_2 \in H_1 H_2$.
Note that $\sigma_1(e) = e$ for all $e \in E_1$ by definition, since H_1 fixes E_1, and $\sigma_2(e) \in E_1$ (?).
Then

$$\sigma_1(e) = e \quad \forall e \in E_1 \implies \sigma_1(\sigma_2(e)) = \sigma_2(e)$$

and substituting $e = \sigma_1(e)$ on the RHS yields

$$\sigma_1 \sigma_2(e) = \sigma_2 \sigma_1(e),$$

where a similar proof holds for $e \in E_2$ and thus for arbitrary $x \in E_1 E_2$.

1.11.3 c

By the Galois correspondence, the subgroup $H_1 H_2 \leq G$ will correspond to an intermediate field E such that $K/E/\mathbb{Q}$ and E is the fixed field of $H_1 H_2$.
But if $\sigma \in H_1 H_2$, then $\sigma = \tau_1 \tau_2$ where τ_i is an automorphism of K that fixes E_i, and so $\sigma(x) = x \iff \tau_1 \tau_2(x) = x \iff \tau_2(x) = x \ \& \ \tau_1(x) = x \iff x \in E_1 \bigcap E_2$.

1.12 Fall 2017 #3

Let F be a field. Let $f(x)$ be an irreducible polynomial in $F[x]$ of degree n and let $g(x)$ be any polynomial in $F[x]$. Let $p(x)$ be an irreducible factor (of degree m) of the polynomial $f(g(x))$.

Prove that n divides m. Use this to prove that if r is an integer which is not a perfect square, and n is a positive integer then every irreducible factor of $x^{2n} - r$ over $\mathbb{Q}[x]$ has even degree.

1.13 Fall 2017 #4

(a) Let $f(x)$ be an irreducible polynomial of degree 4 in $\mathbb{Q}[x]$ whose splitting field K over $\mathbb{Q}$ has Galois group $G = S_4$.

Let θ be a root of $f(x)$. Prove that $\mathbb{Q}[\theta]$ is an extension of $\mathbb{Q}$ of degree 4 and that there are no intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}[\theta]$.

(b) Prove that if K is a Galois extension of $\mathbb{Q}$ of degree 4, then there is an intermediate subfield between K and $\mathbb{Q}$.

1.14 Spring 2017 #7

Let F be a field and let $f(x) \in F[x]$.

a. Define what a splitting field of $f(x)$ over F is.

b. Let F now be a finite field with q elements. Let E/F be a finite extension of degree $n > 0$. Exhibit an explicit polynomial $g(x) \in F[x]$ such that E/F is a splitting field of $g(x)$ over F. Fully justify your answer.

c. Show that the extension E/F in (b) is a Galois extension.

1.15 Spring 2017 #8

a. Let K denote the splitting field of $x^5 - 2$ over $\mathbb{Q}$. Show that the Galois group of $K/\mathbb{Q}$ is isomorphic to the group of invertible matrices

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \quad \text{where} \quad a \in \mathbb{F}_5^\times \text{ and } b \in \mathbb{F}_5.$$

b. Determine all intermediate fields between K and $\mathbb{Q}$ which are Galois over $\mathbb{Q}$.

1.16 Fall 2016 #4

Set $f(x) = x^3 - 5 \in \mathbb{Q}[x]$.

a. Find the splitting field K of $f(x)$ over $\mathbb{Q}$.

b. Find the Galois group G of K over $\mathbb{Q}$.

c. Exhibit explicitly the correspondence between subgroups of G and intermediate fields between $\mathbb{Q}$ and K.

1.17 Spring 2016 #2

Let $K = \mathbb{Q}[\sqrt{2} + \sqrt{5}]$.

a. Find $[K : \mathbb{Q}]$.

b. Show that $K/\mathbb{Q}$ is Galois, and find the Galois group G of $K/\mathbb{Q}$.

c. Exhibit explicitly the correspondence between subgroups of G and intermediate fields between $\mathbb{Q}$ and K.

1.18 Spring 2016 #6

Let K be a Galois extension of a field F with $[K : F] = 2015$. Prove that K is an extension by radicals of the field F.

1.19 Fall 2015 #5

Let $u = \sqrt{2+\sqrt{2}}$, $v = \sqrt{2-\sqrt{2}}$, and $E = \mathbb{Q}(u)$.

a. Find (with justification) the minimal polynomial $f(x)$ of u over $\mathbb{Q}$.

b. Show $v \in E$, and show that E is a splitting field of $f(x)$ over $\mathbb{Q}$.

c. Determine the Galois group of E over $\mathbb{Q}$ and determine all of the intermediate fields F such that $\mathbb{Q} \subset F \subset E$.

1.20 Fall 2015 #6

a. Let G be a finite group. Show that there exists a field extension K/F with $\mathrm{Gal}(K/F) = G$.

You may assume that for any natural number n there is a field extension with Galois group S_n.

b. Let K be a Galois extension of F with $|\mathrm{Gal}(K/F)| = 12$. Prove that there exists an intermediate field E of K/F with $[E : F] = 3$.

c. With K/F as in (b), does an intermediate field L necessarily exist satisfying $[L : F] = 2$? Give a proof or counterexample.

1.21 Spring 2015 #2

Let $\mathbb{F}$ be a finite field.

a. Give (with proof) the decomposition of the additive group $(\mathbb{F}, +)$ into a direct sum of cyclic groups.

b. The *exponent* of a finite group is the least common multiple of the orders of its elements. Prove that a finite abelian group has an element of order equal to its exponent.

c. Prove that the multiplicative group $(\mathbb{F}^\times, \cdot)$ is cyclic.

1.22 Spring 2015 #5

Let $f(x) = x^4 - 5 \in \mathbb{Q}[x]$.

a. Compute the Galois group of f over $\mathbb{Q}$.
b. Compute the Galois group of f over $\mathbb{Q}(\sqrt{5})$.

1.23 Fall 2014 #1

Let $f \in \mathbb{Q}[x]$ be an irreducible polynomial and L a finite Galois extension of $\mathbb{Q}$. Let $f(x) = g_1(x)g_2(x)\cdots g_r(x)$ be a factorization of f into irreducibles in $L[x]$.

a. Prove that each of the factors $g_i(x)$ has the same degree.

b. Give an example showing that if L is not Galois over $\mathbb{Q}$, the conclusion of part (a) need not hold.

1.24 Fall 2014 #3

Consider the polynomial $f(x) = x^4 - 7 \in \mathbb{Q}[x]$ and let $E/\mathbb{Q}$ be the splitting field of f.

a. What is the structure of the Galois group of $E/\mathbb{Q}$?

b. Give an explicit description of all of the intermediate subfields $\mathbb{Q} \subset K \subset E$ in the form $K = \mathbb{Q}(\alpha), \mathbb{Q}(\alpha, \beta), \cdots$ where α, β, etc are complex numbers. Describe the corresponding subgroups of the Galois group.

1.25 Spring 2014 #3

Let $F \subset C$ be a field extension with C algebraically closed.

a. Prove that the intermediate field $C_{\text{alg}} \subset C$ consisting of elements algebraic over F is algebraically closed.

b. Prove that if $F \longrightarrow E$ is an algebraic extension, there exists a homomorphism $E \longrightarrow C$ that is the identity on F.

1.26 Spring 2014 #4

Let $E \subset \mathbb{C}$ denote the splitting field over $\mathbb{Q}$ of the polynomial $x^3 - 11$.

a. Prove that if n is a squarefree positive integer, then $\sqrt{n} \notin E$.

Hint: you can describe all quadratic extensions of $\mathbb{Q}$ contained in E.

b. Find the Galois group of $(x^3 - 11)(x^2 - 2)$ over $\mathbb{Q}$.

c. Prove that the minimal polynomial of $11^{1/3} + 2^{1/2}$ over $\mathbb{Q}$ has degree 6.

1.27 Fall 2013 #5

Let L/K be a finite extension of fields.

a. Define what it means for L/K to be *separable*.

b. Show that if K is a finite field, then L/K is always separable.

c. Give an example of a finite extension L/K that is not separable.

1.28 Fall 2013 #6

Let K be the splitting field of $x^4 - 2$ over $\mathbb{Q}$ and set $G = \text{Gal}(K/\mathbb{Q})$.

a. Show that $K/\mathbb{Q}$ contains both $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt[4]{2})$ and has degree 8 over $\mathbb{Q}/$

b. Let $N = \text{Gal}(K/\mathbb{Q}(i))$ and $H = \text{Gal}(K/\mathbb{Q}(\sqrt[4]{2}))$. Show that N is normal in G and $NH = G$.

Hint: what field is fixed by NH?

c. Show that $\text{Gal}(K/\mathbb{Q})$ is generated by elements σ, τ, of orders 4 and 2 respectively, with $\tau\sigma\tau^{-1} = \sigma^{-1}$.

Equivalently, show it is the dihedral group of order 8.

d. How many distinct quartic subfields of K are there? Justify your answer.

1.29 Spring 2013 #7

Let $f(x) = g(x)h(x) \in \mathbb{Q}[x]$ and $E, B, C/\mathbb{Q}$ be the splitting fields of f, g, h respectively.

a. Prove that $\mathrm{Gal}(E/B)$ and $\mathrm{Gal}(E/C)$ are normal subgroups of $\mathrm{Gal}(E/\mathbb{Q})$.

b. Prove that $\mathrm{Gal}(E/B) \bigcap \mathrm{Gal}(E/C) = \{1\}$.

c. If $B \bigcap C = \mathbb{Q}$, show that $\mathrm{Gal}(E/B)\mathrm{Gal}(E/C) = \mathrm{Gal}(E/\mathbb{Q})$.

d. Under the hypothesis of (c), show that $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathrm{Gal}(E/B) \times \mathrm{Gal}(E/C)$.

e. Use (d) to describe $\mathrm{Gal}(\mathbb{Q}[\alpha]/\mathbb{Q})$ where $\alpha = \sqrt{2} + \sqrt{3}$.

1.30 Spring 2013 #8

Let F be the field with 2 elements and K a splitting field of $f(x) = x^6 + x^3 + 1$ over F. You may assume that f is irreducible over F.

a. Show that if r is a root of f in K, then $r^9 = 1$ but $r^3 \neq 1$.

b. Find $\mathrm{Gal}(K/F)$ and express each intermediate field between F and K as $F(\beta)$ for an appropriate $\beta \in K$.

1.31 Fall 2012 #3

Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 5. Assume that f has all but two roots in $\mathbb{R}$. Compute the Galois group of $f(x)$ over $\mathbb{Q}$ and justify your answer.

1.32 Fall 2012 #4

Let $f(x) \in \mathbb{Q}[x]$ be a polynomial and K be a splitting field of f over $\mathbb{Q}$. Assume that $[K : \mathbb{Q}] = 1225$ and show that $f(x)$ is solvable by radicals.

1.33 Spring 2012 #1

Suppose that $F \subset E$ are fields such that E/F is Galois and $|\mathrm{Gal}(E/F)| = 14$.

a. Show that there exists a unique intermediate field K with $F \subset K \subset E$ such that $[K : F] = 2$.

b. Assume that there are at least two distinct intermediate subfields $F \subset L_1, L_2 \subset E$ with $[L_i : F] = 7$. Prove that $\mathrm{Gal}(E/F)$ is nonabelian.

1.34 Spring 2012 #4

Let $f(x) = x^7 - 3 \in \mathbb{Q}[x]$ and $E/\mathbb{Q}$ be a splitting field of f with $\alpha \in E$ a root of f.

a. Show that E contains a primitive 7th root of unity.
b. Show that $E \neq \mathbb{Q}(\alpha)$.

1.35 Fall 2019 Midterm #6

Compute the Galois group of $f(x) = x^3 - 3x - 3 \in \mathbb{Q}[x]/\mathbb{Q}$.

1.36 Fall 2019 Midterm #7

Show that a field k of characteristic $p \neq 0$ is perfect $\iff$ for every $x \in k$ there exists a $y \in k$ such that $y^p = x$.

1.37 Fall 2019 Midterm #8

Let k be a field of characteristic $p \neq 0$ and $f \in k[x]$ irreducible. Show that $f(x) = g(x^{p^d})$ where $g(x) \in k[x]$ is irreducible and separable. Concluded that every root of f has the same multiplicity p^d in the splitting field of f over k.

1.38 Fall 2019 Midterm #9

Let $n \geq 3$ and ζ_n be a primitive nth root of unity. Show that $[\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}] = \varphi(n)/2$ for φ the totient function. 10. Let L/K be a finite normal extension - Show that if L/K is cyclic and E/K is normal with $L/E/K$ then L/E and E/K are cyclic. - Show that if L/K is cyclic then there exists exactly one extension E/K of degree n with $L/E/K$ for each divisor n of $[L : K]$.