

Galois Theory

Robert F. Coleman

Final

1. True/False If false, give a counter-example.

(i) The Galois group of a finite normal separable extension of a field of characteristic p has order relatively prime to p .

False, $\mathbf{F}_{p^p}/\mathbf{F}_p$.

(ii) Every finite normal extension of a field F is a splitting field of a polynomial in $F[x]$.

True.

(iii) If K is an extension of F and $K = F(\alpha_1, \dots, \alpha_n)$, the transcendence degree of K/F is the maximum number of elements that are algebraically independent over F in $\{\alpha_1, \dots, \alpha_n\}$.

True.

(iv) If K/F is a normal extension of degree at least 5, $\text{Gal}(K/F)$ is not solvable.

False $\mathbf{Q}(\mu_7)/\mathbf{Q}$.

(v) The intersection of normal extensions is a normal extension.

True.

(vi) If F/K and L/K are finite normal separable extensions such that $\text{Gal}(F/K)$ is not isomorphic to a quotient of $\text{Gal}(L/K)$, then F/K is not a subextension of L/K .

True

(vii) Any two finite fields are isomorphic to subfields of some third finite field.

False \mathbf{F}_2 and \mathbf{F}_3 .

(viii) The additive group of a finite field is cyclic.

False \mathbf{F}_4

(ix) Every finite Abelian group is isomorphic to the Galois group of infinitely many finite normal extensions of \mathbf{Q} .

False (e) is the Galois group of only one extension.

(x) The extension $\mathbf{Q}(\sqrt{-1}, \sqrt{2})/\mathbf{Q}$ has three subextensions.

True (It actually has 5.)

(ix) and (x) were sneakier than I intended so I only took off one point for a wrong answer.

(xi) Every field has a normal extension of degree 2.

False \mathbf{C} .

(xii) The intersection of a quadratic extension and a cubic extension of a field K is K .

True

(xiii) A normal extension with a solvable Galois group is a radical extension.

False $\mathbf{Q}(\zeta + \bar{\zeta})/\mathbf{Q}$ where ζ is a complex primitive 7-th root of unity.

(xiv) A non-normal extension of a non-normal extension is not normal.

True

(xv) Two extensions of \mathbf{Q} in \mathbf{C} are isomorphic if and only if they are equal.

False

Suppose K/F is finite normal and separable. Let $G = \text{Gal}(K/F)$.

(xvi) The number of subextensions of F in K is finite.

True

(xvii) If G is Abelian, every subextension of F in K is normal over F .

True

(xviii) If G is solvable, there exists a positive integer d and $\{\alpha_1, \dots, \alpha_n\} \subseteq K$ such that $\alpha_i^d \in F$ and $K = F(\alpha_1, \dots, \alpha_n)$.

False Use the example in (xiii) above.

What meant to say was, If G is solvable, there exists an extension L of K , a positive integer d and $\{\alpha_1, \dots, \alpha_n\} \subseteq L$ such that $\alpha_i^d \in F$ and $L = F(\alpha_1, \dots, \alpha_n)$. Is this true?

(xix) If K is finite, the number of subextensions of F in K is at most $\log_{|F|} |K|$.

True

(xx) If $f(x)$ is an irreducible polynomial over F with three distinct roots in K , α, β, γ , $F(\alpha, \beta)$ is isomorphic to $F(\beta, \gamma)$.

False $x^4 - 2$.

2. Find an extension of \mathbf{Q} with Galois group $C_5 \times C_5$.

We know $\text{Gal}(\mathbf{Q}(\mu_{11 \cdot 31})/\mathbf{Q}) \cong (\mathbf{Z}/11\mathbf{Z})^* \times (\mathbf{Z}/31\mathbf{Z})^*$ and $(\mathbf{Z}/11\mathbf{Z})^*$ is cyclic of order 10 while $(\mathbf{Z}/31\mathbf{Z})^*$ is cyclic of order 30. Let A be the subgroup of $(\mathbf{Z}/11\mathbf{Z})^*$ of order 2 and B be the subgroup of $(\mathbf{Z}/31\mathbf{Z})^*$ of order 6. Then $A \times B$ is a normal subgroup of $(\mathbf{Z}/11\mathbf{Z})^* \times (\mathbf{Z}/31\mathbf{Z})^*$ and $((\mathbf{Z}/11\mathbf{Z})^* \times (\mathbf{Z}/31\mathbf{Z})^*)/(A \times B) \cong C_5 \times C_5$. It follows that $A \times B$ is isomorphic to a normal subgroup H of $\text{Gal}(\mathbf{Q}(\mu_{11 \cdot 31})/\mathbf{Q})$ and $\text{Gal}(\mathbf{Q}(\mu_{11 \cdot 31})^H/\mathbf{Q}) \cong C_5 \times C_5$.

3. Show the Galois group G of $f(x) = x^3 + pqa x + pq^2 b$ is S_3 , where p and q are distinct prime numbers, and a and b are integers, such that $(qb, 2ap) = 1$.

We know G is isomorphic to a subgroup of S_3 . Since f is irreducible by Eisenstein, $3||G|$. The discriminant of f is

$$-4(pqa)^3 - 27(pq^2b)^2 = q^3(-4(pa)^3 - 27q(pb)^2).$$

Since q doesn't divide $(-4(pa)^3 - 27q(pb)^2)$ $((-4(pa)^3 - 27q(pb)^2) \equiv -4(pa)^3 \pmod{q})$ D is not a square so $2||G|$ and $G \cong S_3$.

4. Let p be a prime and $r \geq 1$ an integer. Show $x^{p^r} - x$ is the product of all the monic irreducible polynomials over \mathbf{F}_p of degree dividing r .

Let $g(x) =: x^{p^r} - x$ and suppose

$$g(x) = \prod_i f_i(x)$$

be its factorization into monic irreducibles. Because $g'(x) = -1$ the f_i are all distinct. Now \mathbf{F}_{p^r} is a splitting field of g so contains a splitting field F_i of f_i . Since $\deg f_i | [F_i : \mathbf{F}_p]$ and $[F_i : \mathbf{F}_p] | [F_{p^r} : \mathbf{F}_p] = r$, $\deg f_i | r$.

On the other hand, if f is a monic irreducible whose degree d divides r , $\mathbf{F}_p[x]/(f(x))$ is a field of degree d over \mathbf{F}_p so isomorphic to a subfield of \mathbf{F}_{p^r} . Thus if α is a root of f , $\alpha^r = \alpha$ so $f(x) | g(x)$ and so $f = f_i$ for some i .

5. Suppose F and K are normal (possibly infinite) extensions of \mathbf{Q} in \mathbf{C} . Show $\text{Gal}(\mathbf{Q}(F \cup K)/\mathbf{Q})$ injects into $\text{Gal}(F/\mathbf{Q}) \times \text{Gal}(K/\mathbf{Q})$.

6. Suppose K is a finite, separable, normal extension of a field F and A and B are normal extensions of F in K . Show the smallest field L in K containing A and B is a normal extension of F . (Hint: Show $\text{Gal}(K/L) = \text{Gal}(K/A) \cap \text{Gal}(K/B)$.)

7. Suppose K/F is normal and separable, $G =: \text{Gal}(K/F)$ is a finite simple group which contains a non-trivial subgroup H of index k . Show K is the splitting field over F of a polynomial of degree k .

Let $f(x)$ be the minimal polynomial for a primitive element of K^H . Then K contains a splitting field L of f . Since L/F is normal, $\text{Gal}(K/L)$ is normal. Since, G is simple and $L \neq F$ $L = K$.

8. Let $g(E) = E^6 + 2E^3 - 1$ and K be a splitting field of g over \mathbf{Q} . Determine $G = \text{Gal}(K/\mathbf{Q})$. Find all subfields of K .

Let α be a root of g . Then $K = \mathbf{Q}(\alpha, j)$, $[K : \mathbf{Q}] = 12$ and $\beta_i = j^i \alpha - 1/j^i \alpha$ is a root of $f(x) = x^3 + 3x - 2$. Let $A = \mathbf{Q}(j) = \mathbf{Q}(\sqrt{-3})$. Now K contains the splitting field L of f and $K = \mathbf{Q}(A, K) = K(j)$. So G injects into $\text{Gal}(A/\mathbf{Q}) \times \text{Gal}(K/Q) \cong C_2 \times S_3$. Since $|C_2 \times S_3| = 12$,

$$G \cong C_2 \times S_3.$$

The subfields of K correspond to subgroups of G . These are

$$\{(e, h) : h \in H\} \quad \{(a, h) : a \in C_2, h \in H\}$$

where H is a subgroup of S_3 and $((\tau, \gamma))$ where $(\tau) = C_2$ and $\gamma \in S_3$ has order 2.

This is a complete solution but you may want to see these fields more explicitly. They are

$$\mathbf{Q}(j), \mathbf{Q}(j, \sqrt{2}), \{\mathbf{Q}(j, \beta_i) : 0 \leq i \leq 2\}, K \quad (e), \mathbf{Q}(\sqrt{-6}), \{\mathbf{Q}(\beta_i) : 0 \leq i \leq 2\}, L$$

and $\{\mathbf{Q}(j^i \alpha) : 0 \leq i \leq 2\}$.

9. Determine all irreducible cubics over \mathbf{F}_3 .

First, a cubic is irreducible if it has no roots. Also there are $(|\mathbf{F}_{27}| - |\mathbf{F}_3|)/3 = 8$ monic cubic irreducibles over \mathbf{F}_3 . Suppose $f(x) = x^3 + ax^2 + bx + c$ is irreducible. Then $c \neq 0$,

$$1 + a + b + c \neq 0 \text{ and } -1 + a - b + c \neq 0.$$

Thus when $c = 1$, $a \neq b$ and $a + b \neq 1$. These are

$$x^3 - x^2 + 1, x^3 - x + 1, x^3 + x^2 - x + 1 \text{ and } x^3 - x^2 + x + 1.$$

If f is irreducible $-f(-x)$ is irreducible. Thus the remaining monic irreducibles are

$$x^3 + x^2 - 1, x^3 - x - 1, x^3 - x^2 - x - 1 \text{ and } x^3 + x^2 + x - 1.$$

10. Let $F_n(x) = \sum_{i=0}^n x^i/i!$. Show the Galois group G of the splitting field of $F_n(x)$ over \mathbf{Q} is isomorphic to a subgroup of A_n if $4|n$. (Hint: $F'_n(x) = F_n(x) - x^n/n!$)

We know G is isomorphic to a subgroup of A_n if

$$D =: (-1)^{n(n-1)/2} (n!)^n \prod_{\alpha} F'_n(\alpha) \in \mathbf{Q}^2$$

where α runs over the roots of $F_n(x)$. Now

$$D = (-1)^{n(n-1)/2} (n!)^n \prod_{\alpha} (-\alpha^n/n!) = (-1)^{n(n+1)/2} \left(\prod_{\alpha} \alpha\right)^n.$$

As $\prod_{\alpha} \alpha = (-1)^n n!$,

$$D = (-1)^{n(3n+1)/2} (n!)^n = ((n!)^{n/2})^2 \in \mathbf{Q}^2,$$

since $4|n$.