1 Spring 2002 – Galois Theory

Problem 1.1. Let $\mathbf{F}_7$ be the field with 7 elements and let L be the splitting field of the polynomial $X^{171} - 1 = 0$ over $\mathbf{F}_7$. Determine the degree of L over $\mathbf{F}_7$, explaining carefully the principles underlying your computation.

Solution: Note that $7^3 = 49 \cdot 7 = 343$, so

$$[x \in (\mathbf{F}_{7^3})^\times] \Longrightarrow [x^{342} - 1 = 0],$$

since $(\mathbf{F}_{7^3})^\times$ is a multiplicative group of order 342. Also, $\mathbf{F}_{7^3}$ contains all the roots of $x^{342} - 1 = 0$ since the number of roots of a polynomial cannot exceed its degree (by the Division Algorithm). Next note that $171 \cdot 2 = 342$, so

$$[x^{171} - 1 = 0] \Rightarrow [x^{171} = 1] \Rightarrow [x^{342} - 1 = 0].$$

This implies that all the roots of $X^{171} - 1$ are contained in $\mathbf{F}_{7^3}$ and so $L \subset \mathbf{F}_{7^3}$ since L can be obtained from $\mathbf{F}_7$ by adjoining all the roots of $X^{171} - 1$. We therefore have

$$\underbrace{\mathbf{F}_{7^3} \text{——} L \text{——} \mathbf{F}_7}_{3}$$

and so $L = \mathbf{F}_{7^3}$ or $L = \mathbf{F}_7$ since $3 = [\mathbf{F}_{7^3} : \mathbf{F}_7] = [\mathbf{F}_{7^3} : L][L : \mathbf{F}_7]$ is prime. Next if $\alpha \in (\mathbf{F}_{7^3})^\times$, then α^2 is a root of $X^{171} - 1$. Also, $(\mathbf{F}_{7^3})^\times$ is cyclic and hence isomorphic to $\mathbb{Z}_{7^3} = \{0, 1, 2, \ldots, 342\}$, so the map $\alpha \mapsto \alpha^2$ on $\mathbf{F}_{7^3}$ has an image of size bigger than 7:

$$2\alpha = 2\beta \Leftrightarrow 2(\alpha - \beta) = 0 \text{ in } \mathbb{Z}_{7^3} \Leftrightarrow \alpha - \beta = 171.$$

We therefore conclude that $X^{171} - 1$ has more than 7 distinct roots and hence $L = \mathbf{F}_{7^3}$. □

- Splitting Field: A splitting field of a polynomial $f \in K[x]$ (K a field) is an extension L of K such that f decomposes into linear factors in $L[x]$ and L is generated over K by the roots of f.
- Irreducible Polynomial: An irreducible polynomial is a polynomial of positive degree that does not factor into two polynomials of positive degree.
- Separable Polynomial: A polynomial $f \in K[x]$ is called separable if it does not have multiple roots in any extension of K.
- Irreducible ⇒ Separable: If f is an irreducible polynomials over the following fields then f is separable:

  (i) Field of zero characteristic

  (ii) Field of characteristic $p \nmid \deg f$

  (iii) Finite field

- Field Extensions: If L/K is a field extension, then L can be regarded as a vector space over K. The dimension of L over K is also called the degree of the extension and denoted $[L : K]$.
- Multiplicativity of Degree: If L is a finite extension over K and M is a finite extension over L, then M is a finite extension over K and
$$[M : K] = [M : L][L : K].$$
- Finite Fields: For any prime p and any natural number n, there exists a field with p^n elements which is unique up to isomorphism. These are the only finite fields.
- Cyclicity of $F^\times$: If F is a finite field, then $F^\times$ is cyclic (Use the Fundamental Theorem of Finitely Generated Abelian Groups I and consider the biggest invariant factor n_k and the polynomial $x^{n_k} - 1$).
- Euler Function: The Euler function ϕ assigns to each positive integer n the number $\phi(n)$ of integers k such that $1 \leq k \leq n$ and $(k, n) = 1$.
  - A cyclic group of order n has $\phi(n)$ generators.
  - $(k, n) = 1$ if and only if k is a unit in the ring $\mathbb{Z}_n$.

Problem 1.2. Show that there exists a Galois extension of $\mathbf{Q}$ of degree p for each prime p. State precisely all results which are needed to justify your answer.

Solution: The solution that was here before was incorrect. $x^p - a$ is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion (and hence separable since $\mathbb{Q}$ has characteristic 0) for any a which is square–free. Now let E be the splitting field of such an $x^p - a$. □

- Roots of Unity: The (complex) n^{th} roots unity form a cyclic group C_n. The generators of C_n are the n^{th} primitive roots of unity. These are roots of the form $\mu_k = e^{(2\pi k/n)i}$ for $(n, k) = 1$.
- Algebraic/Transcendental Elements: Let E/F be fields. An element $u \in E$ is algebraic over F if there exists $f \in F[x]$ such that $f(u) = 0$; otherwise u is transcendental. If u is transcendental over F, then
$$F[u] \cong F[x], \text{ where } F[u] = \{f(u) \mid f \in F[x]\}$$
- Irreducible Polynomial $\rightsquigarrow$ Finite Extension: If $h \in F[x]$ is irreducible of degree n:
  (i) $x + (h)$ is a root of h in $E = F[x]/(h) = F[x + (h)]$
  (ii) E is a field. (This is NOT true if h is not irreducible!)
  (iii) E/F is finite and $[E : F] = n$.

- Minimal Polynomial: If $u \in E$ is algebraic over F, then

$$I \equiv \{f \in F[x] \mid f(u) = 0\}$$

is an ideal in the PID $F[x]$. The generator of I is called the minimal polynomial of u and denoted m_u.

(i) m_u is irreducible.

(ii) The degree of m_u is called the degree of u over F.

- Algebraic $\Longleftrightarrow$ Finite: An element $u \in E$ is algebraic over F if and only if $F[u]$ is a finite–dimensional vector space over F. In this case $F[u]$ is a field and

$$[F[u] : F] = deg(m_u).$$

More precisely, we have

$$F[u] \cong F[x]/(m_u)$$

and

$$F[u] \cong F(u).$$

As a consequence, every finite field extension is algebraic (E/F is algebraic if every element of E is algebraic over F: E/F finite implies that for all $u \in E$, $E[u]$ is finite and hence u is algebraic).

- Cyclotomic Extension (prime case): Let p be a prime number. Consider the polynomial over $\mathbb{Q}$

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1) \equiv (x-1)\Phi_p,$$

the roots of which are the p^{th} roots of unity. If ξ is a primitive root of unity, then $\mathbb{Q}(\xi)$ would be a splitting field of Φ_p (since it will contain all p^{th} roots of unity). Since p is prime, any root of Φ_p is a primitive root of unity. Φ_p is irreducible:

Over $\mathbb{Z}_p[x]$, $x^p - 1 = (x-1)^p$, so $[\Phi_p]_p = (x-1)^{p-1}$. If $\Phi_p = gh$, then $[\Phi_p]_p = [g]_p[h]_p = (x-1)^k(x-1)^l$, with $k, l > 0$, and $k + l = p - 1$. But then $[g(1)]_p = [g]_p(1) = 0$ and similarly $[h(1)]_p = 0$ so that $\Phi_p(1) = g(1)h(1)$ is divisible by p^2, which is impossible sinec $\Phi_p(1) = p$.

From this we conclude that $[\mathbb{Q}(\xi) : \mathbb{Q}] = p - 1$.

- Automorphism Groups: Let E/F be fields. The automorphisms of E over F (i.e. automorphisms of E which fixes F) form a group under composition denoted $\mathrm{Aut}_F E$.
  - $|\mathrm{Aut}_F E| \leq [E : F]$

– $E^G = F$ if and only if $|G| = [E : F]$, where $G \subset \mathrm{Aut}_F E$ is a subgroup and

$$E^G = \{u \in E \mid \sigma(u) = u, \forall \sigma \in G\}.$$

- Galois Extension: A finite extension E of a field F is a Galois extension if

$$|\mathrm{Aut}_F E| = [E : F].$$

  $\mathrm{Aut}_E F$ is called the Galois group of the extension E and is denoted $\mathrm{Gal}(E/F)$.

- Separable $\rightsquigarrow$ Galois: Let $f \in F[x]$ be such that all its irreducible factors are separable. Then its splitting field is a Galois extension of F.

- Galois Correspondence: Let E/F be Galois and let $G = \mathrm{Gal}(E/F)$. We have

$$\Phi : \{\text{subfields of } E \text{ containing } F\} \longrightarrow \{\text{subgroups of } G\} : K \mapsto G_K,$$

  where $G_K = \{g \in G \mid g \mid_K = \mathrm{id}\} \subset G$, is a bijection, with inverse

$$\Psi : \{\text{subgroups of G}\} \longrightarrow \{\text{subfields of } E \text{ containing } F\} : H \mapsto E^H,$$

  where $E^H = \{\alpha \in E \mid \sigma(\alpha) = \alpha, \forall h \in H\} \subset F$. Also

$$|G_K| = [E : K],$$

$$[E : E^H] = |H|.$$

  Finally, a Galois extension of F contained in E corresponds to a normal subgroup of G and vice versa.

Problem 1.3. Let $\alpha = \sqrt{i+2}$ where $i = \sqrt{-1}$.

(a) Compute the minimal polynomial of α over $\mathbf{Q}$.

(b) Let F be the splitting field and compute the degree of F over $\mathbf{Q}$;

(c) Show that F contains 3 quadratic extensions of $\mathbf{Q}$;

(d) Use this information to determine the Galois group.

Solution: (a) $\alpha^2(\alpha^2 - 4) = (i+2)(i-2) = -5$, so α is a root of

$$f \equiv x^4 - 4x^2 + 5.$$

We claim f is irreducible and hence $f = m_{\mathbb{Q}}(\alpha)$: Making a change of variable $y = x^2$, we know that $(2+i)$ is a root of the polynomial $y^2 - 4y + 5$, so it must be the case that its complex conjugate $(2-i)$ is also a root, so

$$f = (x^2 - (2+i))(x^2 + (2-i)) = (x - (\sqrt{2+i}))(x + (\sqrt{2+i})(x - (\sqrt{2-i}))(x + (\sqrt{2-i}).$$

If $f = gh$, then the degree of g and h must add up to 4, but if say g is linear, then it is clear from the above that $g \notin \mathbb{Q}[x]$, so it must be the case that both g and h are quadratic. But it is equally easy to see that any product of two linear factors also does not lie in $\mathbb{Q}[x]$.

(b) The splitting field of $m_{\mathbb{Q}}(\alpha)$ can be found by adjoining all the roots, hence is equal to

$$K \equiv \mathbb{Q}(\sqrt{2+i}, \sqrt{2-i}).$$

We have that $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{2+i})][\mathbb{Q}(\sqrt{2+i}) : \mathbb{Q}]$. By (a), the latter is equal to the degree of $m_{\mathbb{Q}}(\alpha)$ and hence is 4. Next observe that $K = [\mathbb{Q}(\sqrt{2+i})](\sqrt{2-i})$, so we look for the minimal polynomial of $\sqrt{2-i}$ over $\mathbb{Q}(\sqrt{2+i})$. To this end note that $(\sqrt{2+i})(\sqrt{2-i}) = \sqrt{5}$ so $\sqrt{2-i}$ is a root of

$$((\sqrt{2+i})x)^2 - 5 = ((\sqrt{2+i})x - \sqrt{5})((\sqrt{2+i})x + \sqrt{5}),$$

which is irreducible. So $[K : \mathbb{Q}(\sqrt{2+i})] = 2$ and $[K : \mathbb{Q}] = 8$.

(c) We again note that $(\sqrt{2+i})(\sqrt{2-i}) = \sqrt{5}$ and $\frac{1}{2}[(\sqrt{2+i})^2 - (\sqrt{2-i})^2] = i$, so that $\sqrt{5}$, $i\sqrt{5}$ and i are all in K. These are all quadratic extensions of $\mathbb{Q}$ since they satisfy polynomials $x^2-5 = (x-\sqrt{5})(x+\sqrt{5})$, $x^2+5 = (x-i\sqrt{5})(x+i\sqrt{5})$ and $x^2+1 = (x-i)(x+i)$, respectively, all of which are irreducible of degree 2 (they are irreducible since they clearly have no root in $\mathbb{Q}$).

(d) $m_{\mathbb{Q}}(\alpha)$ is separable so $K/\mathbb{Q}$ is Galois. Let $G = \mathrm{Gal}(K/\mathbb{Q})$. Then $|G| = [K : \mathbb{Q}] = 8$. By part (c), there are 3 quadratic extensions. In addition, all 3 extensions are in fact also Galois over $\mathbb{Q}$ (since they are all splitting fields of the corresponding minimal polynomials, all of which are separable). By the Galois Correspondence, these correspond to 3 distinct normal subgroups of G of index 2 (hence order 4). There are 3 abelian groups of order 8: $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, none of which has 3 subgroups of order 4. This leaves us with D_4 and Q_8. The quarternion group has only one subgroup of order 2, namely $\langle -1 \rangle$, but again by the Galois Correspondence, G has at least 2 subgroups of order 2, corresponding to $\mathbb{Q}(\sqrt{2+i})$ and $\mathbb{Q}(\sqrt{2-i})$. So we are finally left to conclude that $G = D_4$. □

- Irreducibility – Degree 2 or 3: A polynomial of degree 2 or 3 is reducible if and only if it has a root in the field in question (hence irreducible if it has no root).
- Polynomials Over $\mathbb{Q} \rightsquigarrow$ Galois: The splitting field of any polynomial over $\mathbb{Q}$ is Galois.

2 Winter 2002 – Fields

Problem 2.1. The discriminant of the special cubic polynomial $f(x) = x^3 + ax + b$ is given by $-4a^3 - 27b^2$. Determine the Galois group of the splitting field of $x^3 - x + 1$ over

(a) $\mathbb{F}_3$, the field with 3 elements.

(b) $\mathbb{F}_5$, the field with 5 elements.

(c) $\mathbb{Q}$, the rational numbers.

Solution: (a) Since $x^3 - x + 1$ is a cubic, it is reducible if and only if it has a root. A quick check shows that it has no root in $\mathbb{F}_3$ so it is irreducible over $\mathbb{F}_3$, hence separable and generates a Galois extension of degree divisible by 3 over $\mathbb{F}_3$ (the extension generated by a single root has degree 3). Therefore there are only two possibilities for the Galois group: A_3 or S_3. The Galois group is A_3 if and only if the discriminant is the square of an element in $\mathbb{F}_3$ (the Galois group is contained in A_n if and only if each $\sigma \in G$ fixes $\sqrt{D}$ if and only if $\sqrt{D} \in F$ since F is the fixed field of the Galois group). In this case the discriminant is calculated to be

$$-4 \cdot (-1)^3 - 27 = -23 = 1 = 1^2 \text{ in } \mathbb{F}_3.$$

So the Galois group is indeed A_3. (Or just note that over a finite field all finite extensions are cyclic, so the Galois group cannot be S_3 since it is not cyclic.)

(b) In this case a check shows that 3 is a root of $x^3 - x + 1$ over $\mathbb{F}_5$ and there are no other roots. So the polynomial splits into a linear term and an irreducible quadratic term. This generates a quadratic extension and the Galois group is $\mathbb{Z}/2\mathbb{Z}$ (the order of the Galois group is equal to the degree of the extension).

(c) By the Rational Root Test, the only possible roots are ± 1 neither of which are roots, so $x^3 - x + 1$ is irreducible over $\mathbb{Q}$. The discriminant is -23 which is not a square in $\mathbb{Q}$, so the Galois group is S_3. □

- Polynomials Over Finite Fields $\rightsquigarrow$ Galois: The splitting field of any polynomial over a finite field is Galois (the splitting field of a polynomial f is the splitting field of the product of irreducible factors of f, which is separable).

- Characterization of Galois (Polynomial): An extension E/F is Galois if and only if E is the splitting field of some separable polynomial over F. If this is true, every irreducible polynomial in $F[x]$ which has a root in E is separable and has all its root in E.

- Characterization of Galois (Fixed Field): E/F is Galois if and only if the fixed field of $\mathrm{Aut}_E F$ is exactly F (in general it is bigger).

- Finite Extensions of Finite Fields are Cyclic: If F is a finite field, E/F is finite, then E/F is Galois with cyclic Galois group ($E^\times$ is cyclic so let θ be a generator, then $E = F(\theta)$ and $[E : F] = \deg(m_F(\theta))$. By uniqueness of finite fields and the irreducibility of $m_F(\theta)$, $m_F(\theta)$ must split in E, so that E/F is Galois. Assuming for

simplicity that $F = \mathbb{F}_p$, some prime p, we see that the Galois group is then generated by the Frobenius automorphism).

- Permutation of Roots: Let E/F be a field extension and $\alpha \in E$ algebraic over F. If $\sigma \in \mathrm{Aut}_E F$, then $\sigma(\alpha)$ is a root of $m_F(\alpha)$ (this is obvious since σ fixes F).
- $\mathrm{Gal}(E/F) \hookrightarrow S_n$: Let E/F be Galois. Then E is the splitting field of some separable $f \in F[x]$ with n roots. So any $\sigma \in \mathrm{Gal}(E/F)$ defines a permutation of the n roots.
- Discriminant: The discriminant of a polynomial with roots $x_1, \ldots, x_n$ is given by
$$D = \prod_{i<j} (x_i - x_j)^2.$$
- $\mathrm{Gal}(E/F) \hookrightarrow A_n$?: The Galois group G of $f \in F[x]$ (the Galois group of a polynomial over F is the Galois group of the splitting field of f over F) is a subgroup of A_n if and only if the discriminant $D \in F$ is the square of an element of F.
- Rational Root Test: Suppose $P(x) = a_n x^n + \cdots + a_1 x + a_0$ is a polynomial with integer coefficients, and $x = p/q$ is a rational root of $P(x)$, then
$$p \mid a_0 \text{ and } q \mid a_n.$$

Problem 2.2. A field extension $K/\mathbb{Q}$ is called *biquadratic* if it has degree 4 and if $K = \mathbb{Q}\sqrt{a}, \sqrt{b})$ for some $a, b \in \mathbb{Q}$.

(a) Show that a biquadratic extension is normal with Galois group $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and list all sub–extensions.

(b) Prove that if $K/\mathbb{Q}$ is a normal extension of degree 4 with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ then $K/\mathbb{Q}$ is biquadratic.

Solution: (a) First note that $a \neq b$ since otherwise $[K : \mathbb{Q}] = 2$, which implies that $f \equiv (x^2 - a)(x^2 - b)$ is separable. K is clearly the splitting field of f so $K/\mathbb{Q}$ is normal. Next note that $\mathbb{Q}(\sqrt{a}) \subset \mathbb{Q}(\sqrt{a}, \sqrt{b})$ corresponds to a subgroup $H \subset$ Gal $(K/\mathbb{Q})$ of order 2 by the Galois Correspondence. Similarly, by considering $\mathbb{Q}(\sqrt{b})$, there is another subgroup H' of order 2. $H \neq H'$ by the Galois Correspondence, so the Galois group cannot be $\mathbb{Z}/4\mathbb{Z}$ (which has only one subgroup of order 2). The only other possibility is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

To describe the subfields, let $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q})$, with
$$\sigma : \sqrt{a} \mapsto -\sqrt{a}, \sqrt{b} \mapsto \sqrt{b}$$
and
$$\tau : \sqrt{a} \mapsto \sqrt{a}, \sqrt{b} \mapsto -\sqrt{b}.$$

Then we see that $\sigma\tau = \tau\sigma$, so

$$\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma, \tau \mid \sigma^2 = \tau^2 = e, \tau\sigma = \sigma\tau\}.$$

The subfields are then

$$K^{\langle\sigma\rangle}, K^{\langle\tau\rangle}, K^{\langle\sigma\tau\rangle},$$

where $K^H = \{k \in K \mid \sigma(k) = k, \forall\sigma \in H\}$. These are equal to

$$\mathbb{Q}(\sqrt{b}), \mathbb{Q}(\sqrt{a}), \mathbb{Q}(\sqrt{ab}).$$

(b) By the Galois Correspondence, K contains two distinct quadratic extensions of $\mathbb{Q}$. These extensions are Galois since $\mathrm{Gal}(K/\mathbb{Q})$ is abelian so they must be splitting fields of irreducible quadratics, say $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{b})$ (here $a \neq b$ are the discriminants of the respective quadratics). $[\mathbb{Q}(\sqrt{a})](\sqrt{b})/\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}(\sqrt{a})$ has degree 1 or 2, but cannot be 1 since $a \neq b$, so $\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}$ has degree 4, which implies $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$. □

- Normal Extension: If E/F is algebraic, then E is a normal extension of F if E is the splitting field over F of a collection of polynomials $f \in F[x]$.

Problem 2.3. Let K be a finite extension of the field F with no proper intermediate subfields.

(a) If K/F is normal, show that the degree $[K : F]$ is a prime.

(b) Give an example to show that $[K : F]$ need not be prime if K/F is not normal, and justify your answer.

Solution: (a) Let E be the fixed field of $\mathrm{Aut}_F K$. Since there are no proper intermediate fields, $E = F$ or $E = K$. If $E = F$, then K/F is Galois and by the Galois Correspondence, each subgroup of the Galois group corresponds to a subfield and we are done by Cauchy's Theorem: If the degree is n not a prime, then $\exists p < n$, p prime, such that $p \mid n$, Cauchy's theorem says there is an element g of order p, but then the subfield corresponding to $\langle g\rangle$ would be a proper intermediate field, a contradiction.

If $E = K$, then $\mathrm{Aut}_F K$ is trivial. If F were a perfect field, then it is the case that any irreducible polynomial is separable. K/F is normal so it is the splitting field of a collection of polynomials over F. If f is one of the polynomials and α is a root of f which does not lie in F, then $F(\alpha) = K$, which implies that K is the splitting field of $m_F(\alpha)$, which is irreducible, hence separable, so that K/F is Galois and we are done as before. We may therefore assume that F is not perfect and so in particular $\mathrm{char}(F) = p$, where p is a prime.

With α as before, we have that $[K : F] = \deg(m_F(\alpha))$ and that α is the only root of f which does not lie in F (if β were another one, $F(\alpha) = F(\beta) = K$ and there would be an

automorphism of K sending α to β and fixing everything in F, but since $\mathrm{Aut}_F K$ is trivial, we conclude that $\alpha = \beta$). In the splitting field K, we have

$$m_F(\alpha) = (x-\alpha)(x-\alpha_1)\dots(x-\alpha_{n-1}).$$

Since $m_F(\alpha)$ is irreducible, none of the α_i's is in F, so it must be the case that $\alpha_i = \alpha, \forall i$. Therefore

$$m_F(\alpha) = (x-\alpha)^n.$$

This is a polynomial over F so in particular $\alpha^n \in F$. If $\alpha^k \in F$ for any $k < n$, then $m_F(\alpha) \mid (x^k - \alpha^k)$ would be of lower degree, a contradiction. Since

$$(x-\alpha)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \alpha^{n-k},$$

it must be the case that $p \mid \binom{n}{k}, 1 \le k < n$. In particular $p \mid n$ so $n = \gamma p$, some γ. Now we have

$$F \text{——} F(\alpha^p) \text{——} F(\alpha) = K.$$

Since there are no intermediate fields, $F(\alpha^p) = F(\alpha) = K$, so that $\gamma = 1$ and $[K:F] = p$.

(b) Let F be a field and let α be an element of order 4 over F such that the splitting field L of $m_F(\alpha)$ has S_4 as its Galois group. Let $E = F(\alpha)$, then $[E:F] = 4$ which is not prime and $[L:F] = 4! = 24$. We claim there is no intermediate field between E and F.

By Galois Correspondence, E corresponds to some subgroup $H \subset \mathrm{Gal}(L/F) \cong S_4$ such that $[S_4 : H] = 4$. Showing that there is no intermediate field is then equivalent to showing that $H \subset S_4$ is maximal. To this end, observe that A_4 has no subgroup of index 2: $|A_4| = 24/2 = 12$ so a subgroup of index 2 is a group of order 6, and hence isomorphic to either $\mathbb{Z}/6\mathbb{Z}$ or S_3. It cannot be S_3 since S_3 contains odd permutations. It also cannot be $\mathbb{Z}/6\mathbb{Z}$ since S_4 does not contain any element of order 6: First notice that S_4 does not contain any 6–cycles. Next if σ is an element of order 6, then writing $\sigma = \tau_1 \dots \tau_n$, where the τ_i are disjoint cycles, we see that the order of σ is equal to the least common multiple of the τ_i's. Cycles in S_4 can have lengths 1, 2, 3 or 4, so the only possibility is a cycle of length 2 and a cycle of length 3, but these cannot be disjoint (there are only 4 letters to permute), a contradiction.

Next observe that A_4 is the only subgroup of index 2 in S_4 (more generally, A_n is the only subgroup of index 2 in S_n: Notice that any subgroup A of index 2 is normal and hence $S_n/A \cong \mathbb{Z}/2\mathbb{Z}$. Therefore $\sigma^2 A = A, \forall \sigma \in S_n \Rightarrow \sigma^2 \in A, \forall \sigma \in S_n$. This in particular implies that all three cycles are in A, since if τ is a three cycle, then $\tau^2 = \tau^{-1}$. But A_n is generated by three cycles, so $A = A_n$.) This shows that any subgroup of S_4 of index 4 must be maximal: Suppose $[S_n : A] = 4$ and A is not maximal, then $\exists A \subset B$ a subgroup such that $[B:A] > 1$. So $4 = [S_n : A] = [S_n : B][B : A] > [S_n : B] \Rightarrow [S_n : B] = 2 \Rightarrow B = A_n$

which is a contradiction, because then $[A_n : A] = 2$. We conclude that H is maximal since it has index 4.

□

- Perfection: A field of characteristic p is called perfect if every element of K is a p^{th} power in K, i.e. $K = K^p$. Any field of characteristic 0 is also called perfect. Any finite field is perfect, as is $\mathbb{Q}$. Every irreducible polynomial over a perfect field is separable.

3 Fall 2002 – Fields

Problem 3.1. a) Determine the minimal polynomial of $u = \sqrt{3+2\sqrt{2}}$ over Q.

b) Determine the minimal polynomial of u^{-1} over Q.

Solution: a) $u^2 = 3 + 2\sqrt{2}$, so $(u^2-3)^2 = 8$ and therefore u is a root of

$$f \equiv x^4 - 6x^2 + 1.$$

Making the change of variable $y = x^2$ and using the quadratic equation, we see that f cannot factor as a product of two quadratics. On the other hand, the rational root test shows that it is impossible for f to factor as a linear term times a cubic. We conclude that f is irreducible so $f = m_Q(u)$.

b) $(u^{-1})^2 = \frac{1}{3+2\sqrt{2}}$. So $3(u^{-1})^2 + 2\sqrt{2}(u^{-1})^2 = 1$. Subtracting and squaring to get rid of $\sqrt{2}$, we see that u^{-1} is also a root of $x^4 - 6x^2 + 1$, which we have already determined to be irreducible, so $m_Q(u^{-1}) = x^4 - 6x^2 + 1$. (Or just note $x^4(\frac{1}{x^4} - \frac{6}{x^2} + 1) = x^4 - 6x^2 + 1$.) □

Problem 3.2. a) Let F be the field generated by the roots of the polynomial $X^6 + 3$ over Q. Determine the Galois group F/Q.

b) Describe all subfields of F.

Solution: a) Let $\xi = e^{2\pi i/6}$. Then the roots of $X^6 + 3$ are $\xi^i \sqrt[6]{-3}, 1 \le i \le 6$. So $F = \mathbb{Q}(\xi, \sqrt[6]{-3})$. Now notice that

$$\xi = e^{\pi i/3} = \frac{1}{2} + i\frac{\sqrt{3}}{2} \in \mathbb{Q}(\sqrt[6]{-3}),$$

since $(\sqrt[6]{-3})^3 = \sqrt{-3} = i\sqrt{3}$. So we conclude $F = \mathbb{Q}(\sqrt[6]{-3})$. By Eisenstein's Criterion, $X^6 + 3$ is irreducible and so it is the minimal polynomial of $\sqrt[6]{-3}$ and therefore $[F : \mathbb{Q}] = [\mathbb{Q}(\sqrt[6]{-3} : \mathbb{Q}] = 6$. This extension is Galois (since $X^6 + 3$ has 6 distinct roots, hence separable) so let G denote the Galois group. Then we have that $|G| = 6$, which implies that G is either S_3 or $\mathbb{Z}/6\mathbb{Z}$ (these are the only groups of order 6). To decide which one it is,

notice that $(\sqrt[6]{-3})^2 = (-3)^{1/3} = -\sqrt[3]{3}$, so $\sqrt[3]{3} \in F$. Consider $\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q}$. This extension is not Galois, since $\sqrt[3]{3}$ is a root of X^3-3 but $\mathbb{Q}(\sqrt[3]{3})$ does not contain any other roots of X^3-3, which is also irreducible by Eisenstein. By the Fundamental Theorem of Galois Theory, there is a correspondence between subfields which are Galois over $\mathbb{Q}$ and normal subgroups of G. We therefore conclude that G cannot be abelian since it contains a subgroup which is not normal (the subgroup fixing the subfield $\mathbb{Q}(\sqrt[3]{3})$, so the only possibility is $G = S_3$.

(If we had wished to be more explicit, we could have used the fact that an element of the Galois group maps a root to a root to make computations. First it is clear that $G \subset S_6$. Since $\sqrt[6]{-3}$ generates $\mathbb{Q}(\sqrt[6]{3})$ over $\mathbb{Q}$, any $\sigma \in G$ is completely determined by $\sigma(\sqrt[6]{-3})$. Label the roots 1 through 6 such that $\xi^i \sqrt[6]{3}$ is labeled i. Let $G = \{\sigma_1, \sigma_2, \ldots, \sigma_6\}$ such that σ_i maps $\sqrt[6]{-3}$ to the i^{th} root. Consider $\sigma_1 : \sqrt[6]{-3} \mapsto \xi \sqrt[6]{3}$. We will know everything about σ_1 once we figure out where it maps $\xi = \frac{1}{2} + \frac{\sqrt{-3}}{2}$. To this end notice we calculate:

$$\sigma_1(\sqrt{-3}) = \sigma_1((\sqrt[6]{-3})^3) = \xi^3\sqrt{-3} = -\sqrt{-3} \Rightarrow \sigma\left(\frac{1}{2} + \frac{\sqrt{-3}}{2}\right) = \frac{1}{2} - \frac{\sqrt{-3}}{2} = \xi_5.$$

From this we see that $\sigma_1^2(\xi\sqrt[6]{-3}) = \sigma_1(\sqrt[6]{-3}) = \sigma(\xi^5 \cdot \xi\sqrt[6]{-3}) = (\xi^5)^5\sqrt[6]{-3} = \xi\sqrt[6]{-3}$ (since $\xi^6 = 1$). So we conclude that $\langle\sigma_6\rangle$ is a subgroup of order 2. On the other hand, it is clear that $\sigma_3 : \sqrt[6]{-3} \mapsto \xi^3\sqrt[6]{-3} = -\sqrt[6]{-3}$ also has order 2. Therefore G contains two subgroups of order 2 and hence cannot be cyclic (a cyclic group of order n contains a unique subgroup of order d for each $d \mid n$), so $G = S_3$.)

b) By the Fundamental Theorem of Galois Theory, subfields of F corresponds to subgroups of $G = S_3$ in an order reversing way. S_3 has 3 subgroups of order 2, generated by the three transpositions:

$$\{e, (12)\}, \{e, (13)\}, \{e, (23)\}.$$

These correspond to the three subfields of F which has degree $6/2 = 3$ over $\mathbb{Q}$:

$$\mathbb{Q}(\xi^2\sqrt[3]{-3}), \mathbb{Q}(\xi^4\sqrt[3]{3}), \mathbb{Q}(\sqrt[3]{3}).$$

S_3 has one subgroup of order 3 (3 is prime so this subgroup is cyclic. The only elements in S_3 of order 3 are the cyclic permutations of order 3), namely

$$A_3 = \{e, (123), (123)^2\},$$

which correspond to the subfield of F which has degree 2 over $\mathbb{Q}$:

$$\mathbb{Q}(\sqrt{-3}).$$

There are no other non–trivial subfields. □

Suppose now instead we want to find the Galois group of X^6-3: Let ξ denote a primitive 6^{th} root of unity and $\alpha = e^{\pi i/6}\sqrt[6]{3}$. Then $F = \mathbb{Q}(\xi, \alpha)$. We have $[F : \mathbb{Q}] = [F : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) :$

$\mathbb{Q}]$. $X^6 - 3$ is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion, so it is the minimal polynomial of α and therefore $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$. The minimal polynomial of ξ over $\mathbb{Q}$ is $x^2 - x + 1 = (x - e^{i\pi/3})(x - e^{5\pi i/3})$. Since the degree of the polynomial is 2 and neither of the root is in $\mathbb{Q}(\alpha)$, $x^2 - x + 1$ remains irreducible over $\mathbb{Q}(\alpha)$ and we conclude that $[F : \mathbb{Q}(\alpha)] = 2$ and $[F : \mathbb{Q}] = 12$.

The subextension $\mathbb{Q}(\xi)/\mathbb{Q}$ is Galois (it is the splitting field of $x^2 - x + 1$ over $\mathbb{Q}$), so by the Galois Correspondence this corresponds to a normal subgroup H of $\mathrm{Gal}(F/\mathbb{Q})$ of order 6 fixing $\mathbb{Q}(\xi)$, which can be either $\mathbb{Z}/6\mathbb{Z}$ or S_3 (notice that If $E/K/F$ is such that E/F is Galois, then E/K is also Galois). The roots of $X^6 - 3$ are

$$\alpha, \xi\alpha, \xi^2\alpha, \xi^3\alpha, \xi^4\alpha, \xi^5\alpha.$$

Any $\sigma \in \mathrm{Aut}_{\mathbb{Q}(\xi)}F = \mathrm{Gal}(F/\mathbb{Q}(\xi)$ must map a root to a root and hence is determined by $\sigma(\alpha)$ (remember that σ fixes ξ, so if $\sigma(\alpha) = \xi^m\alpha$, then $\sigma(\xi^k\alpha) = \xi^k\sigma(\alpha) = \xi^{m+k}\alpha$, where m and k are defined modulo 6). We see that $\gamma : \mathrm{Aut}_{\mathbb{Q}(\xi)}F \longrightarrow \mathbb{Z}/6\mathbb{Z}$ by $\sigma \mapsto n$ where $\sigma(\alpha) = \xi^n\alpha$ is an isomorphism (If σ and τ are such that $\sigma(\alpha) = \xi^m\alpha$ and $\tau(\alpha) = \xi^n\alpha$, then $\sigma\tau(\alpha) = \xi^{m+n}\alpha$ and $\sigma\tau(\xi^k\alpha) = \xi^k\sigma\tau(\alpha) = \xi^{m+n}(\xi^k\alpha)$, so $\gamma(\sigma\tau) = \gamma(\sigma) + \gamma(\tau)$) and therefore $H \cong \mathbb{Z}/6\mathbb{Z}$. By considering $\mathbb{Q}(\alpha)/\mathbb{Q}$, we also see that there is a subgroup H_2 of order 2. Therefore $\mathrm{Gal}(F/\mathbb{Q}) \cong H \rtimes H_2$, which gives us two possibilities: $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or D_6 (symmetries of a hexagon). Since $\mathbb{Q}(\alpha)$ is not normal, $\mathrm{Gal}(F/\mathbb{Q})$ cannot be abelian and we are forced to conclude that $\mathrm{Gal}(F/\mathbb{Q}) = D_6$ (symmetries of a regular hexagon).

- Eisenstein's Criterion: Let p be a prime in $\mathbb{Z}$ and let

  $$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x], n \geq 1.$$

  Suppose

  $$p \mid a_i, 0 \leq i < n \text{ but } p^2 \nmid a_0.$$

  Then $f(x)$ is irreducible in both $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$. Sometimes a change of variable is useful if this does not apply directly, e.g. if one can show that the polynomial with $y = x + 1$ is irreducible, then the polynomial must also be irreducible in the original variable(just replace x by y in the factorization if it were reducible).

- Trivial Observation: If $E/K/F$ is such that E/F is Galois, then E/K is also Galois.

- Dihedral Group: The dihedral group D_n is the group of symmetries of a regular n–gon. A regular n–gon has $2n$ symmetries: n rotations and n reflections. A quick observation is then that there are n subgroups of order n if n is odd, corresponding to the n reflections and $n + 1$ subgroups of order 2 if n is even, corresponding to the n reflections plus rotation by π radians about the origin. The presentation for D_n is

  $$D_n = \{r, s \mid r^n = s^2 = 1, rs = sr^{-1}\},$$

where r is rotation counterclockwise about the origin through $2\pi/n$ radians and s is one of the reflections.

- Semidirect Product:
  - Let G be a group. Then G decomposes as a semidirect product of subgroups N and H, write $G = N \rtimes H$, if
    (i) $N \lhd G$; (ii) $N \cap H = \{e\}$; (iii) $NH = G$.
    (i) ensures that $NH = HN$ is a group and (ii) and (iii) says every element can be written uniquely as nh with $n \in N$, $h \in H$.
  - On the other hand, if there are groups H and N such that there is a homomorphism
    $$\alpha : H \longrightarrow \mathrm{Aut}(N),$$
    then $N \times H$ is a group with multiplication given by
    $$(n_1, h_1)(n_2, h_2) = (n_1\alpha(h_1)n_2, h_1h_2).$$
    Denote this group by $N \rtimes_\alpha H$. We have
    $$\tilde{N} \lhd (N \rtimes_\alpha H),$$
    where $\tilde{N} = \{(n, e) \mid n \in N\}$. Define $\tilde{H} = \{(e, h) \mid h \in H\}$, then $\tilde{N} \cap \tilde{H} = \{(e, e)\}$. We see that
    $$N \rtimes_\alpha H = \tilde{N}\tilde{H}$$
    as a semidirect product.
  - If G splits as a semidirect product of N and H, define
    $$\Gamma : H \longrightarrow \mathrm{Aut}(H) : h \mapsto \text{conjugation by } h,$$
    then
    $$N \rtimes_\Gamma H \longrightarrow G : (n, h) \mapsto nh$$
    is a group isomorphism.
  - Now suppose G is a finite group, $N \lhd G$, $N \cap H = \{e\}$ and $|N||H| = |G|$, then it is the case that $NH = G$ and so G splits as a semidirect product of $\tilde{N}$ and $\tilde{H}$. Explicitly, we have that
    $$G = NH \cong N \rtimes_\Gamma H,$$
    where Γ is conjugation by elements of H.

* We can in fact determine all possible isomorphism classes of NH. NH looks like $N \rtimes_\Gamma H$, where

$$(n_1, h_1)(n_2, h_2) = (n_1\Gamma(h_1)(n_2), h_1h_2) = (n_1(h_1n_2h_1^{-1}), h_1h_2).$$

Each $\Gamma(h)$ is an automorphism of N. Note that by associativity and the fact that Γ is a homomorphism

$$\begin{aligned}(n_1, h_1)(n_2, h_2)(n_3, h_3) &= (n_1\Gamma(h_1)(n_2)\Gamma(h_1h_2)(n_3), h_1h_2h_3)\\ &= (n_1\Gamma(h_1)(n_2\Gamma(h_2)(n_3)), h_1h_2h_3)\\ &= (n_1\Gamma(h_1)(n_2)\Gamma(h_1)(\Gamma(h_2)(n_3)), h_1h_2h_3),\end{aligned}$$

so

$$\Gamma(h_1h_2) = \Gamma(h_1) \circ \Gamma(h_2)$$

and therefore

$$\alpha : H \longrightarrow \mathrm{Aut}(N) : h \mapsto \Gamma(h)$$

is a homomorphism. This shows that each isomorphism class of NH arose from some homomorphism $\alpha : H \longrightarrow \mathrm{Aut}(N)$. Conversely, given $\alpha : H \longrightarrow \mathrm{Aut}(N)$, we can form $N \rtimes_\alpha H$ and we have as before

$$N \rtimes_\alpha H \cong \tilde{N}\tilde{H} \cong NH,$$

where $\tilde{N} = \{(n, 0) \mid n \in N\}$ and $\tilde{H} = \{(0, h) \mid h \in H\}$.

* Note that Γ is given by

$$\Gamma(h)(n) = hnh^{-1} = \alpha(h)(n).$$

* It is not the case that different α's necessarily lead to distinct isomorphism classes.

Problem 3.3. Let p be a prime integer such that $p \equiv 2$ or $3 \pmod 5$. Prove that the polynomial

$$1 + X + X^2 + X^3 + X^4$$

is irreducible over Z/pZ.

Solution: $1 + X + X^2 + X^3 + X^4 = \frac{X^5-1}{X-1} \equiv \Phi_5(X)$, the 5^{th} cyclotomic polynomial and has as roots all the primitive 5^{th} roots of unity. If ξ is a primitive 5^{th} root of unity, we would like to find the least n such that $\mathbb{F}_{p^n}$ contains ξ. It will be enough to show that $n = 4$ (if $\Phi_5(X) = f(X)g(X)$ were reducible, then say η is a root of f which has degree k, then η is a primitive root of unity and $\mathbb{F}_p(\eta)$ would be isomorphic to $\mathbb{F}_{p^k}$ with $k < 4$, a contradiction).

First suppose n is such that $\xi \in \mathbb{F}_{p^n}$. $(\mathbb{F}_{p^n})^\times$ is cyclic so let θ be a generator. Then $\theta^{p^n-1} = 1$ and θ raised to a lower power is not equal to 1. If $\xi \in \mathbb{F}_{p^n}$, then $(\exists k \in \mathbb{N})(\theta^k = \xi)$ so

$$(\theta^k)^5 = 1 \text{ in } \mathbb{F}_{p^n} \text{ and } (\theta^k)^l \neq 1 \text{ in } \mathbb{F}_{p^n} \text{ for } l < 5.$$

This implies that

$$5k = \alpha(p^n - 1), \text{ some } \alpha \in \mathbb{N}.$$

If $\alpha \mid 5$ then $\alpha = 5$ since 5 is prime so we conclude $k = p^n - 1$ and $\xi = 1$, a contradiction. If $\alpha \mid k$, then we can cancel α on both sides of the equation to get that

$$5k' = (p^n - 1) \Longrightarrow p^n \equiv 1 \pmod 5.$$

Conversely, suppose $p^n \equiv 1 \pmod 5$. Then $p^n = 5k + 1$, some $k \in \mathbb{N}$. Again let θ be a generator of $(\mathbb{F}_{p^n})^\times$. Then $(\theta^k)^5 = \theta^{p^n-1} = 1$ and so θ^k is a primitive 5^{th} root of unity. The roots of unity form a cyclic group, so that if $\mathbb{F}_{p^n}$ contains one primitive root of unity it must contain all of them, which implies that $\xi \in \mathbb{F}_{p^n}$.

Now let n be the order of p in $\mathbb{F}_5$, i.e. n is minimal such that $p^n \equiv 1 \pmod 5$. Then from the above we know that n is also the minimal n such that $\xi \in \mathbb{F}_{p^n}$. For both $p \equiv 2 \pmod 5$ and $p \equiv 3 \pmod 5$ we have that $n = 4$ so Φ_5 is irreducible over $\mathbb{F}_p$ (here we use the fact that $\mathbb{Z}/n\mathbb{Z}$ is a ring so that $\overline{a_1} = \overline{b_1}, \overline{a_2} = \overline{b_2}$, then $\overline{a_1 + a_2} = \overline{b_1 + b_2}$ and $\overline{a_1 a_2} = \overline{b_1 b_2}$). □

- Factorization of Φ_q over $\mathbb{F}_p$: Let $p \neq q$ be primes. If n is the least integer such that $p^n \equiv 1 \bmod q$, then the minimal polynomial of ξ_q has degree n over $\mathbb{F}_p$. Moreover, Φ_q is the product of $\frac{q-1}{n}$ distinct irreducible polynomials of degree n in $\mathbb{F}_p$.
- $\mathbb{Z}/n\mathbb{Z}$: $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ form a commutative ring with 1 under addition and multiplication modulo n (these operations are of course both well–defined).

4 Winter 2003 – Fields

Problem 4.1. Let $\mathbb{F}_q$ be the finite field of q elements. Answer the following questions:

(a) List all subfields of $\mathbb{F}_{p^6}$ for a prime p. Justify your answer.

(b) Find a formula for the number of monic irreducible polynomials of degree 6 in $\mathbb{F}_p[X]$. Justify your answer.

Solution: (a) $\mathbb{F}_{p^6}$ is the splitting field of $x^{p^6} - x$ over $\mathbb{Z}_p$ ($x^{p^6} - x$ is separable since the derivative is -1 and has no root and therefore has p^6 roots, so by order counting, $\mathbb{F}_{p^6}$ is contained in the splitting field. On the other hand, each element in $\mathbb{F}_{p^6}^\times$ satisfies $x^{p^6-1} = 1$ and so each element in $\mathbb{F}_{p^6}$ is a root of $x^{p^6} - x$ and we conclude the splitting field is equal

to $\mathbb{F}_{p^6}$). The Galois group $\mathrm{Gal}(\mathbb{F}_{p^6}/\mathbb{F})_p$ is generated by the Frobenius automorphism and is cyclic of order 6, hence isomorphic to $\mathbb{Z}/6\mathbb{Z}$. The two non–trivial subgroups of $\mathbb{Z}/6\mathbb{Z}$, namely $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ correspond to intermediate fields between $\mathbb{F}_{p^6}$ and $\mathbb{F}_p$ of degree (over $\mathbb{F}_p$) 3 and 2, respectively. These are the unique splitting fields of $x^{p^3} - x$ and $x^{p^2} - x$ over $\mathbb{F}_p$, namely $\mathbb{F}_{p^3}$ and $\mathbb{F}_{p^2}$, respectively.

(b) Let f be an irreducible polynomial over $\mathbb{F}_p$ of degree $d \mid 6$. If α is a root of f, then $\mathbb{F}_p(\alpha)/\mathbb{F}$ has degree d and hence is equal to $\mathbb{F}_{p^d}$ by uniqueness of splitting fields. $\mathbb{F}_{p^d}/\mathbb{F}_p$ is Galois, so $\mathbb{F}_{p^d} (\subset \mathbb{F}_{p^6})$ in fact contains all roots of f. Since $\mathbb{F}_{p^6}$ is equal to the set of roots of $x^{p^6} - x$, it must be the case that $f \mid x^{p^6} - x$. Now let g be the product of all (monic) minimal polynomials of elements in $\mathbb{F}_{p^6}$ with no repeats, then it follows that $g \mid x^{p^6} - x$. Conversely, it is clearly that $x^{p^6} - x \mid g$ and so we conclude $g = x^{p^6} - x$. Since any irreducible polynomial of degree d is the minimal polynomial of (each of) its roots, we see that in fact $x^{p^6} - x$ is the product of all irreducible polynomials over $\mathbb{F}_p$ of degree $d \mid 6$.

Now let $\psi(d) =$ number of irreducible polynomials of degree d over $\mathbb{F}_p$. Then (since the degree of $x^{p^6} - x$ is p^6) we have

$$p^6 = \sum_{d|6} d\psi(d).$$

By the Mobius Inversion Formula, we get

$$6\psi(6) = \sum_{d|6} \mu(d) p^{6/d},$$

where $\mu(1) = 1$, $\mu(n) = 0$ if n contains a square factor, and $\mu(n) = (-1)^r$ if n has r distinct prime factors. Calculating, we get

$$\begin{aligned} 6\psi(6) &= \mu(1)p^6 + \mu(2)p^3 + \mu(3)p^2 + \mu(6)p \\ &= p^6 - p^3 - p^2 + p. \end{aligned}$$

So $\psi(6) = \frac{1}{6}(p^6 - p^3 - p^2 + p)$.

Instead of using the Mobius Inversion Formula we could have proceeded as follows. First note that if f is an irreducible polynomial over $\mathbb{F}_p$, then f is separable. Say the degree of f is 6, then f has 6 distinct roots and it is the case that none of these roots can lie in $\mathbb{F}_{p^2}$ or $\mathbb{F}_{p^3}$ (if α is a root of f, then $f = m_{\mathbb{F}_p}(\alpha)$ has degree 6. If say $\alpha \in \mathbb{F}_{p^2}$, then the degree of α over $\mathbb{F}_p$ would be 2, a contradiction). Now observe that $\mathbb{F}_{p^2}$ and $\mathbb{F}_{p^3}$ intersect in $\mathbb{F}_p$ since 2 and 3 are relatively prime, so inclusion–exclusion gives that there are

$$p^6 - p^3 - p^2 + p$$

elements of degree 6 over $\mathbb{F}_p$ in $\mathbb{F}_{p^6}$. It suffices to count the number of minimal polynomials of these elements of order 6 (as before if f is irreducible of degree 6, then it is the minimal

polynomial of (each of) its roots). Each such minimal polynomials has 6 distinct roots, so there must be $\frac{1}{6}(p^6 - p^3 - p^2 + p)$ monic irreducible polynomials over $\mathbb{F}_p$ of degree 6. (Explicitly, pick an element α_1 of degree six, write down its minimal polynomial f_1. Now pick some α_2 which is not equal to any of the roots of f_1 and write down its minimal polynomial f_2. Continue this way, we will eventually exhaust all elements of degree 6 and will have found all irreducible polynomials of degree 6. Notice this implies that $6 \mid p^6 - p^3 - p^2 + p$.) □

- $x^{p^n} - x \Leftrightarrow \mathbb{F}_{p^n}$: The finite field $\mathbb{F}_{p^n}$ is precisely the set of roots of the polynomial $x^{p^n} - x$ over $\mathbb{F}_p$.
- $x^{p^n} - x$: The polynomial $x^{p^n} - x$ over $\mathbb{F}_p$ is in fact the product of all irreducible polynomials of degree $d \mid n$ over $\mathbb{F}_p$.
- Mobius Inversion Formula: Let $f(n)$ be a function defined for all nonnegative integers n and let
$$F(n) = \sum_{d|n} f(d).$$
Then we have
$$f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d}),$$
where $\mu(1) = 1$, $\mu(n) = 0$ if n has a square factor, and $\mu(n) = (-1)^r$ if n has r distinct prime factors.
- Splitting Fields of Irreducible Polynomials over $\mathbb{F}_p$: Let f be irreducible of degree n over $\mathbb{F}_p$. Then the splitting field of f is exactly $\mathbb{F}_{p^n}$.

Problem 4.2. Let K/F be a quadratic extension of fields and M/F be a Galois extension over F containing K such that $\mathrm{Gal}(M/K)$ is a cyclic group of odd prime order p. Answer the following two questions:

(a) Determine the possible groups $\mathrm{Gal}(M/F)$ up to isomorphisms, and justify your answer.

(b) Find the number of intermediate fields L between F and M with $[L : F] = p$. Justify your answer.

Solution: (a) Let $G = \mathrm{Gal}(M/F)$. Then
$$|G| = [M : F] = [M : K][K : F] = 2p.$$
Let $H = \mathrm{Gal}(M/K)$. First we claim $H \lhd G$: H has order p so $[G : H] = 2$. Now let G act on the cosets of H by left multiplication. This induces
$$\lambda : G \longrightarrow S_2 : g \mapsto \lambda_g : aH \mapsto haH.$$

We have $\ker(\lambda) = \bigcap_{g\in G} gHg^{-1}$ and by the First Isomorphism Theorem and Lagrange's Theorem, $|G/\ker(\lambda)| \mid |S_2| = 2$, which forces $|\ker(\lambda)| = p$ and therefore $H = \ker(\lambda) \lhd G$. Next by Cauchy's Theorem, there is a subgroup $H_2 \subset G$ of order 2. Hence

$$G = HH_2 \cong \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$$

as a semidirect product. This gives us two possibilities: $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or D_p (symmetries of a p–gon).

(b) By the Galois Correspondence, intermediate field L such that $[L : F] = p$ correspond to subgroups of G of order 2. If $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, then there is exactly one subgroup of order 2 since p is odd. If $G \cong D_p$, then there are p subgroups of order 2, corresponding to the p reflections (there is a reflection through each line joining a vertex and the side opposite to it). □

Problem 4.3. Find the degree of the splitting field E of $X^6 - 3$ over the following fields:

(a) $\mathbb{Q}(\sqrt{-3})$ ($\mathbb{Q}$: the field of rational numbers);

(b) $\mathbb{F}_7$, the field with 7 elements;

(c) $\mathbb{F}_5$, the field with 5 elements,

and justify your answer.

Solution: (a) $X^6 - 3$ is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion applied with the prime 3. The splitting field is given by

$$E = \mathbb{Q}(\xi, 3^{1/6}),$$

where $\xi = e^{\frac{2\pi i}{6}}$ is a primitive 6^{th} root of unity. We claim that $[\mathbb{Q}(\xi, 3^{1/6}) : \mathbb{Q}] = 12$: First we have that $[\mathbb{Q}(3^{1//6}) : \mathbb{Q}] = 6$. Next it is clear that the cyclotomic polynomial $X^2 - X + 1 = \Phi_6$ (which has ξ and ξ^5 as roots) remains irreducible over $\mathbb{Q}(3^{1/6})$, so $[\mathbb{Q}(3^{1/6}, \xi) : \mathbb{Q}(3^{1/6}] = 2$. Finally, $X^2 + 3$ is irreducible over $\mathbb{Q}$ so is the minimal polynomial of $\sqrt{-3}$. Hence $[\mathbb{Q}(\sqrt{-3}) : \mathbb{Q}] = 2$ and

$$12 = [E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt{-3}]2,$$

so $[E : \mathbb{Q}(\sqrt{-3})] = 6$.

(b) First note that $3^6 \equiv 1 \pmod 7$. So

$$x^6 - 3 \mid (x^6)^6 - 3^6 = x^{36} - 1.$$

$\mathbb{F}_{7^n}$ is the (unique) splitting field of $x^{7^n} - x$, so if the roots of $x^6 - 3$ are contained in $\mathbb{F}_{7^n}$, then it must be the case that $x^6 - 3 \mid x^{7^n} - x = x(x^{7^n - 1} - 1)$. Since $(x^m - 1) \mid (x^n - 1)$ if and only if $m \mid n$, we now wish to find the least integer m such that $7^m \equiv 1 \pmod{36}$. To this

end notice first that $7 \in (\mathbb{Z}/36\mathbb{Z})^\times \cong (\mathbb{Z}/2^2\mathbb{Z})^\times \times (\mathbb{Z}/3^2\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, by the Chinese Remainder Theorem. So 7 has either order 2 or order 6 in $(\mathbb{Z}/36\mathbb{Z})^\times$. It clearly does not have order 2 so it must be the case that $7^6 \equiv 1 \pmod{36}$. So $x^{36} - 1 \mid x^{7^6-1} - 1 \mid x^{7^6} - x$ and hence all roots of $x^6 - 3$ are contained in $\mathbb{F}_{7^6}$ which implies that $E \subset \mathbb{F}_{7^6}$ and so $[E : \mathbb{F}] = 1, 2, 3$, or 6 (since it must divide $[\mathbb{F}_{7^6} : \mathbb{F}_7] = 6$).

$E \neq \mathbb{F}_7$ since $a^6 = 1 \neq 3$ for all $a \in \mathbb{F}_7$.

$E \neq \mathbb{F}_{7^2}$ since $a^{7^2-1} = a^{48} = (a^6)^8 = 1$ for all $a \in \mathbb{F}_{7^2}$, but if a is a root of $x^6 - 3$, then $a^6 = 3$ so $(a^6)^8 = 3^8 = 3^2(3^6) \equiv 2 \pmod{7}$ (we have used the fact that $3^6 \equiv 1 \pmod{7}$ and is not equal to 1.

$E \neq \mathbb{F}_{7^3}$ since $a^{7^3-1} = a^3 42 - 1 = (a^6)^5 7 - 1 = 1$ for all $a \in \mathbb{F}_{7^3}$, but if a is a root of $x^6 - 3$, then $a^6 = 3$ so $(a^6)^5 7 = 3^5 7 = (3^3) = 27 = 6$ and is not equal to 1.

We are therefore left to conclude that $E = \mathbb{F}_{7^6}$ and $[E : \mathbb{F}_7] = 6$.

(c) By the same reasoning as in (b), we calculate:

$$x^6 - 3 \mid (x^6)^4 - 3^4 = x^{24} - 1 \mid x^{25} - x = x^{5^2} - x,$$

so all the roots of $x^6 - 3$ are contained in $\mathbb{F}_{5^2}$. Hence $E \subset \mathbb{F}_{5^2}$. $x^{5^2} - x$ has distinct roots since it has derivative -1 so $x^6 - 3$ must also have distinct roots since it divides $x^{5^2} - x$. Therefore $x^6 - 3$ must have 6 roots and so $E \neq \mathbb{F}_5$ (which only has 5 elements) and we conclude $E = \mathbb{F}_{5^2}$ and $[E : \mathbb{F}_5] = 2$. □

- Important Fact About Finite Fields: Every $a \in \mathbb{F}_{p^n}$ (p a prime integer) satisfies $a^{p^n} = a$ and every $0 \neq a \in \mathbb{F}_{p^n}$ satisfies $a^{p^n-1} = 1$.

- Cyclotomic Polynomials: The n^{th} cyclotomic polynomial $\Phi_n(x)$ is defined to be the polynomial whose roots are the primitive n^{th} roots of unity:

$$\Phi_n(x) = \prod_{a<n;\ (a,n)=1} (x - \xi_n^a),$$

where $\xi_n = e^{\frac{2\pi i}{n}}$. Clearly $\deg(\Phi_n) = \phi(n)$, where ϕ is the Euler ϕ–function. Notice that

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

This allows us to compute $\Phi_n(x)$ recursively. It can also be shown inductively that $\Phi_n(x) \in \mathbb{Z}[x]$.

Note that comparing degrees in the last equation gives

$$n = \sum_{d|n} \phi(d).$$

Applying the Mobius Inversion Formula to $n = F(n) = \sum_{d|n} \phi(d)$, we get

$$\phi(n) = \sum_{d|n} \mu(d) \left(\frac{n}{d}\right).$$

- Cyclotomic Extension (general case): If we can now show that $\Phi_n(x)$ is irreducible, then we will be able to conclude that

$$[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \phi(n).$$

To this end suppose

$$\Phi_n(x) = f(x)g(x),$$

with $f, g \in \mathbb{Z}[x]$, f irreducible. Let ξ be a root of f and $p \nmid n$ a prime. Then ξ^p is a root of $\Phi_n(x)$. If $g(\xi^p) = 0$, then ξ is a root of $g(x^p)$. Reducing mod p and using the fact that f is the minimal polynomial of ξ, we get that

$$(\overline{g}(x))^p = \overline{f}(x)\overline{h}(x),$$

some $h(x) \in \mathbb{Z}[x]$. This implies $\overline{f}$ and $\overline{g}$ have a common root, but this implies then $\overline{\Phi}_n(x)$ and therefore $x^n - 1$ has a multiple root over $\mathbb{F}_p$. This is a contradiction since $x^n - 1$ is separable (it has derivative nx^{n-1} which is relatively prime to $x^n - 1$). So ξ^p is a root of f for each $p \nmid n$. Now given any a such that $(a, n) = 1$, write $a = p_1 \dots p_k$ with p_i primes, then we see that $\xi^a = (((\xi^{p_1})^{p_2})^{\cdots})^{p_k}$ is a root of f and therefore all primitive n^{th} roots of unity are roots of f and we conclude $\Phi_n(x) = f(x)$ is irreducible. The map

$$(\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) : \overline{a} \mapsto \sigma_a : \sigma_a(\xi_n) = \xi_n^a$$

is an isomorphism. So

$$\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

- $(a - b) \mid (a^n - b^n)$:

$$(a-1)(a^{n-1} + a^{n-1} + \cdots + a + 1) = a^n - 1$$

since all the intermediate terms telescope. So

$$\begin{aligned} a^n - b^n = b^n \left(\left(\frac{a}{b}\right)^n - 1\right) &= b^n \left(\left(\frac{a}{b}\right) - 1\right)\left(\left(\frac{a}{b}\right)^{n-1} + \left(\frac{a}{b}\right)^{n-2} + \cdots + \left(\frac{a}{b}\right) + 1\right) \\ &= (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-1} + b^{n-1}). \end{aligned}$$

- $(x^m - 1) \mid (x^n - 1) \Leftrightarrow m \mid n$: By the previous item, $(x^m - 1) \mid ((x^m)^k - 1) = x^{km} - 1$ for any $k \in \mathbb{N}$. Conversely, suppose $(x^m - 1) \mid (x^n - 1)$. The roots of $x^m - 1$ are precisely the m^{th} roots of unity. Let ξ be a primitive m^{th} root of unity. Since $(x^m - 1) \mid (x^n - 1)$, ξ must also be a n^{th} root of unity. By the Division Algorithm, write $n = mk + r$, where $r < n$. Then we have that

$$1 = \xi^n = \xi^{mk+r} = \xi^{mk}\xi^r = \xi^r,$$

from which we conclude that $\xi^r = 1$, but since ξ is a primitive root of unity, it must be the case that $r = 0$ and therefore $m \mid n$.