Homework 2

Jonathan Osser

December 25, 2022

1. Let $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$. Describe explicitly a finite extension of $\mathbb{Q}$ having G as Galois group.

   Solution: Corollary 14.22 of Dummit and Foote yields one way to find a field F extension whose Galois group is a direct product of smaller groups; simply take F to be the composite of extensions whose pairwise intersections are trivial. In this case we would want to have two distinct fields with Galois group isomorphic to $\mathbb{Z}/4\mathbb{Z}$ such that their intersection is trivial, and one field whose Galois group is isomorphic to $\mathbb{Z}/12\mathbb{Z}$ which has trivial intersection with both other fields.

   An obvious extension with Galois group $\mathbb{Z}/4\mathbb{Z}$ is the cyclotomic field $F_1 = \mathbb{Q}(\zeta_5)$ adjoining to $\mathbb{Q}$ a primitive fifth root of unity. By theorem 14.26 of Dummit and Foote the Galois group of the extension is isomorphic to $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$. The same result gives us an extension with Galois group $\mathbb{Z}/12\mathbb{Z}$, namely $F_2 = \mathbb{Q}(\zeta_{13})$.

   Finally we use problem 6 of this homework as a hint that $F_3 = \mathbb{Q}(\sqrt{2+\sqrt{2}})$ has Galois group isomorphic to $\mathbb{Z}/4\mathbb{Z}$, which we will show holds true in that problem.

   Finally we need to show that the intersection of any two of these extensions is trivial. Since both It suffices to prove that there is no subfield of degree 2 which lies in the intersection of any pair of F_1, F_2, F_3. Note that there is only one non-trivial subgroup of $\mathbb{Z}/4\mathbb{Z}$, so by the fundamental theorem of Galois Theory, there is only one non-trivial subfield of F_1, F_3 each, both of degree two. However, $F_3/\mathbb{Q}(\sqrt{2})$ and $F_1/\mathbb{Q}(\sqrt{5})$, but $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt{5})$, so $F_1 \cap F_3 = \emptyset$. For F_2, notice that $\mathrm{Gal}(F_2/\mathbb{Q}) = \mathbb{Z}/12\mathbb{Z}$, which has only one unique subgroup of index 2, namely the one of order 6. This subgroup the corresponds to the subfield $\mathbb{Q}(\sqrt{13})$, which is neither $\mathbb{Q}(\sqrt{2})$ nor $\mathbb{Q}(\sqrt{5})$. Hence the pairwise intersection of the fields F_1, F_2, F_3 is trivial. Thus their composite $F = F_1F_2F_3$ has Galois group G.

2. Suppose m is a positive integer and $2^m + 1$ is prime. Show that m itself must be a power of 2.

   Solution: Notice that for $m = 2k+1$ odd we have

$$\begin{aligned} x^m + 1 &= x^{2k+1} + 1 \\ &= x^{2k+1} - x^{2k} + x^{2k} \cdots - x + 1 \\ &= (x^{2k+1} - x^{2k} + \cdots - x^2 + x) + (x^{2k} - x^{2k-1} + \cdots - x + 1) \\ &= (x+1)(x^{2k} - x^{2k-1} + \cdots - x + 1). \end{aligned}$$

   So m cannot be odd, as then $2^m + 1 = (2+1)(\dots)$ would have a non-trivial a factorisation of $2^m + 1$, which contradicts that $2^m + 1$ is prime. In fact, if m has some non-two factor, i.e. $m = 2^k n$ for n odd, then

$$2^m + 1 = 2^{2^k n} + 1 = \left(2^{2^k}\right)^n + 1$$

has a non-trivial factorisation $(2^{2^k} + 1)(\dots)$ from the above, which contradicts so $2^m + 1$ being prime. Hence m cannot have a non-two factor, so $m = 2^k$ for some k.

3. Assume that m is a positive integer, that p is prime and that p divides the Fermat number $2^{2^m} + 1$. Show that $p \equiv 1 \pmod{2^{m+1}}$.

   Solution: Note that $\Phi_{2^{m+1}}(x) = x^{2^m} + 1$ for $m \geq 1$. Since p divides $2^{2^m} + 1 = \Phi_{2^{m+1}}$ we have that $\Phi_{2^{m+1}}(2) = 1 \in \mathbb{F}_p$, so 2 has order 2^{m+1} in $\mathbb{F}_p^\times$. Hence 2^{m+1} divides $p - 1$, which means $p \equiv 1 \pmod{()}2^{m+1})$.

4. Let K be a field. Given $\alpha_1, \dots, \alpha_n \in K$ with $n \geq 2$, the *Vandermonde determinant* of $\alpha_1, \dots, \alpha_n$ is
$$V(\alpha_1, \dots, \alpha_n) = \det \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix}.$$
Show that the Vandermonde determinant satisfies *Vandermonde's Identity*:
$$V(\alpha_1, \dots, \alpha_n) = \prod_{j<i} (\alpha_i - \alpha_j).$$

Solution: We prove this by induction on n.

In the base case, when $n = 2$, we have

$$V(\alpha_1, \alpha_2) = \det \begin{pmatrix} 1 & \alpha_1 \\ 1 & \alpha_2 \end{pmatrix} = (1 - \alpha_2)(1 - \alpha_1) = \alpha_2 - \alpha_1,$$

so we are done.

For the inductive case, assume that for $k \geq 2$ and any $\beta_1, \dots, \beta_k$ we have $V(\beta_1, \dots, \beta_k) = \prod_{j<i}(\beta_i - \beta_k)$, i.e. that the identity holds for $n = k$. We need to show it holds for $n = k+1$ also. Let $\alpha_1, \dots, \alpha_{k+1}$ be given. Then we can subtract the previous column times α_1 from each but the first column, which computes as follows:

$$\begin{aligned} V(\alpha_1, \dots, \alpha_{k+1}) &= \det \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^k \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^k \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_{k+1} & \alpha_{k+1}^2 & \cdots & \alpha_{k+1}^k \end{pmatrix} \\ &= \det \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & \alpha_2 - \alpha_1 & \alpha_2^2 - \alpha_2\alpha_1 & \cdots & \alpha_2^k - \alpha_2^{k-1}\alpha_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_{k+1} - \alpha_1 & \alpha_{k+1}^2 - \alpha_{k+1}\alpha_1 & \cdots & \alpha_{k+1}^k - \alpha_{k+1}^k\alpha_1^k \end{pmatrix} \\ &= \det \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & \alpha_2 - \alpha_1 & \alpha_2(\alpha_2 - \alpha_1) & \cdots & \alpha_2^{k-1}(\alpha_2 - \alpha_1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_{k+1} - \alpha_1 & \alpha_{k+1}(\alpha_{k+1} - \alpha_1) & \cdots & \alpha_{k+1}^{k-1}((\alpha_{k+1} - \alpha_1) \end{pmatrix} \\ &= \det \begin{pmatrix} \alpha_2 - \alpha_1 & \alpha_2(\alpha_2 - \alpha_1) & \cdots & \alpha_2^{k-1}(\alpha_2 - \alpha_1) \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{k+1} - \alpha_1 & \alpha_{k+1}(\alpha_{k+1} - \alpha_1) & \cdots & \alpha_{k+1}^{k-1}((\alpha_{k+1} - \alpha_1) \end{pmatrix} \\ &= \left(\prod_{2 \leq i} (\alpha_i - \alpha_1) \right) \det \begin{pmatrix} 1 & \alpha_2 + f_2(\alpha_2) & \cdots & \alpha_2^{k-1} + f_k(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_{k+1} - f_2(\alpha_{k+1}) & \cdots & \alpha_{k+1}^{k-1} + f_k(\alpha_{k+1}) \end{pmatrix}. \end{aligned}$$

The latter determinant is $\prod_{2 \leq j < i}(\alpha_i - \alpha_j)$ by the inductive hypothesis, so combined with the factor in front we have

$$V(\alpha_1, \dots, \alpha_{k+1}) = \left(\prod_{2 \leq i} (\alpha_i - \alpha_1) \right) \left(\prod_{2 \leq j < i} (\alpha_i - \alpha_j) \right) = \prod_{j<i} (\alpha_i - \alpha_j),$$

which is what we aimed to prove. Hence we conclude by induction that the statement holds for all $n \geq 2$.

5. Let $K = \mathbb{Q}(\sqrt[8]{2}, i)/\mathbb{Q}$. Consider its subfields $F_1 = \mathbb{Q}(i)$, $F_2 = \mathbb{Q}(\sqrt{2})$, and $F_3 = \mathbb{Q}(\sqrt{-2})$. Show that $\mathrm{Gal}(K/F_1) \cong \mathbb{Z}/8\mathbb{Z}$, that $\mathrm{Gal}(K/F_2)$ is dihedral of order 8, and that $\mathrm{Gal}(K/F_3)$ is isomorphic to the quaternion group of order 8.

   Solution:

   Let $\theta = \sqrt[8]{2}$ and ζ be a primite 8th root of unity, as in the example on page 577 of Dummit and Foote. Then we have from said example that

   $$\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3 \rangle,$$

   where

   $$\sigma : \begin{cases} \theta \mapsto \zeta\theta \\ i \mapsto i \end{cases} \quad \text{and} \quad \tau : \begin{cases} \theta \mapsto \theta \\ i \mapsto -i. \end{cases}$$

   This group has order 16. The order of each of the Galois groups $\mathrm{Gal}(K/F_i), 1 \leq i \leq 3$ is 8, since the index of each subgroup in $\mathrm{Gal}(K/\mathbb{Q})$ is 2, which follows from the fact that each field is a quadratric extension of $\mathbb{Q}$, and thus of degree 2.

   Clearly the maps which fix i are precisely the powers of σ, so from this we conclude $\mathrm{Gal}(K/F_1) = \langle \sigma \rangle$, and since σ has order 8, we have $\langle \sigma \rangle \cong \mathbb{Z}/8\mathbb{Z}$ by definition. Hence $\mathrm{Gal}(K/F_1) \cong \mathbb{Z}/8\mathbb{Z}$.

   Similarly, the maps which fix $\sqrt{2} = \theta^4$ are τ, as well as not σ, since $\sigma(\theta^4) = \sigma(\theta)^4 = (\zeta\theta)^4 = -\theta^4$, but rather the powers of σ^2:

   $$\sigma^2(\theta^4) = \sigma(\sigma(\theta^4)) = \sigma(-\theta^4) = -\sigma(\theta^4) = \theta^4.$$

   Clearly $\tau \in \mathrm{Gal}(K/F_2)$. Note that $\langle \sigma^2, \tau \rangle$ has order 8 and is a subgroup of $\mathrm{Gal}(K/F_2)$, so $\mathrm{Gal}(K/F_2) = \langle \sigma^2, \tau \rangle$. This group satisfies the equation $\sigma^2\tau = \sigma\tau\sigma^3 = \tau\sigma^6 = \tau\sigma^{-2}$, i.e. is dihedreal. Thus $\mathrm{Gal}(K/F_2)$ is dihedral of order 8.

   Finally we wish to find the automorphisms which fix $\sqrt{-2} = \sqrt{2}i = \theta^4 i$. Note that $\sigma^2(\theta^4 i) = \theta^4 i$ and $\sigma\tau(\theta^4 i) = \sigma\tau(\theta^4)\sigma\tau(i) = (-\theta^4)(-i) = \theta^4 i$, so

   $$\sigma^2, \sigma\tau \in \mathrm{Gal}(K/F_3).$$

   Furthermore any product of those are in $\mathrm{Gal}(K/F_3)$, so $\langle \sigma^2, \sigma\tau \rangle \leq \mathrm{Gal}(K/F_3)$. Note that

   $$\langle \sigma^2, \sigma\tau \rangle = \{1, \sigma^2, \sigma^4, \sigma^6, \sigma\tau, \sigma^3\tau, \sigma^5\tau\sigma^7\tau\}$$

   has order 8. Hence $\mathrm{Gal}(K/F_3) = \langle \sigma^2, \sigma\tau \rangle$. This group has at least three elements whose square is σ^4, namely σ^2, $\sigma\tau$, $\tau\sigma$:

   $$\begin{aligned} (\sigma^2)^2 &= \sigma^4 \\ (\sigma\tau)^2 &= \sigma\tau\sigma\tau = \sigma\tau\tau\sigma^3 = \sigma^4 \\ (\tau\sigma)^2 &= \tau\sigma\tau\sigma = \tau\tau\sigma^4 = \sigma^4. \end{aligned}$$

   Since the group is non-abelian ($\tau\sigma\sigma^2 = \tau\sigma^3 = \sigma\tau \neq \sigma^2\sigma\tau$) and has more than one element of order 4, it cannot be the dihedral group, and so must be the quaternion group.

6. Show that $\mathbb{Q}(\sqrt{2 + \sqrt{2}})/\mathbb{Q}$ is Galois with Galois group $\mathbb{Z}/4\mathbb{Z}$.

Solution: The minimal polynomial for $\alpha = \sqrt{2+\sqrt{2}}$ is $m_\alpha = x^4 - 4x^2 + 2$, whose other roots are $\beta = \sqrt{2-\sqrt{2}}$, $-\alpha$, and $-\beta$, or rather, the roots of m_α are $\{\pm\alpha, \pm\beta\}$. By computation we can show that $\beta = \frac{\sqrt{2}}{\alpha}$, since

$$\alpha\beta = \sqrt{(2+\sqrt{2})(2-\sqrt{2})} = \sqrt{2} = \alpha^2 - 2 = 2 - \alpha^2,$$

so $\beta = \frac{\alpha\beta}{\alpha} = \frac{\alpha^2-2}{\alpha}$ and $\alpha = \frac{2-\beta^2}{\beta}$.

The minimal polynomial is irreducible over $\mathbb{Q}$, so the Galois group acts transitively on the roots. So we prove by cases that there Galois groups is isomorphic to $\mathbb{Z}/4\mathbb{Z}$:

- If $\sigma(\alpha) = \alpha$, then $\sigma(\beta) = \frac{\sigma(\alpha)^2-2}{\sigma(\alpha)} = \beta$, so σ fixes the whole extension, i.e. σ is the identity map.
- If $\sigma(\alpha) = \beta$, then $\sigma(\beta) = \frac{\sigma(\alpha)^2-2}{\sigma(\alpha)} = \frac{\beta^2-2}{\beta} = -\alpha$.
- If $\sigma(\alpha) = -\alpha$, then $\sigma(\beta) = \frac{\sigma(\alpha)^2-2}{\sigma(\alpha)} = \frac{\alpha^2-2}{-\alpha} = -\beta$.
- If $\sigma(\alpha) = -\beta$, then $\sigma(\beta) = \frac{\sigma(\alpha)^2-2}{\sigma(\alpha} = \frac{\beta^2-2}{-\beta} = \alpha$.

Since any permutation is uniquely determined by where it sends α, the order of the Galois group must be 4, and furthermore any automorphism is determined by the automorphism which satisifies $\sigma(\alpha) = \beta$: $\sigma^2(\alpha) = -\alpha$, $\sigma^3(\alpha) = -\beta$, and $\sigma^4(\alpha) = \alpha$, so $\sigma^4 = \mathrm{id}$, whence $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3\}$.

7. Let $p_1, \ldots, p_n$ be n distinct primes. Show that $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbb{Q}$ is Galois with Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n$.

   Solution: Clearly $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$ is the least field extension over $\mathbb{Q}$ for which the polynomial $f(x) = \prod_{k=1}^n (x^2 - p_k)$ splits completely, and each factor is an irreducible polynomial of degree 2. Hence no factor has a multiple root (Corollary 13.34 of Dummit and Foote), so f is separable. The Galois group of each factor is $\mathbb{Z}/2\mathbb{Z}$, so the Galois group of f is $(\mathbb{Z}/2\mathbb{Z})^n$. Therefore $\mathrm{Gal}(\mathbb{Q}(\sqrt{p_1} \ldots, \sqrt{p_n})/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^n$.

8. Determine the Galois group of $x^5 + x - 1$.

   Solution: We factor the polynomial $x^5 + x - 1 = (x^2 - x + 1)(x^3 + x^2 - 1)$. Clearly the quadratic factor $p(x)$ is irreducible: it only has complex roots $x = \frac{1}{2} \pm \frac{\sqrt{-3}}{2}$. Similarly the cubic $q(x)$ is also irreducible. The discriminant of $q(x)$ is -23, which is not square in $\mathbb{Q}$, so the Galois group of $q(x)$ is S_3. Similarly the Galois group of $p(x)$ is $S_2 \cong \mathbb{Z}/2\mathbb{Z}$. So the Galois group of $x^5 + x - 1$ is $\mathrm{Gal}(E_pE_q/\mathbb{Q})$, where E_p, E_q are the splitting field of $p(x)$ and $q(x)$ respectively. Note that $E_p = \mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-23}) \subset E_q$. Furthermore E_q has precisely one quadratic subfield, the fixed field of A_3, since A_3 is the only subgroup of S_3 with index 2. So if E_p and E_q had non-trivial intersection, then $E_p \subseteq E_q$, so $\mathbb{Q}(\sqrt{-3}) = E_p = \mathbb{Q}(\sqrt{-23})$, which is obviously false. Hence $E_p \cap E_q = \mathbb{Q}$, from which follows that

   $$\mathrm{Gal}(E_pE_q/\mathbb{Q}) = \mathrm{Gal}(E_p/\mathbb{Q}) \times \mathrm{Gal}(E_q/\mathbb{Q}) = S_3 \times \mathbb{Z}/2\mathbb{Z},$$

   which is thus the Galois field of the polynomial $x^5 - x + 1$ over $\mathbb{Q}$.

9. Let p be a prime. Assume that $x^5 + ax + b \in \mathbb{F}_p[x]$ is irreducible over $\mathbb{F}_p$. Show that $5^5b^4 + 4^4a^5$ is a square in $\mathbb{F}_p^\times$.

   Solution: Since $x^5 + ax + b$ is irreducible, its splitting field is of degree 5 over $\mathbb{F}_p$. Hence its Galois group is some cyclic subgroup C_5 of S_5 consisting of 5-cycles and identity. Since every element in $\mathbb{C}_5$ is either identity or a 5-cycle, all elements are even, so $C_5 \leq A_5$. Hence it follows from proposition 34 that the discriminant is a square in F. But the discriminant is $5^5b^4 + 4^4a^5$, so $5^5b^4 + 4^4a^5 \in \mathbb{F}_p$ is square. Furthermore the discriminant is zero precisely if there are multiple roots, but its irreducible and thus seperable. Hence $5^5b^4 + 4^4a^5$ is non-zero, so its in $\mathbb{F}_p^\times$.

10. Let p be a prime. Show that the extension $\mathbb{F}_p(x, y)/\mathbb{F}_p(x^p, y^p)$ does not admit a primitive element.

    Solution: Let $F = \mathbb{F}_p(x^p, y^p)$. Then we have a family of extensions $F(x + y^{kp+1})$, which are obviously subfields of $\mathbb{F}_p(x, y)$ and each are of degree p. Furthermore no two fields in this family of different values k are equal. For $n \neq m$, if $F(x+y^{np+1}) = F(x+y^{mp+1})$, then

    $$(x + y^{np+1}) - (x + y^{mp+1}) = y^{np+1} - y^{mp+1} = y(y^{np} - y^{mp}),$$

    but $y^{np} - y^{mp} \neq 0$, so $y \in F(x + y^{np+1})$, from which follows that $x \in F(x + y^{np+1})$, so then $F(x + y^{np+1}) = \mathbb{F}_p(x, y)$. However, by each field in the family is of degree p, since $(x + y^{kp+1})^p = x^p + y^{kp^2+p} \in \mathbb{F}_p(x^p, y^p$, whereas $\mathbb{F}_p(x, y)$ is of degree p^2 over $\mathbb{F}_p(x^p, y^p)$. Hence all $F(x + y^{kp+1}$ are distinct, and there are infinitely many, so by proposition 14.24 of Dummit and Foote it follows that K is not a simple extension, so it admits no primitive element.