Some Galois theory.

In what follows $\mathbb{F}_q$ is the finite field with q elements.

Proposition 1. *Let* $\gcd(n, q) = 1$. *The polynomial* $x^n - 1$ *splits in* $\mathbb{F}_q$ *if and only if* $n \mid (q - 1)$.

Problem 1. Prove this. *Hint:* Let $H = \{a \in \mathbb{F}_q : a^n = 1\}$. Then show H is a subgroup of the multiplicative $\mathbb{F}_q^\times$, and then show $x^n - 1$ splits in $\mathbb{F}_q$ if and only if $|H| = n$. Thus, since the multiplicative group of a field is cyclic, we have that $\mathbb{F}_q^\times$ has a subgroup of order n if and only if n divides $|\mathbb{F}_q^\times| = q - 1$. $\square$

Proposition 2. *Let p be a prime and n a positive integer with $p \not| n$. Then the splitting field of $x^n - 1$ over $\mathbb{F}_p$ is $\mathbb{F}_q$ where $q = p^k$ and k is the smallest positive integer such that $n \mid (q^k - 1)$.*

Problem 2. Prove this. $\square$

Problem 3. Find the splitting field of $x^{13} - 1$ over $\mathbb{F}_7$. $\square$

Problem 4. What goes wrong with the results above if $n \mid q$? In particular what is the splitting field of $x^p - 1$ over $\mathbb{F}_p$? The splitting field of $x^{p^2} - 1$ over $\mathbb{F}_p$? $\square$

In an earlier problem set (#25) we have proven the following.

Proposition 3. *Let m and n be integers such than none of n, m, or mn are squares of integers. Then $\mathbb{Q}(\sqrt{m} + \sqrt{n}) = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ and the polynomial*

$$\begin{aligned} &x^4 - 2(m+n)x^2 + m - n)^2 \\ &\quad = (x + \sqrt{m} + \sqrt{n})(x + \sqrt{m} - \sqrt{n})(x - \sqrt{m} + \sqrt{n})(x - \sqrt{m} - \sqrt{n}) \end{aligned}$$

is irreducible. $\square$

Problem 5. With the set up of the previous proposition show the Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{m}, \sqrt{n})/\mathbb{Q})$ is $\mathbb{Z}_2 \times \mathbb{Z}_2$ and is generated by the maps

$$\begin{aligned} \sigma_1(\sqrt{m}) &= -\sqrt{m}, & \sigma_1(\sqrt{n}) &= \sqrt{n}, \\ \sigma_2(\sqrt{m}) &= \sqrt{m}, & \sigma_1(\sqrt{n}) &= -\sqrt{n}. \end{aligned}$$

Proposition 4. *Let $n_1, n_2, \ldots, n_k$ be distinct positive integers such that no product $n_{i_1} n_{i_2} \cdots n_{i_r}$ with $1 \le i_1 < i_2 < \cdots i_r \le k$ is a perfect square. Then the degree of the field $\mathbb{Q}(\sqrt{n_1}, \sqrt{n_2}, \ldots, \sqrt{n_k})$ over $\mathbb{Q}$ is 2^k, the Galois group is isomorphic to $\mathbb{Z}_2^k$ and is generated by the k elements defined as permutations of $\{\sqrt{n_1}, \sqrt{n_2}, \ldots, \sqrt{n_k}\}$ by the k permutations $\sigma_1, \sigma_2, \ldots, \sigma_k$ given by*

$$\sigma_j(\sqrt{n_i}) = \begin{cases} -\sqrt{n_i}, & j = i; \\ \sqrt{n_i}, & j \neq i. \end{cases}$$

Problem 6. This is a lemma for proving Proposition 4. Show the group $\mathbb{Z}_2^k$ has 2^{k-1} subgroups of order 2^{k-1}. □

Problem 7. Prove Proposition 4. *Hint:* What seems easiest to me is induction on k. The case of $k = 2$ is covered in Problem 5. Assume the result holds for k.

(a) First show $\sqrt{n_{k+1}} \notin \mathbb{Q}(\sqrt{n_1}, \sqrt{n_2}, \ldots, \sqrt{n_k})$. Towards a contraction assume $\sqrt{n_{k+1}} \in \mathbb{Q}(\sqrt{n_1}, \sqrt{n_2}, \ldots, \sqrt{n_k})$. Then $\mathbb{Q}(\sqrt{n_{k+1}})$ has degree 2 over $\mathbb{Q}$. By the induction hypothesis we know that the Galois group of $\mathbb{Q}(\sqrt{n_1}, \sqrt{n_2}, \ldots, \sqrt{n_k})$ is $\mathbb{Z}_2^k$. This group has $2^k - 1$ subgroups of index 2. So by the Galois correspondence $\mathbb{Q}(\sqrt{n_1}, \sqrt{n_2}, \ldots, \sqrt{n_k})$ has $2^k - 1$ fields of degree 2 over $\mathbb{Q}$. To see what they are note for each non-empty subset $I := \{n_1, n_{i_2}, \ldots, n_{i_r}\}$ of $\{1, 2, \ldots, k\}$ the product $n_I := n_{i_1} n_{i_2} \cdots n_{i_r}$ is not a perfect square and thus $\sqrt{n_I}$ is irrational. Therefore $\mathbb{Q}(\sqrt{n_I})$ is a subfield of $\mathbb{Q}(\sqrt{n_1}, \sqrt{n_2}, \ldots, \sqrt{n_k})$ of degree 2 over $\mathbb{Q}$. Use Problem 5 to show if $I \neq J$, then $\mathbb{Q}(\sqrt{n_I}) \neq \mathbb{Q}(\sqrt{n_J})$. As the number of non-empty subsets, I, of $\{1, 2, \ldots, k\}$ is $2^k - 1$ this implies that we have accounted for all the subfields of $\mathbb{Q}(\sqrt{n_1}, \sqrt{n_2}, \ldots, \sqrt{n_k})$ of degree 2. Therefore $\mathbb{Q}(\sqrt{n_{k+1}}) = \mathbb{Q}(\sqrt{n_I})$ for some subset I. Show this contradicts Problem 5.

(b) Let $\mathbb{F} = \mathbb{Q}(\sqrt{n_1}, \sqrt{n_2}, \ldots, \sqrt{n_k})$. Then $[\mathbb{F}(\sqrt{n_{k+1}}), \mathbb{F}] = 2$ and $a + b\sqrt{n_{k+1}} \mapsto a - b\sqrt{n_{k+1}}$ is an automorphism of $\mathbb{F}(\sqrt{n_{k+1}})$ that fixes all the elements of $\mathbb{F}$. Use this to complete the proof. □

Proposition 5. *With the same hypothesis as Proposition 4, let* $a_0, a_1, \ldots, a_k$ *be rational numbers with* $a_1, a_2, \ldots, a_k$ *nonzero. Then*

$$\mathbb{Q}(a_0 + a_1\sqrt{n_1} + a_2\sqrt{n_2} + \cdots + a_k\sqrt{n_k}) = \mathbb{Q}(\sqrt{n_1}, \sqrt{n_2}, \ldots, \sqrt{n_k}).$$

Problem 8. Prove this. *Hint:* If this does not hold, then $\mathbb{Q}(a_0 + a_1\sqrt{n_1} + a_2\sqrt{n_2} + \cdots + a_k\sqrt{n_k})$ is a proper subfield of $\mathbb{Q}(\sqrt{n_1}, \sqrt{n_2}, \ldots, \sqrt{n_k})$ and therefore there is a nontrivial automorphism of $\mathbb{Q}(\sqrt{n_1}, \sqrt{n_2}, \ldots, \sqrt{n_k})$ that fixes $a_0 + a_1\sqrt{n_1} + a_2\sqrt{n_2} + \cdots + a_k\sqrt{n_k}$. Show this is impossible. □

Problem 9. Let $p_1, p_2, \ldots, p_k$ be distinct primes and $a_0, a_1, \ldots, a_k$ rational numbers with $a_1, a_2, \ldots, a_k$ nonzero. Use what we have done above to show

$$\mathbb{Q}(a_0 + a_1\sqrt{p_1} + a_2\sqrt{p_2} + \cdots + a_k\sqrt{p_k}) = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_k}),$$

this extension has degree 2^k over $\mathbb{Q}$, and the Galois group is $\mathbb{Z}_2^k$. □

Problem 10 (January, 2018 Problem 10). For a positive integer n, let $\alpha = \sum_{k=1}^{n} \sqrt{k}$. Prove the minimal polynomial of α over $\mathbb{Q}$ has degree $2^{\pi(n)}$ where $\pi(n)$ is the number of prime numbers $\leq n$. □