Problem 4. Write $F = k(s_1, \ldots, s_n)$. Let $f(X)$ be the polynomial $X^{2n} + \sum_{j=1}^{n}(-1)^{j}s_jX^{2(n-j)}$ of the problem. Then, in a splitting field $L$, we have the factorization

$$f(X) = (x - r_1)(x + r_1) \cdots (x - r_n)(x + r_n)$$

where the roots of $f$ are $\pm r_j$, $1 \leq j \leq n$. Clearly $L = F(r_1, \ldots, r_n) = k(r_1, \ldots, r_n)$.

Multiplying out equation (1), we find that $s_j$ is the $j$-th symmetric polynomial in $r_1^2, \ldots, r_n^2$. By an argument almost identical to Jacobson 4.15, the roots $r_j$ in $L$ are algebraically independent over $F$. Set $K := F(r_1^2, \ldots, r_n^2)$, so that $F \subset K \subset L$. Then $K$ is the splitting field of $X^n + \sum_{j=1}^{n}(-1)^{j}s_jX^{n-j}$ over $F$, so by Jacobson 4.15, Gal($K/F$) = $S_n$.

We claim that $[L:K] = 2^n$. This is proved by adjoining the $r_j$’s one at a time and observing that the degree goes up by a factor of 2 each time. For example, $r_1 \not\in K$, but $r_1^2 \in K$, so that $[K(r_1) : K] = 2$. Similarly $[K(r_1, r_2) : K(r_1)] = 2$, etc., and in the end $[L : K] = [K(r_1, \ldots, r_n) : K(r_1, \ldots, r_{n-1})] \cdots [K(r_1, r_2) : K(r_1)] [K(r_1) : K] = 2^n$.

Now let $\sigma \in$ Gal($L/F$). We know $\sigma$ must permute the roots $\pm r_j$ in some fashion; the only question is which permutations are admissible for $\sigma$. Any automorphism must satisfy $\sigma(-r_j) = -\sigma(r_j)$, and one checks easily that there are exactly $2^n n!$ permutations of the set $\{\pm r_1, \pm r_2, \ldots, \pm r_n\}$ that satisfy $\sigma(-r_j) = -\sigma(r_j)$ for all $j$. Since every $\sigma \in$ Gal($L/F$) must have this form, we conclude that there are at most $2^n n!$ elements in Gal($L/F$). But we also know that $[L : F] = [L : K][K : F] = 2^n n!$, so by the fundamental theorem of Galois theory, there are exactly $2^n n!$ elements in Gal($L/F$), and it follows that every such permutation above corresponds to an element of Gal($L/F$).

Therefore, the Galois group Gal($L/F$) is the group of permutations $\sigma$ of the set $\{\pm r_j\}$ satisfying $\sigma(-r_j) = -\sigma(r_j)$. This group is not isomorphic to ($\mathbb{Z}/2\mathbb{Z}$)$^n \times S_n$—one easy way to see this is to take the case $n = 2$, where one can compute explicitly that the group is isomorphic to the nonabelian group $D_4$ and not to the abelian group ($\mathbb{Z}/2\mathbb{Z}$)$^2 \times S_2$. One can also describe Gal($L/F$) as the semidirect product ($\mathbb{Z}/2\mathbb{Z}$)$^n \rtimes S_n$, where $S_n$ acts on ($\mathbb{Z}/2\mathbb{Z}$)$^n$ by permuting the factors.


Problem 7. Let $\zeta := e^{2\pi i/p}$ be a primitive $p$-th root of unity. Then the roots of $x^p - c$ are $\zeta^j \sqrt[2]{c}$, for $0 \leq j \leq p - 1$. The splitting field $K$ of $x^p - c$ is then $\mathbb{Q}(\sqrt[2]{c}, \zeta \sqrt[2]{c}, \ldots, \zeta^{p-1} \sqrt[2]{c}) = \mathbb{Q}(\zeta, \sqrt[2]{c})$.

We claim $[K : \mathbb{Q}] = p(p-1)$. From class we know that the minimal polynomial for $\zeta$ over $\mathbb{Q}$ is $(x^p - 1)/(x - 1)$, so $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$. We are given that $x^p - c$ is irreducible over $\mathbb{Q}$, so $[\mathbb{Q}(\sqrt[2]{c}) : \mathbb{Q}] = p$. Since $K$ contains both $\mathbb{Q}(\zeta)$ and $\mathbb{Q}(\sqrt[2]{c})$, the degree $[K : \mathbb{Q}]$ is at least as big as the LCM of $p$ and $p - 1$, which is $p(p-1)$. On the other hand, $\sqrt[2]{c}$ has degree at most $p$ over $\mathbb{Q}(\zeta)$ (since it satisfies the polynomial equation $x^p - c = 0$ over $\mathbb{Q}(\zeta)$), so

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta) : \mathbb{Q}] \leq p(p-1).$$

$^1$Explicitly, they are given as follows: there are $n!$ ways to permute $\{r_j\}$, and given such a permutation there are $2^n$ ways to assign $+$ signs or $-$ signs to the values of the $r_j$’s.
Therefore \([K : \mathbb{Q}] = p(p - 1)\).

Any element \(\sigma\) of \(\text{Gal}(K/\mathbb{Q})\) must map \(\sqrt[p]{c}\) to another root of \(x^p - c\), and \(\zeta\) to another root of \((x^p - 1)/(x - 1)\). Also, \(\sigma\) is determined by its action on these two elements. There are \(p\) choices in the first case and \(p - 1\) choices in the second case, so there are at most \(p(p - 1)\) possibilities for \(\sigma\). But we know \([K : \mathbb{Q}] = p(p - 1)\), so each of these possibilities must actually occur. If we make the choice \(\sigma(\sqrt[p]{c}) = \zeta^b \sqrt[p]{c}\), and \(\sigma(\zeta) = \zeta^a\), then

\[
\sigma(\zeta^x \sqrt[p]{c}) = \zeta^{ax+b} \sqrt[p]{c}. \quad (1 \leq a \leq p - 1, \quad 0 \leq b \leq p - 1)
\]

(2)

The isomorphism from \(\text{Gal}(K/\mathbb{Q})\) to the “ax + b group mod p” is given by identifying \(\mathbb{Z}/p\mathbb{Z}\) with the multiplicative group \(G = \{1, \zeta, \zeta^2, \ldots, \zeta^{p-1}\}\). By (2), the element \(\sigma\) induces an action on \(G\) exactly equal to the “ax + b group” action on \(\mathbb{Z}/p\mathbb{Z}\), and by the previous paragraph, all possibilities for \(a\) and \(b\) actually occur in \(\text{Gal}(K/\mathbb{Q})\).