Due in class F 1 Nov. Feel free to ask for hints. Give proofs.
In the following, \( F \) is a subfield of \( \mathbb{C} \).

(1) (10 points) Let \( f \in F[X] \) be a separable polynomial of degree \( n \geq 1 \). Let \( \Sigma \subseteq \mathbb{C} \) be its splitting field, with Galois group \( \text{Aut}(\Sigma : F) \) of the extension.

Explain how a choice of labelling \( \alpha_1, \ldots, \alpha_n \) of the roots of \( f \) allows you to identify \( \text{Aut}(\Sigma : F) \) with a subgroup \( G \) of the symmetric group \( S_n \). In the following, this subgroup \( G \) will be called a Galois group of the polynomial \( f \).

Then show that for two different labellings of the roots of \( f \), the corresponding Galois groups are conjugate as subgroups of \( S_n \). (Two subgroups \( G, G' \subseteq H \) are conjugate if there exists \( h \in H \) such that \( hGh^{-1} = G' \).)

**Solution.** If the roots are labelled \( \alpha_1, \ldots, \alpha_n \), then any element \( \phi \in \text{Aut}(\Sigma : F) \) defines a permutation \( \sigma_\phi \) of the set \( \{1, \ldots, n\} \), by the formula
\[
\phi(\alpha_k) = \alpha_{\sigma_\phi(k)}.
\]
The assignment \( \phi \mapsto \sigma_\phi \) defines a homomorphism of groups \( \sigma : \text{Aut}(\Sigma : F) \rightarrow S_n \), since the identity map goes to the identity, and we have
\[
\psi(\phi(\alpha_k)) = \psi(\alpha_{\sigma_\phi(k)}) = \alpha_{\sigma_\psi(\sigma_\phi(k))},
\]
so that \( \sigma_\psi = \sigma_\psi \circ \sigma_\phi \).

The homomorphism \( \sigma \) is clearly injective, since if \( \sigma_\phi \) is the identity permutation then \( \phi(\alpha_k) = \alpha_k \) for all \( k = 1, \ldots, n \), and since \( \Sigma = F(\alpha_1, \ldots, \alpha_n) \) this implies that \( \phi \) is the identity. Thus \( \text{Aut}(\Sigma : F) \) is isomorphic to the subgroup \( G = \sigma(\text{Aut}(\Sigma : F)) \) of \( S_n \) which is the image of this homomorphism.

Suppose we have a different labelling \( \beta_1, \ldots, \beta_n \) of the roots, so that \( \beta_k = \alpha_{\gamma(k)} \) where \( \gamma \in S_n \). The homomorphism \( \tau : \text{Aut}(\Sigma : F) \rightarrow S_n \) defined by the new labelling is defined by \( \phi(\beta_k) = \beta_{\tau\gamma(k)} \). Its image is a subgroup \( G' = \tau(\text{Aut}(\Sigma : F)) \).

We compute
\[
\phi(\beta_k) = \phi(\alpha_{\gamma(k)}) = \alpha_{\sigma_\phi(\gamma(k))},
\]
so that \( \sigma_\phi \circ \gamma = \gamma \circ \tau_\phi \).

That is, \( \tau_\phi = \gamma^{-1} \circ \sigma_\phi \circ \gamma \). This shows that \( G' = \gamma^{-1}G\gamma \). \( \square \)
(2) (10 points) Consider a polynomial of the form \( f = X^4 + bX^2 + c \in F[X] \). Determine the values of \( b \) and \( c \) such that \( f \) is a separable polynomial.

**Solution.** The polynomial is separable if and only if \( c \neq 0 \) and \( b^2 - 4c \neq 0 \).

**First proof.** We have \( Df = 4X^3 + 2bX \), which factors as \( f = 2X(X^2 + \frac{b}{2}) \). For \( f \) to be relatively prime to \( Df \), we must have (i) \( f \) relatively prime to \( X \), and (ii) \( f \) relatively prime to \( X^2 + \frac{b}{2} \). For (i), \( X \nmid f \) iff \( c \neq 0 \). For (ii), apply the division algorithm to \( f \div (X^2 + \frac{b}{2}) \):

\[
X^4 + bX^2 + c = (X^2 + \frac{b}{2})(X^2 + \frac{b}{2}) + (4c - b^2)/4.
\]

Thus if \( b^2 - 4c = 0 \) then \( f \) and \( X^2 - \frac{b}{2} \) must be relatively prime, while if \( b^2 - 4c = 0 \) then \( X^2 - \frac{b}{2} \) divides \( f \).

**Second proof.** The quadratic formula gives roots

\[
X = \pm \sqrt{-b \pm \sqrt{b^2 - 4c}}.
\]

Clearly if either \( c = 0 \) or \( b^2 - 4c = 0 \) then there are repeated roots. So we need to prove the converse: if \( c \neq 0 \) and \( b^2 - 4c \neq 0 \), then there are four distinct roots here.

Let’s be more careful about how we name these roots. Make a choice \( \gamma \in \mathbb{C} \) such that \( \gamma^2 = b^2 - 4c \). Then make choices \( \alpha, \beta \in \mathbb{C} \) such that \( \alpha^2 = (-b + \gamma)/2 \) and \( \beta^2 = (-b - \gamma)/2 \). Then \( \pm \alpha, \pm \beta \) are roots of \( f \). Note that

\[
\alpha^2 + \beta^2 = -b, \quad \alpha^2 \beta^2 = c.
\]

If \( b^2 - 4c \neq 0 \), then \( \gamma \neq 0 \), and therefore \( \alpha^2 \neq \beta^2 \), which implies that \( \pm \alpha \neq \pm \beta \) (for any choice of sign). If \( c = 0 \), then \( \alpha^2 \neq 0 \) and \( \beta^2 \neq 0 \), and thus \( \alpha \neq -\alpha \) and \( \beta \neq -\beta \). Therefore the elements \( \alpha, -\alpha, \beta, -\beta \) are pairwise distinct.

\[
\square
\]

(3) (20 points) Consider a separable polynomial \( f = X^4 + bX^2 + c \in F[X] \). Pick a labelling of its roots and consider the Galois group \( G \leq S_4 \). Show that \( G \) must be conjugate to a subgroup of \( D_4 \leq S_4 \), where this group is defined by

\[
D_4 = \{ e, r, r^2, r^3, s, sr, sr^2, sr^3 \}, \quad r = (1 \ 2 \ 3 \ 4), \quad s = (2 \ 4).
\]

(This is isomorphic to a group of symmetries of a square, with vertices labelled 1 2 3 4 sequentially.)

**Solution.** As in the second proof of part (2), we have four distinct roots \( \pm \alpha, \pm \beta \), where

\[
\alpha^2 + \beta^2 = -b, \quad \alpha^2 \beta^2 = c.
\]

Note that \( \alpha^2 \neq \beta^2 \), since \( \alpha \neq \pm \beta \).

By part (1), changing the labelling of the roots replaces \( G \) with a conjugate subgroup of \( S_4 \). So to prove the claim, I just need to find a choice of labelling which identifies elements of \( \text{Aut}(\Sigma : F) \) with elements of \( D_4 \). Set

\[
\alpha_1 = \alpha, \quad \alpha_2 = \beta, \quad \alpha_3 = -\alpha, \quad \alpha_4 = -\beta.
\]

The identities involving the roots constrain the types of permutations of the roots elements \( \phi \in \text{Aut}(\Sigma : F) \) can give. For instance, \( \alpha_3 = -\alpha_1 \) and \( \alpha_4 = -\alpha_2 \) say that
\( \phi \) can either (i) preserve each of the sets \( \{\pm \alpha\}, \{\pm \beta\} \), or (ii) switch the two sets between each other.

Therefore there are at most eight possibilities, which as elements of the symmetric group may be written

\[
e, \quad (2\ 4), \quad (1\ 3), \quad (1\ 3)(2\ 4), \quad (1\ 2)(3\ 4), \quad (1\ 2\ 3\ 4), \quad (1\ 4\ 3\ 2), \quad (1\ 4)(2\ 3).
\]

You can prove this formally by a case analysis based on where \( \sigma \) goes: \( \sigma(\alpha) \) determines \( \sigma(-\alpha) \), and leaves only two possibilities for \( \sigma(\beta) \), which then determines \( \sigma(-\beta) \).

\[
\begin{array}{|c|c|c|c|c|c|c|c|}
\hline
\sigma & e & s & sr^2 & r^2 & sr^3 & r & sr \\
\hline
\sigma(\alpha_1) = \sigma(\alpha) & \alpha & \alpha & -\alpha & -\alpha & \beta & \beta & -\beta \\
\sigma(\alpha_2) = \sigma(\beta) & \beta & -\beta & \beta & -\beta & \alpha & -\alpha & \alpha \\
\sigma(\alpha_3) = \sigma(-\alpha) & -\alpha & -\alpha & \alpha & \alpha & -\beta & \beta & \beta \\
\sigma(\alpha_4) = \sigma(-\beta) & -\beta & \beta & -\beta & \beta & \alpha & \alpha & -\alpha \\
\hline
\end{array}
\]

Setting \( r = (1\ 2\ 3\ 4) \) and \( s = (2\ 4) \), we get the expressions in the bottom row of the chart. This is clearly all the elements of the subgroup \( D_4 \), as you can see by verifying that \( r^4 = e = s^2 \) and \( rs = sr^3 \).

(4) (20 points) Classify up to conjugacy in \( S_4 \) all subgroups of \( S_4 \) which are conjugate (by an element of \( S_4 \)) to a subgroup of the group \( D_4 \) of the previous problem. Give a representative subgroup of \( D_4 \) for each of these conjugacy classes. (Hint: there are exactly 7 such classes.)

**Solution.** Since by definition the subgroups we are interested in are conjugate to subgroups of \( D_4 \), all we need to do is classify the subgroups of \( D_4 \) up to conjugacy in \( S_4 \). The group \( D_4 \) has exactly 10 subgroups, but some of these turn out to be conjugate to each other in \( S_4 \). Here is a list of representatives.

(a) \( G = \{e\} \).

(b) \( G = \langle s \rangle = \{e, (2\ 4)\} \). (Note that this is conjugate in \( S_4 \) to \( \langle sr^2 \rangle \) since \( s = (2\ 4) \) and \( sr^2 = (1\ 3) \) are both 2-cycles.)

(c) \( G = \langle r^2 \rangle = \{e, (1\ 3)(2\ 4)\} \). (Note that this is conjugate in \( S_4 \) to \( \langle sr \rangle \) and to \( \langle sr^3 \rangle \), since \( r^2 = (1\ 3)(2\ 4) \), \( sr = (1\ 4)(2\ 3) \), and \( sr^3 = (1\ 2)(3\ 4) \) are all products of two disjoint 2-cycles.)

(d) \( G = \langle r \rangle = \{e, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\} \). (This is isomorphic to \( \mathbb{Z}/4 \).)

(e) \( G = \langle s, r^2 \rangle = \{e, (2\ 4), (1\ 3)(2\ 4), (1\ 3)\} \). (This is isomorphic to \( \mathbb{Z}/2 \times \mathbb{Z}/2 \).)

(f) \( G = \langle sr, r^2 \rangle = \{e, (1\ 4)(2\ 3), (1\ 3)(2\ 4), (1\ 2)(3\ 4)\} \). (This is also isomorphic to \( \mathbb{Z}/2 \times \mathbb{Z}/2 \).)

(g) \( G = D_4 \).

To see that these represent distinct conjugacy classes in \( S_4 \), it suffices to apply the conjugacy formula for cycles in symmetric groups: \( \sigma(a_1 \cdots a_k)\sigma^{-1} = (a_{\sigma(1)} \cdots a_{\sigma(k)}) \).

By inspection we see that no two of the representative subgroups listed above have matching cycle-decomposition-types for all of their elements.

Note: There are eight conjugacy classes of subgroups in \( D_4 \), but only seven when viewed as conjugacy classes in \( S_4 \). The sets \( \{\langle sr \rangle, \langle sr^3 \rangle\} \) and \( \{\langle r^2 \rangle \} \) are distinct conjugacy classes of subgroups of \( D_4 \), but lie in the same conjugacy class of subgroups of \( S_4 \).
(5) (20 points) Consider an irreducible polynomial \( f = X^4 + bX^2 + c \in \text{Irred}(F) \). Show that its Galois group \( G \) is isomorphic to \( \mathbb{Z}/2 \times \mathbb{Z}/2 \) if and only if \( c = u^2 \) for some \( u \in F \), and is isomorphic to \( \mathbb{Z}/4 \) if and only if \( (b^2 - 4c)/c = v^2 \) for some \( v \in F \).

**Solution.** Because \( f \) is irreducible it must be separable, since we are in characteristic 0. As proved earlier there exists a labelling of the roots of the form

\[
\alpha_1 = \alpha, \quad \alpha_2 = \beta, \quad \alpha_3 = -\alpha, \quad \alpha_4 = -\beta,
\]

so that \( \alpha^2 + \beta^2 = -b \) and \( \alpha^2\beta^2 = c \), and with this labelling Galois group \( G \) is a subgroup of \( D_4 \).

Since \( f \) is irreducible, the Galois group \( G \) must act transitively on the roots, i.e., \( G\alpha = \{ \pm\alpha, \pm\beta \} \). This means that \( G \) must fall in one of the cases (d), (f), or (g) of the solution to part (4), since these are the only cases where the subgroup \( G \) acts transitively on the roots.

Case (f) happens if and only if \( \alpha\beta \in F \), since the products of two disjoint 2-cycles in \( D_4 \) fix this element, but the 4-cycles in \( D_4 \) send \( \alpha\beta \mapsto -\alpha\beta \). If \( \alpha\beta \in F \), then certainly \( c = \alpha^2\beta^2 = (\alpha\beta)^2 \) is a square of an element of \( F \). Conversely, if \( c = u^2 \) for some \( u \in F \), then \( c = (\alpha\beta)^2 \) implies \( \alpha\beta = \pm u \), so \( \alpha\beta \in F \).

Case (d) happens if and only if \( \epsilon := \alpha/\beta - \beta/\alpha = (\alpha^2 - \beta^2)/(\alpha\beta) \in F \), since the 4-cycles in \( D_4 \) fix this element, but \( (1\ 2)(3\ 4) \) and \( (1\ 4)(2\ 3) \) send \( \epsilon \mapsto -\epsilon \). Compute that

\[
e^2 = \frac{(\alpha^2 - \beta^2)^2}{(\alpha\beta)^2} = \frac{\alpha^4 - 2\alpha^2\beta^2 + \beta^4}{\alpha^2\beta^2} = \frac{(\alpha^2 + \beta^2)^2 - 4\alpha^2\beta^2}{\alpha^2\beta^2} = \frac{b^2 - 4c}{c}.
\]

If \( \epsilon \in F \), then certainly \( (b^2 - 4c)/c = \epsilon^2 \) is a square of an element of \( F \). Conversely, if \( (b^2 - 4c)/c = \epsilon^2 \) for some \( v \in F \), then \( (b^2 - 4c)/c = \epsilon^2 \) implies \( \epsilon = \pm v \), so \( \epsilon \in F \).

**Remark.** Irreducibility is important here. The same ideas prove that (for any separable \( f \), not necessarily irreducible), that \( c \) is a square in \( F \) iff \( G \) is conjugate (in \( S_4 \)) to a subgroup of \( \langle sr, r^2 \rangle \), and that, \( (b^2 - 4c)/c \) is a square in \( F \) iff \( G \) conjugate (in \( S_4 \)) to a subgroup of \( \langle r \rangle \).

\( \Box \)

(6) (20 points) For each of the 7 representative subgroups you described in part (4), find a separable polynomial of the form \( f = X^4 + bX^2 + c \in \mathbb{Q}[X] \), together with a labelling of its roots, which has the given subgroup as its Galois group.

**Solution.**

(a) \( G = \{ e \} \). Any polynomial of this form which splits over \( \mathbb{Q} \) works, e.g., \( f = (X^2 - 1)(X^2 - 4) = X^4 - 5X^2 + 4 \), with any labelling of the roots \( \pm 1, \pm 2 \).

(b) \( G = \langle s \rangle = \langle (2\ 4) \rangle \). Any polynomial of this form which factors over \( \mathbb{Q} \) into an irreducible quadratic and two linear terms works, e.g., \( f = (X^2 - 1)(X^2 + 1) = X^4 - 1 \), with roots labelled in order: \( 1, i, -1, -i \).

(c) \( G = \langle r^2 \rangle = \langle (1\ 3)(2\ 4) \rangle \). For example, \( f = (X^2 + 1)(X^2 + 4) = X^4 + 5X^2 + 4 \), with roots labelled in order: \( i, 2i, -i, 2i \).

Any product of two irreducible quadratics which have the same splitting field works.

Another good example is \( X^4 + X^2 + 1 \), with roots \( \pm \omega, \pm \omega^2 \), which you can list in the order: \( \omega, \omega^2, -\omega, -\omega^2 \). Note that none of the roots are squareroots of elements of \( \mathbb{Q} \), but the polynomial still factors over \( \mathbb{Q} \) as \( (X^2 + X + 1)(X^2 - X + 1) \).
(d) \( G = \langle r \rangle = \langle (1\ 2\ 3\ 4) \rangle \). For example, \( f = X^4 + 5X^2 + 5 \), with roots labelled in order: \( \zeta - \zeta^{-1}, \zeta^2 - \zeta^{-2}, \zeta^{-1} - \zeta, \zeta^2 - \zeta^2 \), where \( \zeta = e^{2\pi i/5} \). The splitting field \( \Sigma : \mathbb{Q} \) is generated by \( \zeta \), and \( r \in G \) sends \( \zeta \mapsto \zeta^2 \). You can also write the roots as \( \pm \sqrt{-\frac{5\pm\sqrt{5}}{2}} \), which you can list in the order: \( i\sqrt{\frac{5+\sqrt{5}}{2}}, i\sqrt{\frac{5-\sqrt{5}}{2}}, -i\sqrt{\frac{5+\sqrt{5}}{2}}, -i\sqrt{\frac{5-\sqrt{5}}{2}} \), where in each case the squareroot is a positive real number.

Observe that \( f \in \text{Irred}(\mathbb{Q}) \) (by Eisenstein), and that \( (b^2 - 4c)/c = 1^2 \) is a square of an element of \( \mathbb{Q} \).

(e) \( G = \langle s, r^2 \rangle = \langle (2\ 4), (1\ 3) \rangle \). For example, \( f = (X^2 + 1)(X^2 - 2) = X^4 - X^2 - 2 \) with roots labelled in order: \( i, \sqrt{2}, -i, -\sqrt{2} \).

Any product of two irreducible quadratics which have different splitting fields works.

(f) \( G = \langle sr, r^2 \rangle = \langle (1\ 2)(3\ 4), (1\ 4)(2\ 3) \rangle \). For example, \( f = X^4 - 2X^2 + 9 \) with roots labelled in order: \( \sqrt{2} + i, \sqrt{2} - i, -\sqrt{2} - i, -\sqrt{2} + i \).

Observe that \( f \in \text{Irred}(\mathbb{Q}) \), and that \( c = 3^2 \) is a square of an element of \( \mathbb{Q} \). To prove that \( f \) is irreducible: clearly none of the roots are in \( \mathbb{Q} \), so it suffices to show there is no irreducible quadratic which is a factor. Such a quadratic would have the form \( (X - u)(X - v) = X^2 - (u + v)X + uv \) where \( u, v \) are two distinct roots, and its easy to check by explicit calculation that there is no such pair with both \( u + v, uv \in \mathbb{Q} \).

Another good examples of \( f \) is \( X^4 + 1 \) with roots \( (\pm 1 \pm i)/\sqrt{2} \), which you can list in order: \( (1 + i)/\sqrt{2}, (1 - i)/\sqrt{2}, (-1 - i)/\sqrt{2}, (-1 + i)/\sqrt{2} \).

(g) \( G = D_4 \). For example, \( f = X^4 - 2 \) with roots labelled in order: \( \sqrt{2}, i\sqrt{2}, -\sqrt{2}, -i\sqrt{2} \).

Observe that \( f \in \text{Irred}(\mathbb{Q}) \) (e.g., by Eisenstein), and that neither \( (b^2 - 4c)/c = -4 \) nor \( c = -2 \) are squares of elements of \( \mathbb{Q} \).

\( \square \)

Additional remark about factorization of quartics. To show \( f = X^4 + bX^2 + c \in F[X] \) is irreducible, it suffices to show

1. \( f \) has no root in \( F \), and
2. \( f \neq gh \) for any monic quadratics \( g, h \in F[X] \).

If \( f \) is separable, then we know the roots of \( f \) have form \( \{\pm \alpha, \pm \beta\} \), with \( \alpha^2 + \beta^2 = -b \) and \( \alpha^2\beta^2 = c \). Then \( f = (X - \alpha)(X + \alpha)(X - \beta)(X + \beta) \), so there are exactly three ways to factor \( f \) into monic quadratics (up to reordering):

(a) \( f = (X^2 - \alpha^2)(X^2 - \beta^2) \).
(b) \( f = (X^2 - (\alpha + \beta)X + \alpha\beta)(X^2 + (\alpha + \beta) + \alpha\beta) \).
(c) \( f = (X^2 - (\alpha - \beta)X - \alpha\beta)(X^2 + (\beta - \alpha)X - \alpha\beta) \).

These are factorizations over \( F \) iff (in each case):

1. \( \alpha^2 \in F \iff \beta^2 \in F \).
2. \( \alpha\beta, \alpha + \beta \in F \).
3. \( \alpha\beta, \alpha - \beta \in F \).
For instance, \( f = X^4 + X^2 + 1 \in \mathbb{Q}[X] \) has roots \( \pm \omega, \pm \omega^2 \), so it factors as in (b) or (c) (depending on how you label the roots), but not as in (a). On the other hand, \( g = X^4 + 5X^2 + 4 \in \mathbb{Q}[X] \) has roots \( \pm i, \pm 2i \), so it factors as in (a) but not as in (b) or (c).