Notation: \( \mathbb{C} \) and \( \mathbb{R} \) denote the fields of real and complex numbers, \( \mathbb{F}_p \) denotes the finite field with \( p \) elements, and \( S_n \) and \( A_n \) denote the symmetric and alternating groups.

**Problem 1.** Give examples of groups \( G_1 \) and \( G_2 \) of order 8 such that:

1. \( G_1 \) is a semi-direct product of \( C_2 \) and \( C_4 \), with \( C_4 \) normal, but is not isomorphic to the direct product \( C_2 \times C_4 \).
2. \( G_2 \) contains a cyclic group of order 4, but is not isomorphic to a semi-direct product of \( C_2 \) and \( C_4 \).

Here \( C_n \) denotes the cyclic group of order \( n \). Be sure to rigorously justify your assertions.

**Solution.** Let \( G_1 \) be the dihedral group with 8 elements (the group of symmetries of a square). The group of rotations of the square forms a normal copy of \( C_4 \), and any reflection forms a copy of \( C_2 \) with trivial intersection with it, so \( G_1 = C_2 \rtimes C_4 \). Since \( G_1 \) is not abelian, it is not the direct product of \( C_2 \) and \( C_4 \).

Take \( G_2 = C_8 \). Then \( G_2 \) has a normal copy of \( C_4 \), with quotient \( C_2 \), but the only order 2 element of \( G_2 \) lies in \( C_4 \), so \( G_2 \) is not a semidirect product. (Alternatively, one could use the quaternion 8 group.)

**Problem 2.** Let \( G \) be a finite group of order \( n \). Let \( G \) act on itself by left multiplication, and let \( \phi : G \to S_n \) be the homomorphism associated to this action. Show that \( \text{im}(\phi) \subset A_n \) if and only if (1) \( n \) is odd; or (2) \( n \) is even and the 2-Sylow subgroups of \( G \) are not cyclic.

**Solution.** Let the order of \( G \) be \( n = 2^k m \), with \( m \) odd.

First, suppose that \( n \) is even and that the 2-Sylow subgroups of \( G \) are cyclic. Let \( g \) generate a 2-Sylow. Then the action of \( g \) on \( G \) is by \( m \) cycles of length \( 2^k \), so \( g \) has sign \((-1)^m = -1\) and is not alternating.

We now must show that the action lands in \( A_n \) in all other cases. If \( |G| \) is odd, then every element of \( g \) acts on \( G \) by a collection of cycles of odd length, and hence has even sign. Now suppose that \( |G| \) is even, and that the 2-sylows of \( G \) are not cyclic. Let \( g \) be an element of \( G \) of order \( 2^a b \), with \( b \) odd. Then \( g^b \) has order \( 2^a \) and hence is contained in a 2-Sylow; since the 2-Sylow’s aren’t cyclic, we deduce that \( a < k \). Then \( g \) acts on \( G \) by \( 2^{k-a} \frac{m}{b} \) many cycles of the same length. \( 2^{k-a} \frac{m}{b} \) is even, so this permutation is in \( A_n \).
Problem 3. Let $n$ be a positive integer. Show that $\mathbb{C}(t)/\mathbb{R}(t^n)$ is a Galois extension, and determine its Galois group. Here $t$ is an indeterminate and $\mathbb{C}(t)$ is the rational function field.

Solution. Let $\zeta$ be a primitive $n$-th root of unity; we claim that the Galois group is generated by the symmetries $\sigma(t) = \zeta t$ and the symmetry $\rho(z) = \overline{z}$ of $\mathbb{C}$. These generate a group isomorphic to the dihedral group of order $2n$, since $\sigma^n = \rho^2 = 1$ and $\rho \sigma \rho^{-1} = \sigma^{-1}$.

All of these are clearly field symmetries which preserve the subfield $\mathbb{R}(t)$, and $[\mathbb{C}(t) : \mathbb{R}(t^n)] = 2n$, so this is all the symmetries and the extension is Galois.

Problem 4. Suppose that $p$ is a Fermat prime, i.e., $p$ has the form $2^r + 1$ for some positive integer $r$. Let $a, b \in \mathbb{F}_p^\times$. Show that either $a = b^n$ for some integer $n$, or $b = a^m$ for some integer $m$.

Solution. The multiplicative group of a finite field is cyclic, so $\mathbb{F}_p^\times \cong C_{2r}$. The subgroups of $C_{2r}$ are all of the form $C_{2s}$ for $0 \leq s \leq r$. Let $a$ and $b$ generate subgroups of orders $2^s$ and $2^t$ respectively. Then, if $s \geq t$, we have $b \in \langle a \rangle$ and, if $t \leq s$, we have $a \in \langle b \rangle$.

Problem 5. Let $F$ be a field of characteristic $\neq 2$, and let $a, b,$ and $c$ be non-zero elements of $F$ such that $a, b, c, ab, ac, bc,$ and $abc$ are all non-squares in $F$. Show that $F(\sqrt{a}, \sqrt{b}, \sqrt{c})$ is a degree 8 extension of $F$.

Solution. Look at the chain of extensions $F \subseteq F(\sqrt{a}) \subseteq F(\sqrt{a}, \sqrt{b}) \subseteq F(\sqrt{a}, \sqrt{b}, \sqrt{c})$. Each extension is either of degree 1 or 2, and we want to show that they are all of degree 2. By assumption, $a$ is not square in $F$, so $[F(\sqrt{a}) : F] = 2$. It remains to see that $b$ is not square in $F(\sqrt{a})$ and that $c$ is not square in $F(\sqrt{a}, \sqrt{b})$.

Let’s first see that $b$ is not square in $F(\sqrt{a})$. Indeed, suppose to the contrary that $(x + y\sqrt{a})^2 = b$. Then $x^2 + ay^2 = b$ and $2xy = 0$, so either $x = 0$ or $y = 0$. Then we get either $x^2 = b$ or $ay^2 = b$, so either $b$ or $ab$ is square in $F$, which we assumed was not true.

Now, let us see that $c$ is not square in $F(\sqrt{a}, \sqrt{b})$. At this point, we know that $[F(\sqrt{a}, \sqrt{b}) : F(\sqrt{a})] = 2$, so every element of $F(\sqrt{a}, \sqrt{b})$ can be written uniquely in the form $\alpha + \beta\sqrt{b}$ for $\alpha$ and $\beta \in F(\sqrt{a})$. Suppose, for the sake of contradiction, that $(\alpha + \beta\sqrt{b})^2 = c$ for $\alpha$ and $\beta$ in $F(\sqrt{a})$. Then, as before, either $\alpha = 0$ or $\beta = 0$, so we deduce that either $c$ or $bc$ is a square in $F(\sqrt{a})$. Then, let $(x + y\sqrt{a})^2$ be $c$ or $bc$. 


accordingly. As before, we deduce that $x = 0$ or $y = 0$, and so either $c$, $bc$, $ac$ or $abc$ is square in $F$, which we assumed not to be so.