SOLUTION SHEET 11:

Problem 1: Recall that $\Delta(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2 \in \mathbb{Q}$ where α_i, α_j are roots of f.

It is not hard to see that $f'(\alpha_j) = \prod_{i=1, i\neq j}^{n} (\alpha_j - \alpha_i)$. Now notice that

$$N_{L/K}(f'(\alpha)) = \prod_{\sigma \in Gal(L/K)} \sigma(f'(\alpha)) = \prod_{\substack{\sigma \in Gal(L/K) \\ \sigma(\alpha_j) \neq \alpha_j}} \sigma(f'(\alpha))$$

$$= \prod_{\ell} \sigma^{\ell}(f'(\alpha)) \quad \text{where } \sigma^{\ell}(\alpha) = \alpha_\ell$$

therefore $N_{L/K}(f'(\alpha)) = \prod_j f'(\alpha_j) = \prod_j \prod_{i=1, i\neq j}^{n} (\alpha_j - \alpha_i) = (-1)^{\frac{n(n-1)}{2}} \cdot \Delta(f)$.

Problem 2:

(i) To see that f is irr. reduce it modulo 3. Note that f doesn't have a root mod 3. It can also be shown by explicit computation that it can't be written as a product of two quadratic polynomials.

Computing the resultent we obtain, $r(X) = X^3 - X^2 - 4X + 3$. To see that $r(X)$ is irr. reduce it modulo 2 & observe that there are no roots. This shows that $G_f := Gal(SF_{\mathbb{Q}}(f)/\mathbb{Q})$ is either S_4 or A_4. Recall that $G_f = S_4 \Leftrightarrow [SF_{\mathbb{Q}}(r) : \mathbb{Q}] = 6 \Leftrightarrow \Delta(r)$ is not a square. Using a change of variables and the formulas from the course we can show that $\Delta(r) = 257$ which is not a square. $\Rightarrow G_f = S_4$.

(ii) Let us recall somethings from the lecture. Let $f = \prod_{i=1}^{4} (x - \alpha_i)$ be a quartic poly. and define $\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$, $\beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4$, $\beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$ and define $r(X) = (X - \beta_1)(X - \beta_2)(X - \beta_3)$. Then the extension $SF_{\mathbb{Q}}(r(X))/\mathbb{Q}$ gives us information about $Gal(SF_{\mathbb{Q}}(f)/\mathbb{Q})$ as discussed in the course.
Now the coefficients of f can be expressed in terms of α_i. Likewise the coeff. of r can be expressed in β_i which can be expressed in terms of α_j. Therefore we can express the coefficients of $r(X)$ by those of $f(X)$.
If $f(X) = X^4 + aX^3 + bX^2 + cX + d$ then $r(X)$ is given by

$$r(X) = X^3 - bX^2 + (ac - 4d)X - (a^2 d + c^2 - 4bd).$$

In our case, $f(X) = X^4 - 4X^3 + 4X^2 + 6$ thus $r(X) = X^3 - 4X^2 - 24X$ and $SF_{\mathbb{Q}}(r) = SF_{\mathbb{Q}}(X^2 - 4X - 24)$ now the roots of this polynomial are not in $\mathbb{Q}$ thus $[SF_{\mathbb{Q}}(r(X)) : \mathbb{Q}] = 2$.

Indeed, it can be seen that the roots of $X^2 - 4X - 24$ are $\frac{4 \pm \sqrt{7 \cdot 16}}{2}$ thus $SF_{\mathbb{Q}}(r) = \mathbb{Q}(\sqrt{7})$. Now

$$G_f \cong [SF_{\mathbb{Q}}(f) : \mathbb{Q}] = \begin{cases} D_4 & \text{if } f \text{ is irr. over } \mathbb{Q}(\sqrt{7}) \\ C_4 & \text{if } f \text{ is reducible} / \mathbb{Q}(\sqrt{7}). \end{cases}$$

To see that $f/\mathbb{Q}(\sqrt{7})$ is irreducible first note that if f only has one root in $\mathbb{Q}(\sqrt{7})$ then $[SF_{\mathbb{Q}}(f) : \mathbb{Q}(\sqrt{7})] = 3$ or 6 but $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{7}) \subseteq SF_{\mathbb{Q}}(f)$ is an intermediate extension and $[SF_{\mathbb{Q}}(f) : \mathbb{Q}] = 4$ or 8 thus it is not possible. Therefore if $f/\mathbb{Q}(\sqrt{7})$ is reducible then it can be written as a product of two polynomials of degree 2 in $\mathbb{Q}(\sqrt{7})$. It can be shown by direct computation that it is not possible.

Problem 3: For $\alpha=1$, $SF_{\mathbb{Q}}(f_\alpha)=SF_{\mathbb{Q}}(x^5-1)$ therefore $G_1\cong \mathbb{Z}/4\mathbb{Z}$. For $\alpha=0$ $f_0(x)=x^4+x^3+x+x=x.(x^3+x^2+x+1) \Rightarrow SF_{\mathbb{Q}}(f_0)=\mathbb{Q}(\omega_4)$ where ω_4 is a 4th root of unity & $G_0\cong\mathbb{Z}/3\mathbb{Z}$. For $\alpha=-4$ $f_{-4}(x)=x^4+x^3+x^2+x-4$ and 1 is a root of $f_{-4}(x)$. Let us proceed by polynomial division.

$$
\begin{array}{r|l}
x^4+x^3+x^2+x-4 & x-1 \\
\underline{x^4-x^3} & x^3+2x^2+3x+4 \\
2x^3+x^2+x-4 & \\
\underline{2x^3-2x^2} & \\
3x^2+x-4 & \\
\underline{3x^2-3x} & \\
4x-4 &
\end{array}
$$

hence $SF_{\mathbb{Q}}(f_{-4})=SF_{\mathbb{Q}}(x^3+2x^2+3x+4)$. Let $g=x^3+2x^2+3x+4$. Note that it is irreducible as its reduction modulo 3 which is $\bar{g}=x^3+2x^2+1$ is irreducible. Thus by the course $Gal(SF_{\mathbb{Q}}(f_{-4})/\mathbb{Q})\cong A_3$ or S_3.

Finally $f_{-1}(x)=x^4+x^3+x^2+x-1$ is irreducible as its reduction modulo 2 is. We compute that $r_{-1}(x)=x^3-x^2+4x-5$ which is also irreducible as its reduction modulo 2 is. As r_{-1} is irreducible, $[SF_{\mathbb{Q}}(r_{-1}):\mathbb{Q}]\in\{3,6\}$ and therefore $Gal(SF_{\mathbb{Q}}(f)/\mathbb{Q})\cong S_4$ or A_4

Problem 4: Recall that Galois extensions of finite fields are always cyclic. As S_n & A_n are not cyclic for $n\geq 4$ $Gal(SF_{\mathbb{F}_p}(f)/\mathbb{F}_p)\ncong S_n$ or A_n the same argument shows that $Gal(SF_{\mathbb{F}_p}(f)/\mathbb{F}_p)\ncong S_3$. Finally as $A_3=\mathbb{Z}/3\mathbb{Z}$ it is easy to find examples where $Gal(SF_{\mathbb{F}_p}(f)/\mathbb{F}_p)\cong A_3$.

Problem 5: First it can be shown that the discriminant of a polynomial x^5+ax+b is $2^8a^5+5^5b^4$. To learn more about how to compute discriminants you may see for instance, p. 258, "Basic Algebra I" by Jacobson.

Now as seen in the course, the Galois group of the splitting field over $\mathbb{Q}$ of a cubic or a quartic is a subgroup of the alternating group A_3 and A_4 respectively if and only if the discriminant is a square in $\mathbb{Q}$. This in fact holds for polynomials of arbitrary degree.

Computing the discriminant of $x^5+20x+16$ we obtain $\Delta=2^{16}.5^6$. which is a square thus $G:=Gal(SF_{\mathbb{Q}}(f)/\mathbb{Q})\subseteq A_5$.

We also know that $|G|\geq 15$ therefore the index of G in A_5 is at least 4. Here is the claim that says that this is not possible.

Claim: Let G be a finite non-abelian simple group. Let H be a proper subgroup of G. Then $[G:H]\geq 5$.

Proof: G acts on the left cosets of H by multiplication. The action is non-trivial as $H\neq G$. As G is simple this action has trivial kernel and it defines an embedding $G\hookrightarrow S_{[G:H]}$. Now S_n doesn't have a non-abelian simple subgroup for $n\leq 4$ thus $n\geq 5$.

This shows that G is not a proper subgroup of A_5 and $G=A_5$.