10.2 Let $\zeta = e^{\frac{2\pi i}{17}}, \sigma : \zeta \mapsto \zeta^3, K = \mathbb{Q}(\zeta)$, and the intermediate fields $\mathbb{Q} \subset L_1 \subset L_2 \subset L_3 \subset K$ which correspond to the subgroups of $\mathbb{Z}\backslash 16\mathbb{Z}$. We want to construct the generators of L_2 explicitly. Note that $[L_2 : \mathbb{Q}] = 4$, and $L_2 = K^{<\sigma^4>}$, therefore we must find 4 elements which are invariant under σ^4. We know from artin that σ has the following cycle on the exponents of ζ: $[1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1]$, Thus counting off every 4th one from 3 yields $[1, 13, 16, 4]$. Therefore the number $\alpha_1 = \zeta + \zeta^{13} + \zeta^{14} + \zeta^4$ is invariant under σ^4. Furthermore we can construct $\alpha_2, \alpha_3, \alpha_4$ by $\sigma^{i-1}(\alpha_1) = \alpha_i$ for $i = 2, 3, 4$, which exactly correspond to the cosets of $[1, 13, 16, 4]$, $\alpha_1 : [1, 13, 16, 4], \alpha_2 : [3, 5, 14, 12], \alpha_3 : [9, 15, 8, 2], \alpha_4 : [10, 11, 7, 6]$. Note that $\mathbb{Q}$ is the field which is fixed by σ, therefore by theorem 16.5.2, since the orbit of α_1 is $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$, thus the irreducible polynomial over $\mathbb{Q}$ for α_1 is degree 4, and as established before $[L_2 : \mathbb{Q}] = 4$. Additionally since $\mathbb{Q}(\alpha_1)$ contains a single root of the irreducible polynomial of α_1 then it contains $\alpha_2, \alpha_3, \alpha_4$. Thus $\mathbb{Q}(\alpha_1) = L_2$, making α_1 the generator of L_1.

10.9b Let $\zeta = e^{\frac{2\pi}{p} i}$. Note that $(-1)^{\frac{p(p-1)}{2}} \prod_{k=0}^{p-1} f'(\zeta) = (-1)^{\frac{p(p-1)}{2}} \prod_{i=0}^{p-1} p\zeta^{k(p-1)} = (-1)^{\frac{p(p-1)}{2}} p^p \zeta^{\frac{p(p-1)^2}{2}} = (-1)^{\frac{p(p-1)}{2}} p^p 1^{\frac{(p-1)^2}{2}} = (-1)^{\frac{p(p-1)}{2}} p^p$. Additionally we know that the discriminate is equivalent to $\prod_{i<j}^{p} (\zeta^i - \zeta^j)^2$, therefore trivially we can take the square root as $\prod_{i<j}^{p} (\zeta^i - \zeta^j)$. Thus we know that $\mathbb{Q}(\zeta)$ contains $\sqrt{(-1)^{\frac{p(p-1)}{2}} p^p}$. Furthermore since we assume p is odd then there exists $p = 2n + 1$, thus we have $p^n \sqrt{(-1)^{\frac{p(p-1)}{2}} p}$, and since $p^n \in \mathbb{Q}$ then our quadratic extension contains $\sqrt{(-1)^{\frac{p(p-1)}{2}} p}$. If $p \equiv 1 \mod 4$ then $\frac{p-1}{2} \equiv 0 \mod 2$, thus $\sqrt{(-1)^{\frac{p(p-1)}{2}} p} = \sqrt{p}$. If $p \equiv 3 \mod 4$ then $\frac{p-1}{2} \equiv 1 \mod 2$, thus $\sqrt{(-1)^{\frac{p(p-1)}{2}} p} = \sqrt{-p}$.

11.1 Let $f(x)$ be a cubic in $F[x]$, and let K be the splitting field of f. Suppose that the discriminant of f is not a square in F. We want to show that we can't obtain the roots by adjoining a cube root. Suppose for contradiction that we can. We know that the discriminate being square free implies that $G(K/F) = S_3$. Furthermore if our roots are contained within $K = \sqrt[3]{l}, l \in F$ then they are of the form $u_i = a_i + b_i \sqrt[3]{l} + c_i \sqrt[3]{l^2}$. The issue is that there is only 1 F-automorphisms of K, because if we send $\sqrt[3]{l} \mapsto \sqrt[3]{l^2}$ would imply that $\sqrt[3]{l^2} \mapsto l\sqrt[3]{l}$, which would contradict it being an automorphism unless $l^2 = l$, which only occurs if $l = 1$, contradicting that one adjoined a cube root. Since we only have a field with 1 automorphism and we know that we must have 6 automorphisms then we have a contradiction.

12.4 a We want to show that the field of rational functions on n variable, $F(u)$, is the galois extension of $F(s_1, \cdots, s_n)$ where s_i is the ith symmetric function on $u_1, \cdots, u_n$, and that $G(F(u)/F(s_1, \cdots, s_n)) = S_n$. Observe that $F(u)$ is a galois extension of $F(s_1, \cdots, s_n)$ since

$$(x - u_1) \cdots (x - u_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^{n \mod 2} s_n,$$

and clearly this polynomial only factors if $u_1, \cdots, u_n$ are contained in the field. Furthermore, our polynomial above is invariant under any possible permutation of the roots, thus the galois group must be S_n.

c Let G finite group G with $|G| = n$. Note that by Cayley's theorem that G has an embedding in S_n as a subgroup. Therefore let $F(s_1, \cdots, s_n)$ be the base field. We know by the main theorem of Galois theory that the fixed field $F(u)^G$ is a subfield of $F(u)$ and $G(F(u)/F(u)^G) = G$. This demonstrates the desired result.