Facts, results that can be used on Test 2.

Here is a list of results, facts that you can use on Test 2. Below F is a field, and K is an extension field of F. You can take these into Test 2, and refer to any of them (by number) in your proofs. I will also distribute a copy of this at the beginning of Test 2 (in case you don't bring it to the exam for some reason.)

1. "Roots-to-Roots": Suppose $[K : F]$ is finite. Let $\gamma \in K$ with minimal polynomial $m_{\gamma,F}(x)$: If $\sigma \in Aut(K/F)$, then $\sigma(\gamma)$ is also a root of $m_{\gamma,F}(x)$.

2. Let $t(x) \in F[x]$ be a polynomial, and let K/F be a splitting field of $t(x)$. Let $\{r_1, \ldots, r_k\}$ be the roots of $t(x)$. Thus $K = F(r_1, \ldots, r_k)$.

   (a) $Aut(K/F)$ acts on $\{r_1, \ldots, r_k\}$—it permutes the elements of $\{r_1, \ldots, r_k\}$. (This is just a special case of "Roots-to-Roots" above.)

   (b) $Aut(K/F)$ acts **faithfully** on $\{r_1, \ldots, r_k\}$—meaning that if $\sigma \in Aut(K/F)$, and for all $i \in \{1, \ldots, k\}$, we have $\sigma(r_i) = r_i$, then $\sigma = id_K$—from which it follows that $Aut(K/F)$ can be embedded in S_k, the symmetric group on k letters.

3. Let $n \in \mathbb{N}$. Recall that $\Phi_n(x) = (x - \alpha_1)\ldots(x - \alpha_{\phi(n)})$, where $\{\alpha_1, \ldots, \alpha_{\phi(n)}\}$ is the set of all primitive n-th roots of unity. Then $\Phi_n(x) \in \mathbb{Q}[x]$ is irreducible and separable, and $\deg(\Phi_n(x)) = \phi(n)$, the Euler number of n.

4. Finite fields: If K is a finite field, then the following hold. Let p be prime, and let F_p denote the p-element field.

   (a) There exist a prime number p and a positive integer n such that $|K| = p^n$.

   (b) K is an extension of the field F_p (also known as $\mathbb{Z}_p$).

   (c) For all $c, d \in K$, $(c + d)^p = c^p + d^p$.

5. The following four properties are equivalent for a finite dimensional field extension K/F:

   (a) K/F is Galois. (That is, $|Aut(K/F)| = [K : F]$.)

   (b) The fixed field of $Aut(K/F)$ is F.

(c) For $\gamma \in K$, $m_{\gamma,F}(x) \in F[x]$ is separable and all roots of $m_{\gamma,F}(x)$ are in K.

(d) K is a splitting field of a separable polynomial $t(x) \in F[x]$.

6. Let K be a splitting field of a polynomial $t(x) \in F[x]$. Recall that $Sub(Aut(K/F))$ is the set of all subgroups of $Aut(K/F)$, a set that is partially ordered under set-inclusion, and that $Subf(K/F)$ is the set of all *intermediate fields*, the fields $\{J : F \subseteq J \subseteq K$ where J is a field$\}$.

   Let $\iota : Sub(Aut(K/F)) \to Subf(K/F)$ be the following map: For all $H \in Sub(Aut(K/F))$, $\iota(H)$ is the fixed field of H. The Fundamental Theorem of Galois Theory states, in part, that

   (a) ι is an order-reversing bijection, and

   (b) if $H_1 \leq H_2$ in $Sub(G)$, J_2 is the fixed field of H_2, and J_1 the fixed field of H_1, then $[J_1 : J_2] = [H_2 : H_1]$.