Math 418, Spring 2024 – Practice Problems 2

13.2.6 *Prove directly from the definitions that the field $F(a_1, \ldots, a_n)$ is the composite of the fields $F(a_1), F(a_2), \ldots, F(a_n)$.*

Solution. $F(a_1, ldots, a_n)$ is the smallest field containing $F, a_1, \ldots, a_n$. This must contain $F(a_1), \ldots, F(a_n)$, so it contains their composite. Conversely, any field containg all of $F(a_1), \ldots, F(a_n)$ contains F and $a_1, \ldots, a_n$, so it contains $F(a_1, \ldots, a_n)$, and the composite by definition is such a field.

13.3.1 *Prove that it is impossible to construct the regular 9-gon.*

Solution. Consider the triple angle formula for cosines: $\cos\theta = 4\cos^3(\theta/3) - 3\cos(\theta/3)$. Substituting $\theta = \frac{2\pi}{3}$, we see that $\cos\frac{2\pi}{9}$ is a root of $4x^3 - 3x + \frac{1}{2}$, so $2\cos\frac{2\pi}{9}$ is a root of $x^3 - 3x + 1$. this is irreducible by the rational root theorem, so $[\mathbb{Q}(\cos\frac{2\pi}{9}) : \mathbb{Q}] = 3$, which is not a power of 2. Since the interior angle of a regular 9-gon has angle $\pi - \frac{2\pi}{9}$, the regular 9-gon is not constructible. (See Dummit and Foote, pp. 534 for more details on this argument).

13.4.4 *Determine the splitting field and its degree over $\mathbb{Q}$ for $f(x) = x^6 - 4$.*

Solution. This is a difference of squares, so $f(x) = (x^3 + 2)(x^3 - 2)$. The roots of $x^3 - 2$ are $\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}$, where ζ is a primitive cube root of 1 and $\sqrt[3]{2}$ is the unique positive real cube root of 2. The roots of $x^3 - 2$ are cube roots of -2 i.e. the negatives of the cube roots of 2. Thus, the splitting field of $f(x)$ is just the splitting field of $x^3 - 2$ i.e. $\mathbb{Q}(\zeta, \sqrt[3]{2})$, and this has degree 6.

13.5.2 *Find all irreducible polynomials of degrees 1, 2 and 4 over $\mathbb{F}_2$ and prove that their product is $x^{16} - x$.*

Solution. This is a simple (if tedious) check. I'll mention that it's an example of a more general phenomenon, which we'll cover soon.

13.5.4 *Let $a > 1$ be an integer. Prove for any positive integers n, d that d divides n if and only if $a^d - 1$ divides $a^n - 1$. Conclude in particular that $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ if and only if d divides n.*

Solution. The first statement follows by setting $x = a$ in Problem 13.5.3, which was a homework problem. The second follows from setting $a = p$: $p^d - 1$ divides $p^n - 1$ if an only if $d|n$. Therefore, applying 13.5.3 again, $x^{p^d-1} - 1$ divides $x^{p^n-1} - 1$ if and only if $d|n$. Multiplying by x, $x^{p^d} - x$ divides $x^{p^n} - x$ if and only if $d|n$. Now the result follows since $\mathbb{F}_{p^m}$ is the set of all roots of $x^{p^m} - x$ lying in a fixed algebraic closure $\overline{\mathbb{F}_p}$.

13.6.6 *Prove that for n odd, $n > 1$ that $\Phi_{2n}(x) = \Phi_n(-x)$*

Solution. The map $\zeta \mapsto -\zeta$ is a bijection between primitive roots of Φ_n and Φ_{2n}, and there are an even number of each (check these facts yourself). Therefore,

$$\Phi_n(-x) = \prod_{\zeta \in \mu_n} (-x - \zeta) = (-1)^{|\mu_n|} \prod_{\zeta \in \mu_n} (x + \zeta) = \prod_{\zeta \in \mu_n} (x + \zeta) = \Phi_{2n}(x).$$

13.6.10 *Let ϕ denote the Frobenius map $\mathbb{F}_{p^n}$. Prove that ϕ gives an automorphism of order n*

Solution. We've already proved ϕ is an automorphism, since $\mathbb{F}_{p^n}$ is a finite field. Now, $\phi^n(a) = a^{p^n} = a$ since the multiplicative group $\mathbb{F}_{p^n}^\times$ has p^{n-1} elements. Therefore, the order of ϕ divides n. Conversely, if ϕ has order d then every element of $\mathbb{F}_{p^n}$ is a root of the polynomial $x^{p^d} - x$, and if $d < n$ this is more roots than the degree of the polynomial.

14.1.1 (a) *Show that if the field K is generated over F by the elements $a_1, ..., a_n$ then an automorphism a of K fixing F is uniquely determined by $\sigma(a_1), \ldots, \sigma(a_n)$. In particular, show that an automorphism fixes K if and only if it fixes a set of generators for K.*

Solution. Let σ, σ' be two elements of $\mathrm{Aut}(K/F)$ with the same images of $a_1, \ldots, a_n$. Let $E = \{b \in K | \sigma(b) = \sigma'(b)\} \subseteq K$. Then E contains F and $a_n, \ldots, a_n$. However, E must be a field since if $b, c \in E$, $\sigma(b+c) = \sigma(b) + \sigma(c) = \sigma'(b) + \sigma'(c) = \sigma'(b+c)$, and similarly for multipication. Therefore, $E = K$ since K is the smallest field containing $F, a_1, \ldots, a_n$.

The second statement follows from the first.

(b) *Let $G \leq Gal(K/F)$ be a subgroup of the Galois group of the extension K/F and suppose $\sigma_1, \ldots, \sigma_k$ are generators for G. Show that the subfield E of K containing F is fixed by G if and only if it is fixed by the generators $\sigma_1, \ldots, \sigma_k$.*

Solution. This is similar to the above. If E is not fixed by $\sigma_1, \ldots, \sigma_k$, it certainly isn't fixed by all of G. On the other hand, the subset of $\mathrm{Gal}(K/F)$ fixing E must be a subgroup (proof: if $\sigma(b) = b, \sigma'(b) = b$, then $\sigma\sigma'(b) = b$, and similarly for inverse), so if E is fixed by $\sigma_1, \ldots, \sigma_k$, it is fixed by G.

14.1.9 *Determine the fixed field of the automorphism $\phi : t \mapsto t + 1$ of $k(t)$*

Solution. One can show directly that this indeed determines a unique automorphism. Let $f(t) = p(t)/q(t)$, where $p, q \in k[t]$ are relatively prime, and p is monic. If $f(x) \in Fix(\phi)$, then $f(t+1) = f(t)$, so $p(t+1)/q(t+1) = p(t)/q(t)$, so $p(t+1)q(t) = p(t)q(t+1)$. If $p(t+1) \neq p(t)$, then they have no common (nonunit) factor since they are monic of the same degree. But then $p(t)$ is coprime with both factors, $p(t+1)$ and $q(t)$ on the right side, which is a contradiction.

Therefore, $p(t) = p(t+1)$, and by a similar argument $q(t) = q(t+1)$. Therefore, $\mathrm{Fix}(\phi)$ is the set of functions $f(t) = p(t)/q(t)$, where $p, q \in k[t]$ are relatively prime,

p is monic, and $p(t) = p(t+1), q(t) = q(t+1)$. We only need to determine which polynomials have this property.

For any root α of f we have $0 = f(\alpha) = f(\alpha+1) = f(\alpha+2) = \cdots$, so if char $k = 0$, f has no root in any field i.e. $f(t) \in k$. If char $k = p$, then let $\lambda(t) = t(t+1)\cdots(t+p-1) \in k[t]$. We have $\lambda(t) = \lambda(t+1)$, and any polynomial in $k[t]$ generated by λ and elements of k (e.g. $\lambda^2 + 2\lambda + 5$) also has this property. Conversely, let $f(t) = f(t+1)$, and let $f(0) = a$. Then $q(t) = f(t) - a$ has the same property, and $q(0) = 0$, so $q(1) = q(2) = \cdots = q(p-1) = 0$, and so $\lambda | q$. By induction, every polynomial fixed by ϕ is a multiple of λ plus a constant, and therefore the fixed field consists of rational functions where both numerator and denominator are generated by λ and k.

14.1.10 *Let K be an extension of the field F. Let $\phi : K \to K'$ be an isomorphism of K with a field K' which maps F to the subfield F' of K'. Prove that the map $\sigma \mapsto \phi\sigma\phi^{-1}$ defines a group isomorphism $Aut(K/F) \to Aut(K'/F)$.*

Solution. If $\sigma \in \mathrm{Aut}(K/F)$, then we first need to show that $\sigma' := \phi\sigma\phi^{-1}$ is indeed an element of $\mathrm{Aut}(K'/F')$. Since σ is the composition of three isomorphisms, it is itself an isomorphism, hence in $\mathrm{Aut}(K')$. Since σ fixes F, if $a \in F'$, then $\phi^{-1}(a) \in F$, so $\sigma'(a) = \phi(\sigma(\phi^{-1}(a))) = a$, and $\sigma' \in \mathrm{Aut}(K'/F')$.

Now, if $\sigma, \tau \in \mathrm{Aut}(K/F)$, then $\sigma\tau \mapsto \phi\sigma\tau\phi^{-1} = \phi\sigma\phi^{-1} \cdot \phi\tau\phi^{-1}$, so this map is a homomorphism. It is injective since if $\phi\sigma\phi^{-1} = \phi\tau\phi^{-1}$, $\sigma = \phi^{-1}\phi\sigma\phi^{-1}\phi = \phi^{-1}\phi\tau\phi^{-1}\phi = \tau$. Finally, for surjectivity, suppose that $\sigma' \in \mathrm{Aut}(K'/F')$. Then setting $\sigma := \phi^{-1}\sigma'\phi$, we have $\sigma \mapsto \phi\sigma\phi^{-1} = \phi\phi^{-1}\sigma'\phi\phi^{-1} = \sigma'$.