Math 5020 - Galois Representations
Suggested Exercises

P1 Let $L = \mathbb{Q}(\{\sqrt{-1}, \sqrt{p} : p \text{ prime}\})$. Then, $A = \mathrm{Aut}(L/\mathbb{Q}) = \prod_{k \geq 0}\{\pm 1\}$. Find a subgroup H of A of index 2 such that L^H, the subfield of L fixed by H, cannot correspond to a quadratic extension of $\mathbb{Q}$ via the Galois correspondence.

P2 Prove that $\mathrm{Hom}(\mathbb{F}_2^\infty, \mathbb{F}_2)$ is uncountably infinite.

P3 Let $F = \mathbb{Q}(\sqrt{2})$ and $K = \mathbb{Q}(\sqrt[4]{2})$. Show that $F/\mathbb{Q}$ and K/F are Galois, but $K/\mathbb{Q}$ is not Galois.

P4 Let $\mathbb{F}$ be a finite field of size $q = p^n$, where p is prime and $n \geq 1$, and let $\phi \colon \mathbb{F} \to \mathbb{F}$ such that $\phi(k) = k^p$ be the Frobenius map. Show that ϕ is an automorphism of $\mathbb{F}$.

P5 Show that $F = \mathbb{Q}(\sqrt{2+\sqrt{2}})$ is a Galois extension of $\mathbb{Q}$ and $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$.

P6 Show that $K = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ is Galois, with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

P7 Let $\pi \in \mathbb{C}$ be a transcendental number over $\mathbb{Q}$. Show that $\mathbb{Q}(\pi)/\mathbb{Q}$ contains infinitely many distinct intermediary subfields.

P8 Let p be a prime and let $K = \mathbb{F}_p(x, y)$ and $F = \mathbb{F}_p[x^p, y^p]$. Let $L_n = \mathbb{F}_p[x^p, y^p, x + x^{p^n}y]$.

(a) Show that $F \subsetneq L_n \subsetneq K$ and all L_n are distinct.
(b) Prove that K/F is finite of degree p^2.
(c) Conclude that K/F is a finite extension that contains infinitely many distinct intermediary subfields.

P9 (Dummit and Foote, Ch. 14.5, Problem 8)

P10 (Dummit and Foote, Ch. 14.7, Problem 19)

P11 Let $p > 2$ be a prime. Prove that the discriminant of the number field $\mathbb{Q}(\zeta_p)$ is $(-1)^{\frac{p-1}{2}} \cdot p^{p-2}$.

P12 Let $K/\mathbb{Q}$ be a finite extension of $\mathbb{Q}$.

(a) Prove that $K \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$ for all but finitely many prime numbers p.
(b) Suppose $K/\mathbb{Q}$ is Galois. Conclude that the cyclotomic character $\chi_p^K \colon \mathrm{Gal}(K/\mathbb{Q}) \to (\mathbb{Z}/p\mathbb{Z})^\times$ is trivial for all but finitely many prime numbers p.

P13 Let K be a Galois extension of $\mathbb{Q}$ such that $\mathbb{Q}(\zeta_n) \subset K$ for some $n \geq 3$, and let $F \subseteq K$ be a subfield. Show that the restriction of the cyclotomic character $\chi_n^{K/F} \colon \mathrm{Gal}(K/F) \to (\mathbb{Z}/n\mathbb{Z})^\times$ is surjective if and only if $\mathbb{Q}(\zeta_n) \cap F = \mathbb{Q}$.

P14 Let $\oplus$ be a binary operation defined on $\mathbb{Z}/p^n\mathbb{Z}$ by $k \oplus k' \equiv k + k' + kk'p \bmod p^n$, for a fixed $n \geq 2$.

(a) Prove that $(\mathbb{Z}/p^n\mathbb{Z}, \oplus)$ is an abelian group.
(b) Show that $(\mathbb{Z}/p^n\mathbb{Z}, \oplus)$ is isomorphic to $(\mathbb{Z}/p^n\mathbb{Z}, +)$ with its usual addition of congruences.
(c) Let U_n be the subset of $(\mathbb{Z}/p^n\mathbb{Z})^\times$ formed by units that are congruent to 1 mod p. Show that U_n is a subgroup and that $U_n \cong \mathbb{Z}/p^{n-1}\mathbb{Z}$, where $\mathbb{Z}/p^{n-1}\mathbb{Z}$ comes equipped with $\oplus$.

P15 Let p be an odd prime and let K_p be the unique subfield of $\mathbb{Q}(\zeta_{p^2})$ such that $[K_p : \mathbb{Q}] = p$. For $p = 3$, 5, and 7, find a polynomial $f_p(x)$ such that K_p is the splitting field of $f_p(x)$. (You are welcome to use Magma to find these.)

P16 Let p be a prime. Let $G = \mathrm{GL}(2, \mathbb{Z}_p)$ and $G_n = \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$.

(a) Let $\pi_n \colon \mathrm{GL}(2, \mathbb{Z}_p) \to \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ be the reduction mod-p^n map. Let H_n be a subgroup of $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$. Show that $\pi_n^{-1}(H_n)$ is an open subgroup of $\mathrm{GL}(2, \mathbb{Z}_p)$ of finite index.

(b) Let H be a subgroup of $\mathrm{GL}(2, \mathbb{Z}_p)$ of finite index, and let $H_n = \pi_n(H)$ for every $n \geq 1$. Show that the natural map $G/H \to G_n/H_n$ is surjective. Conclude that $[G : H] \geq [G_n : H_n]$.

(c) With notation as in (b), show that there is some number $N \geq 1$ such that $[G : H] = [G_n : H_n]$ for all $n \geq N$.

(d) With notation as in (b) and (c), show that $H = \pi_n^{-1}(H_N)$.