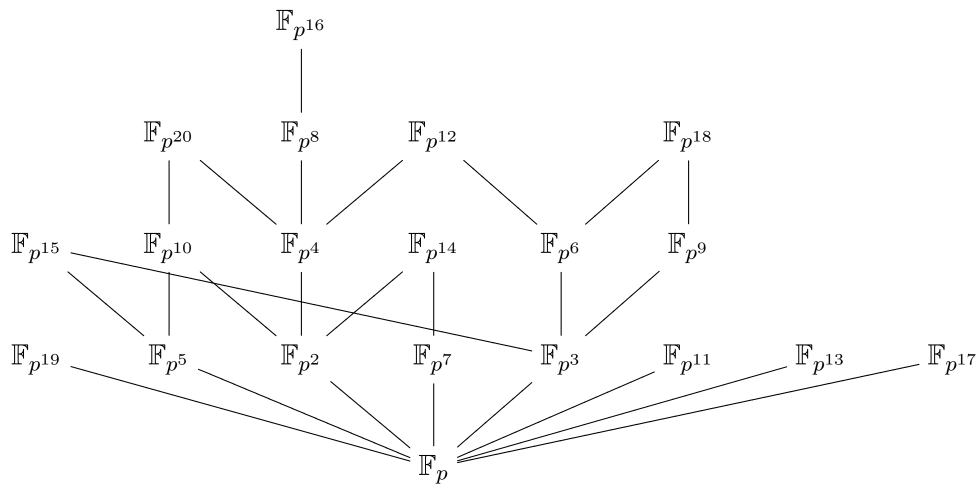
Math 306, Spring 2012
Homework 10 Solutions

(1) (5 pts) Let p be prime. Construct a tree contaning all the fields $\mathbb{F}_{p^n}$ for $n \in \{1, 2, \ldots, 20\}$ and depicting the subfield structure.

Solution:



(2) (5 pts) For any prime p, prove that there is an irreducible polynomial $f \in \mathbb{Z}_p[x]$ whose Galois group is $\mathbb{Z}_p$.

Solution: Let p be a prime. Consider the polynomial $f = x^p - x + 1$ in $\mathbb{Z}_p[x]$. We know that f is irreducible and, if α is a root of f, then $\mathbb{Z}_p(\alpha)$ is a splitting field of f. The index $[\mathbb{Z}_p(\alpha)\colon \mathbb{Z}_p] = p$. Since f is separable, the extension is Galois, so the fundamental theorem gives $\mathsf{Gal}(\mathbb{Z}_p(\alpha)/\mathbb{Z}_p) \cong \mathbb{Z}_p$.

(3) (5 pts) Suppose that $f \in \mathbb{Z}[x]$ is an irreducible quartic whose splitting field L has Galois group S_4. Let θ be a root of f and let $M = \mathbb{Q}(\theta)$. Prove that $M\colon \mathbb{Q}$ has degree 4 with no proper subfields. (Hint: Your proof should be by contradiction. You will want to identify the sole subgroup of S_4 with 12 elements, and the 4 subgroups of S_4 with 6 elements.)

Solution: The only subgroup of order 12 is A_4 and the 4 subgroups of order 6 are the ones isomorphic to S_3. Since θ is a root of an irreducible quartic, then clearly $\mathbb{Q}(\theta)\colon \mathbb{Q}$ has degree 4, so $[M\colon \mathbb{Q}] = 4$. Now suppose that there is an intermediate subfield N of $M\colon \mathbb{Q}$. Then we have a tower of fields $\mathbb{Q} \subseteq N \subseteq M \subseteq L$. Since $L\colon \mathbb{Q}$ is Galois, we can take apply the map $*$ to this sequence to give $S_4 \geq N^* \geq M^* \geq \langle e \rangle$. By the Fundamental Theorem, we must have $[S_4\colon N^*] = [N\colon \mathbb{Q}] = 2$, so $N = A_4$. Also $[M^*\colon N^*] = [N\colon M] = 2$, so $|M^*| = 6$, i.e. $M^* \cong S_3$. Since $M^* \leq N^*$, we have a copy of S_3 sitting inside A_4, which is a contradiction, since S_3 has elements of odd order and A_4 does not.

(4) (5 pts/part) Let $L\colon K$ be a Galois extension with Galois group G and let $\alpha \in L$. Define the norm and trace of α respectively as

$$\mathsf{N}_{L/K}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) \quad \text{and} \quad \mathsf{Tr}_{L/K}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha).$$

(a) By showing that $\mathsf{N}_{L/K}(\alpha)$ and $\mathsf{Tr}_{L/K}(\alpha)$ are fixed by G, prove that the norm and trace of α are both in K.

(b) Prove that, for all $\alpha, \beta \in L$, we have

$$\mathsf{N}_{L/K}(\alpha\beta) = \mathsf{N}_{L/K}(\alpha)\mathsf{N}_{L/K}(\beta) \quad \text{and} \quad \mathsf{Tr}_{L/K}(\alpha + \beta) = \mathsf{Tr}_{L/K}(\alpha) + \mathsf{Tr}_{L/K}(\beta).$$

(c) Let $L = K(\sqrt{D})$ be a quadratic extension of K. Prove that $\mathsf{N}_{L/K}(a + b\sqrt{D}) = a^2 - Db^2$ and $\mathsf{Tr}_{L/K}(a + b\sqrt{D}) = 2a$.

Solution:

(a) Let $\alpha \in L$ and let $\tau \in G$. Then

$$\tau(\mathsf{N}_{L/K}(\alpha)) = \tau\left(\prod_{\sigma\in G}\sigma(\alpha)\right) = \prod_{\sigma\in G}\tau\sigma(\alpha) = \prod_{\rho\in G}\rho(\alpha) = \mathsf{N}_{L/K}(\alpha).$$

We also have

$$\tau(\mathsf{Tr}_{L/K}(\alpha)) = \tau\left(\sum_{\sigma\in G}\sigma(\alpha)\right) = \sum_{\sigma\in G}\tau\sigma(\alpha) = \sum_{\rho\in G}\rho(\alpha) = \mathsf{Tr}_{L/K}(\alpha).$$

Since τ is arbitrary, both the norm and the trace of α belong to the fixed field of G, so the norm and the trace of α lie in K.

(b) Let $\alpha, \beta \in L$. Then clearly

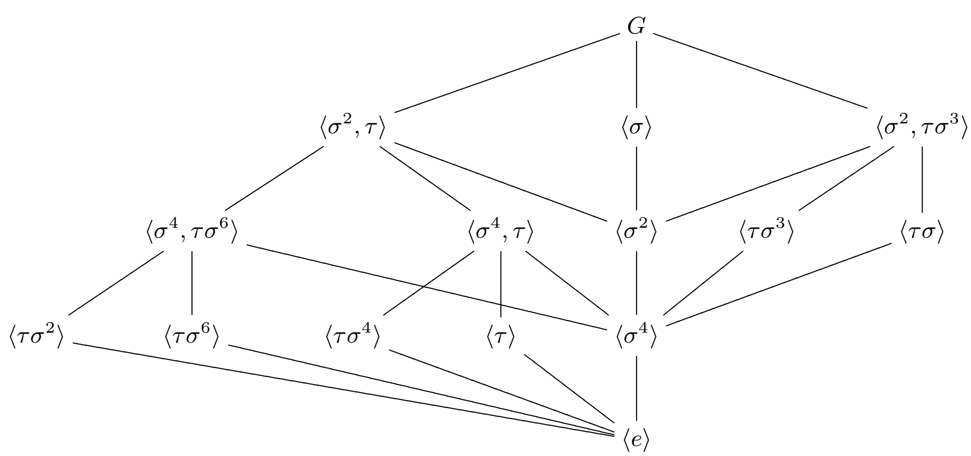
$$\mathsf{N}_{L/K}(\alpha\beta) = \prod_{\sigma\in G}\sigma(\alpha\beta) = \prod_{\sigma\in G}\sigma(\alpha)\sigma(\beta) = \prod_{\sigma\in G}\sigma(\alpha)\prod_{\sigma\in G}\sigma(\beta) = \mathsf{N}_{L/K}(\alpha)\mathsf{N}_{L/K}(\beta).$$

We also have

$$\mathsf{Tr}_{L/K}(\alpha+\beta) = \sum_{\sigma\in G}\sigma(\alpha+\beta) = \sum_{\sigma\in G}\sigma(\alpha)+\sigma(\beta) = \sum_{\sigma\in G}\sigma(\alpha)+\sum_{\sigma\in G}\sigma(\beta) = \mathsf{Tr}_{L/K}(\alpha)+\mathsf{Tr}_{L/K}(\beta).$$

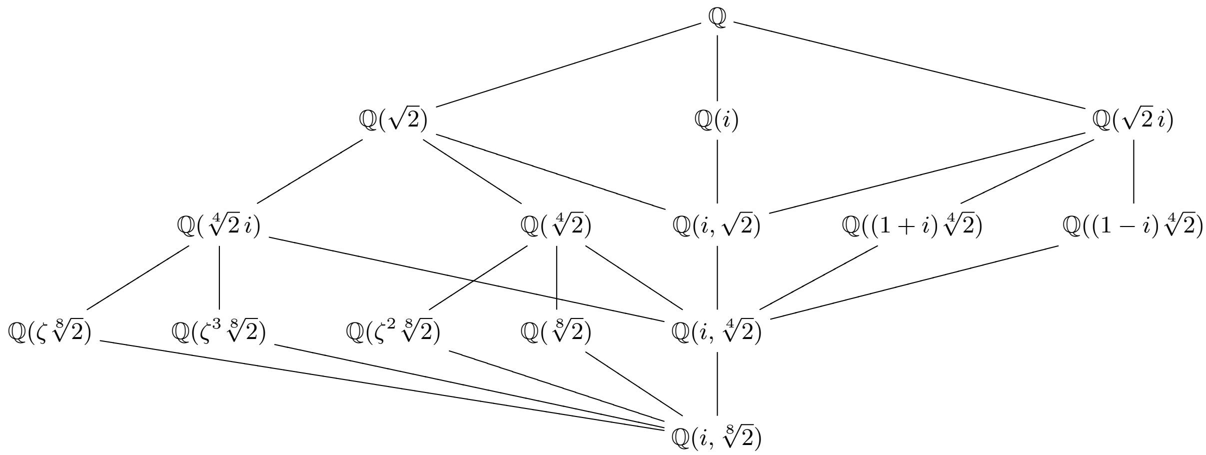
(c) If $K(\sqrt{D})$ is a quadratic extension of K, then there are two automorphisms in the Galois group determined by $\sqrt{D} \mapsto \sqrt{D}$ and $\sqrt{D} \mapsto -\sqrt{D}$. Hence $\mathsf{Tr}_{L/K}(a + b\sqrt{D}) = (a + b\sqrt{D}) + (a - b\sqrt{D}) = 2a$ and $\mathsf{N}_{L/K}(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2$.

(5) (5 pts) The splitting field of $x^8 - 2$ over $\mathbb{Q}$ is given by $\mathbb{Q}(\sqrt[8]{2}, i)$ which is an extension of degree 16 over $\mathbb{Q}$. If $\zeta = e^{2\pi i/8}$, then every $\mathbb{Q}$-automorphism of $\mathbb{Q}(\sqrt[8]{2}, i)$ is determined by $\sqrt[8]{2} \mapsto \zeta^k\sqrt[8]{2}$ and $i \mapsto \pm i$, where $k \in \{0, 1, \ldots, 7\}$. Let σ be determined by $\sqrt[8]{2} \mapsto \zeta\sqrt[8]{2}$ and $i \mapsto i$ and let τ be determined by $\sqrt[8]{2} \mapsto \sqrt[8]{2}$ and $i \mapsto -i$. The 16-element Galois group G is given by $\langle\sigma, \tau\rangle$, where $\sigma^8 = \tau^2 = e$ and $\sigma\tau = \tau\sigma^3$. Below is a subgroup lattice for G.



The subfields are given by $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i\sqrt[4]{2})$, $\mathbb{Q}(\sqrt{2}\,i)$, $\mathbb{Q}(i)$, $\mathbb{Q}$, $\mathbb{Q}((1+i)\sqrt[4]{2})$, $\mathbb{Q}(i, \sqrt[8]{2})$, $\mathbb{Q}(\zeta^2\sqrt[8]{2})$, $\mathbb{Q}(\zeta^3\sqrt[8]{2})$, $\mathbb{Q}((1-i)\sqrt[4]{2})$, $\mathbb{Q}(i, \sqrt{2})$, $\mathbb{Q}(i, \sqrt[4]{2})$, $\mathbb{Q}(\zeta\sqrt[8]{2})$, $\mathbb{Q}(\sqrt[4]{2})$, $\mathbb{Q}(\sqrt[8]{2})$. Construct the subfield lattice. No explanation required.

Solution:



$\mathbb{Q}$
$\mathbb{Q}(\sqrt{2})$
$\mathbb{Q}(i)$
$\mathbb{Q}(\sqrt{2}\,i)$
$\mathbb{Q}(\sqrt[4]{2}\,i)$
$\mathbb{Q}(\sqrt[4]{2})$
$\mathbb{Q}(i, \sqrt{2})$
$\mathbb{Q}((1+i)\sqrt[4]{2})$
$\mathbb{Q}((1-i)\sqrt[4]{2})$
$\mathbb{Q}(\zeta\sqrt[8]{2})$
$\mathbb{Q}(\zeta^3\sqrt[8]{2})$
$\mathbb{Q}(\zeta^2\sqrt[8]{2})$
$\mathbb{Q}(\sqrt[8]{2})$
$\mathbb{Q}(i, \sqrt[4]{2})$
$\mathbb{Q}(i, \sqrt[8]{2})$