Lior Silberman's Math 501: Problem Set 8 (due 13/11/2020)

(From PS7) Example: Cyclotomic fields

PRAC For practice (but not for submission)

(a) Show that $x^n - 1 \in \mathbb{Q}[x]$ has n distinct roots.

(b) Write μ_n for the set of roots of this polynomial. Show that it forms a cyclic group of order n.

DEF μ_n is called the *group of roots of unity of order [dividing] n*. A root of unity $\zeta \in \mu_n$ is called *primitive* if it is a generator, that is if it has order exactly n. We write ζ_n for a primitive root of unity of order n, for example $e^{\frac{2\pi i}{n}} \in \mathbb{C}$ (by problem 6(a) the choice doesn't matter). For the purpose of the problem set we also write $P_n \subset \mu_n$ for the set of primitive roots of unity of order n. The polynomial $\Phi_n(x) = \prod_{\zeta \in P_n}(x - \zeta)$ is called the nth *cyclotomic polynomial*. The field $\mathbb{Q}(\zeta_n)$ is called the nth *cyclotomic field*.

(c) Show that $\prod_{d|n} \Phi_d(x) = x^n - 1$. We'll later show that this is the factorization of $x^n - 1$ into irreducibles in $\mathbb{Q}[x]$.

1. Let ζ_n be a primitive nth root of unity.
   (a) Show that $\mathbb{Q}(\zeta_n)$ is the splitting field of $x^n - 1$ over $\mathbb{Q}$.
   (b) Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$. For $\sigma \in G$ show there is a unique $j \in (\mathbb{Z}/n\mathbb{Z})^\times$ so that $\sigma(\zeta_n) = \zeta_n^{j(\sigma)}$ and that $j \colon G \to (\mathbb{Z}/n\mathbb{Z})^\times$ is an injective homomorphism (we'll later show that this map is an isomorphism).
   (c) Show that $\Phi_n(x) \in \mathbb{Q}[x]$ and that the degree of Φ_n is exactly $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$.

2. (prime power and prime order) Fix an odd prime p and let $r \geq 1$.
   (a) Show that $\Phi_{p^r}(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1}$ and that this polynomial is irreducible.
   (b) Show that $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}) \simeq (\mathbb{Z}/p^r\mathbb{Z})^\times$.
   RMK Parts (a),(b) hold for $p = 2$ as well.
   (c) Show that $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q})$ is cyclic.
   (d) Show that $\mathbb{Q}(\zeta_p)$ has a unique subfield K so that $[K : \mathbb{Q}] = 2$.
   (e) Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p) : \mathbb{Q})$. Show that there is a unique non-trivial homomorphism $\chi \colon G \to \{\pm 1\}$.
   (f) Let $g = \sum_{\sigma \in G} \chi(\sigma)\sigma(\zeta_p)$ (the "Gauss sum"). Show that $g \in K$, $g \notin \mathbb{Q}$, but $g^2 \in \mathbb{Q}$.
   (*g) Show that $g^2 = (-1)^{\frac{p-1}{2}} p$, giving a different proof that $K = \mathbb{Q}(g)$.

Examples

3. (Quadratic extension) Let $L = K(\sqrt{d})$ be a quadratic extension of characteristic not equal to 2.
   (a) Write down the matrix of multiplication by $\alpha = a + b\sqrt{d} \in L$ in the basis $\left\{1, \sqrt{d}\right\}$.
   (b) Find the trace and determinant of this matrix.
   (c) Let σ be the non-trivial element of $\mathrm{Gal}(L/K)$. Show that the answers to (b) agree with $\alpha + \sigma(\alpha)$, $\alpha\sigma(\alpha)$ respectively.
   RMK Meditate on the case $L = \mathbb{C}$, $K = \mathbb{R}$.

4. (Cyclotomic extension) Let ζ_p be a primitive root of unity of order p and equip $\mathbb{Q}(\zeta)$ with the basis $\left\{1, \zeta_p, \ldots, \zeta_p^{p-2}\right\}$. Let G be the cyclic group $\mathrm{Gal}(\mathbb{Q}(\zeta_p) : \mathbb{Q})$.
   (a) Write down the matrix of multiplication by ζ_p in this basis.
   (b) Find the trace and determinant of this matrix.
   (*c) Find its characteristic polynomial.
   (*d) Explicitly compute $\sum_{\sigma \in G} \sigma(\zeta_p)$ and $\prod_{\sigma \in G} \sigma(\zeta_p)$ and show that they equal your answers from parts (b),(d).

The trace

When L/K is a finite Galois extension and $\alpha \in L$ we encounter in class the combination ("trace") $\mathrm{Tr}_K^L(\alpha) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma\alpha$, which we need to be non-zero. We will study this construction when L/K is a finite separable extension, fixed for the purpose of the problems 5-7.

5. Let N/K be a finite normal extension containing L.
   (a) For $\alpha \in L$ we provisionally set
   $$\mathrm{Tr}_K^L(\alpha) = \sum_{\mu \in \mathrm{Hom}_K(L,N)} \mu\alpha \qquad \text{"trace of } \alpha\text{"}$$
   $$N_K^L(\alpha) = \prod_{\mu \in \mathrm{Hom}_K(L,N)} \mu\alpha \qquad \text{"norm of } \alpha\text{"}$$
   Where the sum and product range over all K-embeddings of L in N. Show that the definition is independent of the choice of N.
   (b) Making a judicious choice of N show that the trace and norm defined in part (a) are elements of K.
   (c) Show that when L/K is a Galois extension the definition from part (a) reduces to the combination used in class.

6. (Elements of zero trace) In the application in class we are interested in $L_0 = \{\alpha \in L \mid \mathrm{Tr}_K^L(\alpha) = 0\}$.
   (a) Show that $\mathrm{Tr}_K^L \colon L \to K$ is a K-linear functional on L, so that L_0 is a K-subspace of L.
   (b) When $\mathrm{char}(K) = 0$, show that $L = K \oplus L_0$ as vector spaces over K (direct sum of vector spaces; the analogue of direct product of groups). Conclude that when $[L : K] \geq 2$ the set $L_0 \setminus K$ is non-empty. (e..g the normal closure).
   (c) Show that Tr_K^L is a non-zero linear functional in all characteristics.
   (d) Show that L_0 is not contained in K unless $[L : K] = \mathrm{char}(K) = 2$, in which case $L_0 = K$, or $[L : K] = 1$ in which case $L_0 = \{0\}$.

7. (Yet another definition) We continue with the separable extension L/K of degree n.
   (a) Let $f \in K[x]$ be the (monic) minimal polynomial of $\alpha \in L$, say that $f = \sum_{i=0}^{d} a_i x^i$ with $a_d = 1$. Show that $\mathrm{Tr}_K^{K(\alpha)}(\alpha) = -a_{d-1}$ and that $N_K^{K(\alpha)}(\alpha) = (-1)^d a_0$.
   (b) Show that $\mathrm{Tr}_K^L(\alpha) = -\frac{n}{d} a_{d-1}$ and that $N_K^L(\alpha) = (-1)^n a_0^{n/d}$.
   Hint: Recall the proof that $[L : K]$ has n embeddings into a normal closure.
   (c) Show that $\mathrm{Tr}_K^L(\alpha)$ and $N_K^L(\alpha)$ are, respectively, the trace and determinant of multiplication by α, thought of as a K-linear map $L \to L$.
   Hint: Show that we have $L \simeq (K(\alpha))^{n/d}$ as $K(\alpha)$-vector spaces,.

Definition. From now on we define the trace and norm of α as in 7(c). Note that this definition makes sense even if L/K is not separable.

8. (Transitivity) Let $K \subset L \subset M$ be a tower of finite extensions. Show that
   (a) $\mathrm{Tr}_K^M = \mathrm{Tr}_K^L \circ \mathrm{Tr}_L^M$.
   (b) $N_K^M = N_K^L \circ N_L^M$.

Supplementary problems

A. (Purely inseparable extension) Let L/K be an purely inseparable algebraic extension of fields of characteristic p.

(a) For every $\alpha \in L$ show that there exists $r \geq 0$ so that $\alpha^{p^r} \in K$. In fact, show that the minimal polynomial of α is of the form $x^{p^r} - \alpha^{p^r}$.

Hint: Consider the minimal polynomials of α and α^p

(b) Conclude that when $[L : K]$ is finite it is a power of p.

(c) When $[L : K]$ is finite show that Tr^L_K is identically zero.

B. Let $L = \mathbb{C}(x)$ (the field of rational functions in variable) and for $f \in L$ let $(\sigma(f))(x) = f(\frac{1}{x})$, $(\tau(f))(x) = f(1-x)$.

(a) Show that $\sigma, \tau \in \mathrm{Aut}(L)$ and that $\sigma^2 = \tau^2 = 1$.

(b) Show that $G = \langle \sigma, \tau \rangle$ is a subgroup of order 6 of $\mathrm{Aut}(L)$ and find its isomorphism class.

(c) Let $K = \mathrm{Fix}(G)$. Find this field explin elements $\alpha \in L$ with trace zero. For this, leticitly.