HOMEWORK 3

This homework does not need to be submitted.

1. In this exercise we prove that any finite abelian group can be realized as a Galois group over $\mathbb{Q}$.

(a) First prove the following special case of Dirichlet's Prime Number Theorem: For any integer $n \geq 2$ there are infinitely many primes p with $p \equiv 1 \pmod{n}$. (Hint: Assume there are only finitely many such p, and let m be their product. Let Φ_n be the nth cyclotomic polynomial. Explain why there must be some $x \in \mathbb{Z}$ and prime p such that $p | \Phi_n(xnm)$ and derive a contradiction.)

(b) Prove that for any finite abelian group A there is a Galois extension $F/\mathbb{Q}$ with $\mathrm{Gal}(F/\mathbb{Q}) \cong A$.

2. Let $F/\mathbb{Q}$ be quadratic and let d_F be the discriminant of F. Prove that $F \subseteq \mathbb{Q}(\zeta)$ with ζ a primitive d_F-th root of unity, and that this is the smallest cyclotomic field containing F.

3. Let ζ be a primitive nth root of 1. Prove that $\mathbb{Z}[\zeta + \zeta^{-1}]$ is the ring of integers of $\mathbb{Q}(\zeta + \zeta^{-1})$.

4. Let ζ be a primitive nth root of 1 and let $\mathbb{Q}(\zeta)^+ = \mathbb{Q}(\zeta + \zeta^{-1})$ be the maximal totally real subfield of $\mathbb{Q}(\zeta)$.

(a) Prove that if $n = p^r$ with p a prime, then there is a unique prime ideal P of $\mathbb{Q}(\zeta)^+$ above p, it ramified in $\mathbb{Q}(\zeta)$, and $\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta)^+$ is unramified at all other prime ideals of $\mathbb{Q}(\zeta)^+$. (This follows very quickly from what we did in class, but I wanted to include this to contrast it with the next part.)

(b) Prove that if n is not a prime power, then all prime ideals of $\mathbb{Q}(\zeta)^+$ are unramified in $\mathbb{Q}(\zeta)$. (You may use without proof the following fact: if F is a number field, K/F and L/F are two finite extension, and P is a prime ideal of $\mathcal{O}_F$ that is unramified in K, then any prime in L above P is unramified in the compositum KL.)

5. Recall from earlier homework that if F is a CM field with maximal totally real subfield F^+, and $\mu(F)$ is the group of roots of unity in F, then $\mu(F)\mathcal{O}_{F^+}^\times$ has index at most 2 in $\mathcal{O}_F^\times$. This was proved by showing that the map $\psi : \mathcal{O}_F^\times \to \mu(F)$ given by $\psi(\varepsilon) = \varepsilon/c(\varepsilon)$, with c the nontrivial element of $\mathrm{Gal}(F/F^+)$, induces an injection $\mathcal{O}_F^\times/\mu(F)\mathcal{O}_{F^+}^\times \hookrightarrow \mu(F)/\mu(F)^2$.

We now consider the case where F is a cyclotomic field, and let $F = \mathbb{Q}(\zeta)$ with ζ a primitive nth root of 1 with n either odd or divisible by 4.

(a) Prove that if n is a prime power, then $\mu(F)\mathcal{O}_{F^+}^\times = \mathcal{O}_F^\times$.
(Hint: You need to show that $\varepsilon/c(\varepsilon) \in \mu(F)^2$ for any unit ε.

- When the prime is odd, explain why this is equivalent to $\varepsilon/c(\varepsilon) \neq -\zeta^j$ for any j. Then show that this can't happen by considering congruences modulo the prime $(1-\zeta)$.
- When the prime is 2, explain why this is equivalent to $\varepsilon/c(\varepsilon)$ not being a primitive nth root of unity. Then show that this can't happen by considering norms from $\mathbb{Q}(\zeta)$ to $\mathbb{Q}(i)$.)

(b) Prove that if n is not a prime power, then $\mu(F)\mathcal{O}_{F^+}^\times \neq \mathcal{O}_F^\times$. (Hint: Under the assumption that n is not a prime power, you proved on a previous homework that $1-\zeta$ is a unit $\mathbb{Z}[\zeta]$. Consider ψ applied to this unit.)

6. Let D be a unique factorization domain with fraction field F and let $f \in D$ be irreducible. Prove that there is a unique additive valuation $v : F \to \mathbb{R} \cup \{\infty\}$ such that $v(f) = 1$ and $v(g) = 0$ for any irreducible $g \in D$ not associate to f.

7. Let k be a field and let $k(T)$ be the fraction field of the polynomial ring $k[T]$
(a) Since $k(T)$ is the fraction field of the polynomial ring $k[T^{-1}]$, we have the T^{-1}-adic additive valuation on $k(T)$ (it is the unique additive valuation on $k(T)$ satisfying $v(T^{-1}) = 1$). Describe its restriction to $k[T]$.
(b) Show that any nontrivial additive valuation on $k(T)$ that is trivial on k is equivalent to either the T^{-1}-adic valuation from part (a) or the f-adic valuation for some irreducible $f \in k[T]$.

Remark. Part (b) shows that equivalence classes of nontrivial additive valuations (or nontrivial nonarchimedean absolute values) that are trivial on k are in bijection with the points of one-dimensional projective space $\mathbb{P}^1_k$ defined over k. This fact remains true for any smooth projective curve C over k, replacing $k(T)$ with the function field $k(C)$ of C.

8. Let F be a field equipped with a nontrivial nonarchimedean absolute value $|\cdot|$ and let $\mathcal{O}$ be the corresponding valuation ring.
(a) For any real $r > 0$, let $B_r = \{x \in F \mid |x| < r\}$ and $C_r = \{x \in F \mid |x| \leq r\}$. Prove that B_r and C_r are $\mathcal{O}$-submodules of F.
(b) For any real $0 < r < 1$, let $U_r = \{x \in F \mid |x-1| < r\}$ and $V_r = \{x \in F \mid |x-1| \leq r\}$. Show that U_r and V_r are subgroups of $\mathcal{O}^\times$.

9. Let F be a field equipped with a nontrivial nonarchimedean absolute value $|\cdot|$ and let $\mathcal{O}$ be the valuation ring.
(a) Prove that the ideals of $\mathcal{O}$ are totally ordered by inclusion.
(b) Prove that any finitely generated ideal of $\mathcal{O}$ is principal.
(c) Prove that if $|\cdot|$ is not discrete, then $\mathcal{O}$ is not Noetherian.

10. Let k be a finite field of cardinality q. Note that any absolute value on k is necessarily trivial (any nonzero element is a root of 1). So by Question 7 above, any nontrivial additive valuation v on $k(T)$ is equivalent to precisely one of:
(i) the f-adic valuation v_f associated to some monic irreducible $f \in k[T]$,
(ii) the T^{-1}-adic valuation $v_{T^{-1}}$.
Define absolute values $|\cdot|_v$ by
(i) $|\cdot|_v = (q^{\deg(f)})^{-v(\cdot)}$ if $v = v_f$ for $f \in k[T]$ monic and irreducible,
(ii) $|\cdot|_v = q^{-v(\cdot)}$ if $v = v_{T^{-1}}$.
Prove the product formula:

$$\prod_v |x|_v = 1 \quad \text{for any} \quad x \in k(T)^\times.$$

Remark. The set of valuations v above are in bijection with the points of projective space $\mathbb{P}^1$ defined over k. The T^{-1}-adic valuation can be thought of as corresponding to the "point at infinity:" $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$. So considering all the valuations defined using irreducibles in $k[T]$, we are missing one "coming from infinity," and upon including this one, we have the product formula.

Compare this with $\mathbb{Q}$: we have a collection of absolute values $|\cdot|_p$ associated to each (associate class of) irreducibles p in $\mathbb{Z}$, and upon adding the one missing (i.e. the archimedean one), we have the product formula. This analogy partially motivates the the reason the archimedean absolute value on $\mathbb{Q}$ is denoted by $|\cdot|_\infty$.

11. Let F be a field equipped with a nonarchimedean absolute value $|\cdot|$ and its induced topology.
(a) Prove that any open ball is a closed set (so this topology has a basis of clopen sets).
(b) Prove that F is totally disconnected (i.e. any nonempty open set can be written as the disjoint union of two nonempty open sets).

12. Let $|\cdot|$ be an absolute value on a field F and give F the topology induced by $|\cdot|$. Prove that if F is locally compact, then F is complete. (This holds more generally for any metric group.)

13. Let F be a field complete with respect to a discrete nonarchimedean absolute value. Let $\mathcal{O}$ be its valuation ring and let k be its residue field. Prove that $F \cong k(\!(T)\!)$ if and only if $\mathcal{O}$ contains a field k' that maps isomorphically onto k via the quotient map $\mathcal{O} \to k$.

Remark. It can be shown that such a k' always exists when $\mathrm{char}(F) = \mathrm{char}(k)$ (which is clearly a necessary condition).

14. Let F be a field complete with respect to a nontrivial nonarchimedean absolute value $|\cdot|$. Let $\mathcal{O}$ be the valuation ring of F and let k be the residue field. Prove that the following are equivalent.
(a) F is locally compact.
(b) $\mathcal{O}$ is compact.
(c) $|\cdot|$ is discrete and k is finite.

15. (a) Let p be an odd prime. Prove that $x \in \mathbb{Q}_p^\times$ is a $(p-1)m$-th power in $\mathbb{Q}_p$ for all integers $m \geq 1$ coprime with p if and only if $x \in 1 + p\mathbb{Z}_p$.
(b) Prove that $x \in \mathbb{Q}_2^\times$ is a $2m$-th power in $\mathbb{Q}_p$ for all odd integers $m \geq 1$ if and only if $x \in 1 + 8\mathbb{Z}_p$.
(c) Use (a) and (b) to prove that for any prime p, the only field automorphism of $\mathbb{Q}_p$ is the identity.

Remark. Note that this is also true of $\mathbb{R}$. In both cases, the algebraic structure of the field determines its topology, so field automorphism are forced to be continuous. This continuity and the density of $\mathbb{Q}$ then forces the automorphism to be the identity.

16. Give an example of a field F that is complete with respect to a nontrivial nonarchimedean absolute value $|\cdot|$ with algebraically closed residue field but such that F is not algebraically closed. Explain why this does not violate Hensel's Lemma. What does this say about irreducible polynomials in $F[X]$?

17. Prove that $(X^2-2)(X^2-17)(X^2-34)$ has a root in $\mathbb{Q}_p$ for every prime p. (Note that it also has a root in $\mathbb{R}$. So this polynomial has a root in all completions of $\mathbb{Q}$, but not in $\mathbb{Q}$ itself.)

18. (a) Let F be a field complete with respect to a discrete nonarchimedean absolute value. Prove that an algebraic closure of F has infinite degree over F.
(b) Let $\overline{\mathbb{Q}}_p$ be an algebraic closure of $\mathbb{Q}_p$. Construct a Cauchy sequence in $\overline{\mathbb{Q}}_p$ that does not converge in $\overline{\mathbb{Q}}_p$.

19. Let F be an algebraically closed field equipped with a nontrivial nonarchimedean absolute value $|\cdot|$. Define $\|\cdot\|$ on $F[X]$ by

$$\|a_0 + \cdots + a_n X^n\| = \max\{|a_0|, \ldots, |a_n|\}.$$

It can be shown that $\|\cdot\|$ extends to a nonarchimedean aboslute value on $F(X)$.

Let $f, g \in F[X]$ be monic of the same degree n, and let $\alpha \in F$ be a root of f.

(a) Show that $|\alpha| \leq \|f\|$.

(b) Show that $|g(\alpha)| \leq \|f - g\|\|f\|^{n-1}$.

(c) Show that there is a root $\beta \in F$ of g such that

$$|\alpha - \beta| \leq \|f - g\|^{1/n}\|f\|.$$

(This property is known as *continuity of roots*.)

20. Let F be an algebraically closed field equipped with a nontrivial nonarchimedean absolute value $|\cdot|$. Prove that the completion of F is algebraically closed.

Remark. Let $\overline{\mathbb{Q}}_p$ be an algebraic closure of $\mathbb{Q}_p$. We know that $|\cdot|_p$ extends uniquely to $\overline{\mathbb{Q}}_p$. By Question 18.(b), $\overline{\mathbb{Q}}_p$ is not complete. But by Question 20, its completion is algebraically closed. This is (up to isomorphism) the smallest algebraically closed complete field extension of $\mathbb{Q}_p$. For this reason it is often denoted $\mathbb{C}_p$ and thought of as the "p-adic complex numbers."