Homework 3.5: Additional problems to homework 3
due on Thursday, March 28

Read Chapter 5 of Miln's book. Solve the following problems.

Problem 1. Recall that if A, C are abelian groups then the set $\mathrm{Hom}(A, C)$ of all group homomorphisms from A to C is also an abelian group (with $(f+g)(a) = f(a) + g(a)$).

a) Show that $\mathrm{Hom}(A \times B, C)$ is naturally isomorphic to $\mathrm{Hom}(A, C) \times \mathrm{Hom}(B, C)$.

b) Suppose that A is a cyclic group of order which divides n and C is a cyclic group of order n. Prove that the groups $\mathrm{Hom}(A, C)$ and A are isomorphic.

c) Use the structure theorem for finite abelian groups to show that if A is abelian of exponent dividing n and C is cyclic of order n then the groups $\mathrm{Hom}(A, C)$ and A are isomorphic.

d) Let A, B, C be abelian groups. A map $F : A \times B \longrightarrow C$ is called **bilinear** if for any $a \in A$ the map $F(a, -) : b \mapsto F(a, b)$ is a homomorphism from B to C and for any $b \in B$ the map $F(-, b) : a \mapsto F(a, b)$ is a homomorphism from A to C. Show that if F is bilinear then the assignment $a \mapsto F(a, -)$ defines a homomorphism from A to $\mathrm{Hom}(B, C)$ and the assignment $b \mapsto F(-, b)$ defines a homomorphism from B to $\mathrm{Hom}(A, C)$. We say that F is **non-degenerate** if these two homomorphisms are injective.

d) Let C be a cyclic group of order n. Suppose that A, B are finite abelian groups and $F : A \times B \longrightarrow C$ is a non-degenrate bilinear map (we ofetn say that F is a non-degenerate pairing in this situation). Prove that the groups A and $\mathrm{Hom}(B, C)$ are isomorphic. Conclude that A and B are isomorphic and of exponent which divides n.

Problem 2. This problem extends some results proved in class. First let us recall what we proved in class. Let K be a field and n a positive integer not divisible by the characteristic of K. We assume that K contains the group μ_n of n-th roots of 1.

For $0 \neq a \in K$ consider the splitting field L of the polynomial $x^n - a$ over K. Since the polynomial $x^n - a$ is separable over K, L/K is a finite Galois extension. Choose a root u of $x^n - a$ in L. Any such root is an n-th root of a. The roots of $x^n - a$ in L are exactly the elements $u\xi$, with $\xi \in \mu_n$.

We proved the following.

1. $L = K[u]$.
2. The map $\mathrm{Gal}(L/K) \longrightarrow \mu_n$ which sends each automorphisms σ to $\sigma(u)/u$ does not depend on which root u we choose and it is an injective group homomorphism.
3. $\mathrm{Gal}(L/K)$ is cyclic of order d for some $d|n$. Let σ be a generator of $\mathrm{Gal}(L/K)$. Then $\sigma(u) = \zeta u$ for some primitive d-th root of 1 ζ.
4. $u^d = b \in K$ and u is a root of $x^d - b$. Also, $b^{n/d} = a$.
5. d is the smallest positive integer such that a^d is an n-th power in K.
6. $x^n - c$ splits in L (i.e. L contains n-th roots of c) if and only if c/a^i is an n-th power in K for some $i > 0$.

By $(K^\times)^n$ we mean the set of all n-th powers in $K^\times$. This is a subgroup of $K^\times$ and the group $K^\times/(K^\times)^n$ is an abelian group (usually infinite) of exponent dividing n. We will

often write the same symbol for an element in $K^\times$ and its image in $K^\times/(K^\times)^n$. We can now restate 5. and 6. above as follows:

5. d is the order of a in $K^\times/(K^\times)^n$.

6. For $c \in K^\times$, L contains n-th root of c if and only if c belongs to the cyclic subgroup of $K^\times/(K^\times)^n$ generated by a.

Suppose now that $L = K(u_1, \ldots, u_s)$ is a finite extension of K which is generated by several elements u_1,..., u_s such tat $u_i^n = a_i \in K$ (we keep the assumptions about K as before).

a) Prove that $\mathrm{Gal}(L/K)$ is abelian of exponent dividing n.

b) Let $T = \{t \in L^\times : t^n \in K^\times\}$ and let $P = \{t^n : t \in T\}$. Then T is a subgroup of $L^\times$ which contains $K^\times$ and P is a subgroup of $K^\times$ which contains $(K^\times)^n$. Let $W = P/(K^\times)^n$, so W is a subgroup of $K^\times/(K^\times)^n$. For $\sigma \in \mathrm{Gal}(L/K)$ and $w \in W$ choose $t \in T$ such that $t^n = w$. Prove that $\sigma(t)/t \in \mu_n$ does not depend on which t you choose. We define $< \sigma, w >$ to be the quantity $\sigma(t)/t \in \mu_n$.

c) In b) we defined a function $< -, - >$: $\mathrm{Gal}(L/K) \times W \longrightarrow \mu_n$. Prove that this function is bilinear and non-degenerate. Conculde that $\mathrm{Gal}(L/K)$ is naturally isomorphic with $\mathrm{Hom}(W, \mu_n)$. Conclude that the groups W and $\mathrm{Gal}(L/K)$ are isomorphic.

d) Conversely, suppose that W is a finite subgroup of $K^\times/(K^\times)^n$. Then we can define the field L_W as follows: for every $w \in W$ choose $k_w \in K^\times$ representing w and set L_W to be the splitting field of $\prod_{w \in W}(x^n - k_w)$. Prove that L_W/K is Galois with Galois group isomorphic to $\mathrm{Hom}(W, \mu_n)$.

e) We will show soon that if K contains all n-th roots of 1 and L/K has cyclic group of order n as the Galois group then $L = K(u)$, where u is a root of $x^n - a$ for some $a \in K^\times$. Use this and the above results to conclude that if A is a finite abelian group of exponent n then there is a bijection between finite subgroups of $K^\times/(K^\times)^n$ which are isomorphic to A and finite extensions L/K with $\mathrm{Gal}(L/K)$ isomorphic to A (which assignes subgroup W to the field L_W).

Remark. We have established a bijection between finite abelian extensions of K of exponent dividing n and finite subgroups of $K^\times/(K^\times)^n$. This correspondence can be nicely generalized as follows. Fix an algebraic closure F of K. All extensions of K will be assumed to be inside F. We can easily see that there is the largest extension $K(n)$ of K which is abelian of exponent dividing n. It corresponds to $W = K^\times/(K^\times)^n$, i.e. it is the splitting field of all polynomials $x^n - t$, where $t \in K^\times$. Let $\Gamma(n) = \mathrm{Aut}(K(n)/K)$. We need to consider a natural topology on $\Gamma(n)$ which makes it a compact, totally disconnected group (i.e. a profinite group) (I am not going to describe this topology here). We also consider $K^\times/(K^\times)^n$ as a topological group with discrete topology and we identify μ_n with the unique cyclic subgroup of order n of the group $\mathbb{Q}/\mathbb{Z}$, with discrete topology. Then the bilinear map considered above becomes a continuous map $< , >$: $\Gamma(n) \times K^\times/(K^\times)^n \longrightarrow \mathbb{Q}/\mathbb{Z}$ and it gives natural isomorphisms $\Gamma(n) \simeq \mathrm{Hom}_{cont}(K^\times/(K^\times)^n, \mathbb{Q}/\mathbb{Z})$ and $K^\times/(K^\times)^n \simeq \mathrm{Hom}_{cont}(\Gamma(n), \mathbb{Q}/\mathbb{Z})$. The subscript *cont* indicates that only continuous homomorphisms are considered and the Hom groups are appropriately topologized so the isomorphisms are of topological groups. Now extendidng the problem, every subgroup W of $K^\times/(K^\times)^n$ corresponds to a subfield L_W of $K(n)$. It is not hard to see that if $\Gamma_W = \{\tau \in \Gamma(n) :< \tau, w >= 0 \text{ for all } w \in W\}$ then $\Gamma_W = \mathrm{Aut}(K(n)/L_W)$ is a closed subgroup of $\Gamma(n)$ and $L_W = K(n)^{\Gamma_W}$. Moreover, $\mathrm{Aut}(L_W/K) \simeq \Gamma(n)/\Gamma_W$ (recall that $\Gamma(n)$ is abelian). Conversely, if Γ is a closed subgroup

of $\Gamma(n)$ then $L = K(n)^{\Gamma}$ is a subfield of $K(n)$, hence $L = L_W$ for some W. It is not hard to see that $W = \{w \in K^{\times}/(K^{\times})^n :< \tau, w >= 0 \text{ for all } \tau \in \Gamma\}$. These results are usually referred to as Kummer theory.