Topics in field theory: exercises

Mathematisch Instituut, Universiteit Leiden, Fall 2013
Bart de Smit & Hendrik Lenstra
http://www.math.leidenuniv.nl/∼desmit/edu/topics_ft_2013/

Exercise 48 (preferred). The *additive Hilbert Theorem 90* asserts that, for a Galois extension $k \subset l$ of fields with group G and a function $a\colon G \to l$, the following two statements are equivalent:

(i) the map a is continuous if l is given the discrete topology, and for all σ, $\tau \in G$ one has $a(\sigma\tau) = a(\sigma) + \sigma(a(\tau))$;

(ii) there exists $b \in l$ such that for all $\sigma \in G$ one has $a(\sigma) = b - \sigma(b)$.

In class, a proof of this theorem was sketched. Provide the details of this proof.

Exercise 64. Let A and B be commutative rings. Suppose that there exists a ring into which both A and B can be embedded as subrings (with the same 1). Prove that there is a *commutative* ring with that property.

Exercise 65. Let $k \subset l$ be a Galois extension of fields with Galois group G, let H be a closed subgroup of G, and let W be an l-vector space. Prove that every continuous semilinear action of H on W can be extended to a continuous semilinear action of G on W.

Exercise 66 (for the ambitious). Let A and B be commutative rings of characteristic 0. Exercise 40(b) gives a necessary condition for the existence of a commutative ring into which A and B can be embedded as subrings, and it was wrongly claimed that this condition is also sufficient. Can you formulate a similar but stronger condition and prove that it is both necessary and sufficient?

Exercise 67. Let G be the projective limit of a directed system of groups G_i. Give each G_i the discrete topology, $\prod_i G_i$ the product topology, and $G \subset \prod_i G_i$ the restriction topology. Prove that every continuous group homomorphism $G \to \mathbf{R}/\mathbf{Z}$ factors through one of the maps $G \to G_i$.

Exercise 68 (preferred). Let $k \subset l$ be a finite Galois extension of fields, with group G, and let $a\colon G \to l^*$ be a 1-cocycle. Define $t\colon l \to l$ by $t(x) = \sum_{\sigma \in G} a(\sigma)\sigma(x)$. Prove that t is a k-linear map, that its image $t(l)$ has k-dimension 1, and that $t(l) = \{b \in l^* : \text{ for all } \sigma \in G \text{ one has } a(\sigma) = b/\sigma(b)\} \cup \{0\}$.

Exercise 69. Deduce the additive Hilbert theorem 90 (see Exercise 48) from the normal basis theorem (see Exercise 50) and Exercise 55. (Do include the case of infinite Galois extensions.)

In the following two exercises, 1-cocycles are *not* assumed to be continuous; so, for a topological group G and a topological G-module A, we write $Z^1(G, A)$ for the group of *all* 1-cocycles $G \to A$, and $H^1(G, A) = Z^1(G, A)/B^1(G, A)$.

Exercise 70. Let $\bar{\mathbf{Q}}$ be an algebraic closure of $\mathbf{Q}$. Prove that there exists a group homomorphism $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{Z}/2\mathbf{Z}$ that is not continuous, and that $H^1(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}), \bar{\mathbf{Q}}^*)$ is not the trivial group.

Exercise 71 (preferred). Let k be a finite field, write $q = \#k$, and let l be an algebraic field extension of k. Let $\varphi\colon l \to l$ be the Frobenius map, defined by $\varphi(\alpha) = \alpha^q$ (for $\alpha \in l$).

(a) Prove: one has $\varphi \in \mathrm{Aut}\, l$; the field l is Galois over k; and $\mathrm{Gal}(l/k)$ is topologically generated by φ in the sense that $\mathrm{Gal}(l/k)$ is the closure of the subgroup generated by φ.

(b) Let $a \in Z^1(\mathrm{Gal}(l/k), l^*)$, and let H be the subgroup $\mathrm{Gal}(l/k(a(\varphi)))$ of $\mathrm{Gal}(l/k)$. Prove: the restriction of a to H is a group homomorphism $H \to k^*$, and $a\colon \mathrm{Gal}(l/k) \to l^*$ is continuous.

(c) Prove: $H^1(\mathrm{Gal}(l/k), l^*)$ is the trivial group.

Exercise 72 (preferred). Let k be a finite field, write $q = \#k$, and let l be any field extension of k. Define $\varphi\colon l \to l$ by $\varphi(\alpha) = \alpha^q$ (for $\alpha \in l$). For $f = \sum_i a_i X^i \in k[X]$ and $\alpha \in l$ we define $f \circ \alpha = \sum_i a_i \varphi^i(\alpha)$.

(a) Prove that the map $k[X] \times l \to l$, $(f, \alpha) \mapsto f \circ \alpha$, makes the additive group of l into a module over $k[X]$.

(b) Prove that every finite $k[X]$-submodule of l is cyclic, i.e. of the form $k[X] \circ \alpha$ for some $\alpha \in l$. (*Hint.* Imitate the proof that each finite subgroup of l^* is cyclic.)

Exercise 73 (preferred). (a) Let $k \subset l$ be finite fields, and write $q = \#k$ and $n = [l : k]$. Use Exercise 72 to show that l has a normal basis over k, and prove that the number of $\alpha \in l$ that belong to a normal basis of l over k equals the order of the group $(k[X]/(X^n - 1))^*$.

(b) Prove that $\mathbf{F}_2[X]/(X^3 + X + 1)$ is a field, and find all normal bases of this field over $\mathbf{F}_2$.

Exercise 74 (preferred). (a) Let p be a positive integer. Assume that $2^p - 1$ is a prime number and that $X^p + X + 1 \in \mathbf{F}_2[X]$ is irreducible. Prove that $X^{2^p-1} + X + 1 \in \mathbf{F}_2[X]$ is irreducible. (You may use the results of Exercise 72.)

(b) Prove that the polynomial

$$X^{2^{2^{2^{2^2-1}-1}-1}-1} + X + 1$$

is irreducible over $\mathbf{F}_2$. (You may use that 170141183460469231731687303715884105727 is a prime number.)