HOMEWORK 10

Due date: Tuesday of Week 11

Exercises: 4.1, 6.1, 6.2, 6.3, 7.2, 7.7, 7.11, 8.2, 8.4. Pages 506-508

Problem 1. *Let K be the splitting field of $x^3 - 2 \in \mathbb{Q}[x]$ over $\mathbb{Q}$. Compute* $\mathrm{Gal}(K/\mathbb{Q})$.

Let $\alpha = \sqrt[3]{2}$. In one of our previous exam, you are required to compute the inverse of the element $a + b\alpha + c\alpha^2$ explicitly in $\mathbb{Q}[\alpha]$. Here $a, b, c \in \mathbb{Q}$ and at least one of them is nonzero. That is, find $x, y, z \in \mathbb{Q}$ such that $\frac{1}{a+b\alpha+c\alpha^2} = x + y\alpha + z\alpha^2$. It turns out that this is quite complicate. On the other hand, the inverse of the element $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ is very easy to compute. Actually, we know that

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{a-b\sqrt{2}}{a^2+2b^2}.$$

You may now see that the reason is the "conjugate" $a - b\sqrt{2}$ is easy to find. In our terminology of Galois theory, we have $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \sigma\}$, where σ is the element $\sigma(x + y\sqrt{2}) = x - y\sqrt{2}$. Since we know the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ explicitly now, we could find all of the conjugates of $a + b\alpha + c\alpha^2$. So it is possible to imitate the above example on $a + b\sqrt{2}$ to find the inverse of $a + b\alpha + c\alpha^2$.

Problem 2. *For $\alpha = \sqrt[3]{2}$. Find the inverse of $2 + \alpha$ explicitly using a similar method as in the $a + b\sqrt{2}$ case.*

The method described above is just

$$\frac{1}{a+b\alpha+c\alpha^2} = \frac{\prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q}),\sigma\neq 1}\sigma(a+b\alpha+c\alpha^2)}{\prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})}\sigma(a+b\alpha+c\alpha^2)}.$$

The bottom is just $\mathrm{Nm}_{K/\mathbb{Q}}(a+b\alpha+c\alpha^2)$, which is clearly in $\mathbb{Q}$. This is still very complicate, because the Galois group is relatively big. In the above, we work in the larger field K not $\mathbb{Q}(\alpha)$ directly. One reason is that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is not Galois. But it is possible to work over $\mathbb{Q}(\alpha)$ directly. In this case, instead of using the Galois group $\mathrm{Gal}(K/\mathbb{Q})$, one needs to use all $\mathbb{Q}$-embeddings $\mathbb{Q}(\alpha) \to \mathbb{C}$. This is indeed a little bit simpler.

1. Trace is non-degenerate for separable extensions

Problem 3. *Let G be a group and Ω be a field. Let $\chi_j : G \to \Omega^\times, j = 1, \ldots, m$ be pairwise distinct homomorphisms (namely, $\chi_j(g_1g_2) = \chi_j(g_1)\chi_j(g_2), \forall g_1, g_2 \in G$). Show that if $c_1, \ldots, c_m \in \Omega$ such that*

$$\sum_j c_j\chi_j(g) = 0, \forall g \in G,$$

then $c_j = 0$ for all j. In other words, $\chi_1, \ldots, \chi_n$ are linearly independent over Ω.

Hint: Consider a relation $\sum c_j\chi_j = 0$ with minimal nonzero c_j and try to obtain a relation with fewer lengths. This is Theorem 4.1 (a theorem of Dedekind), page 283 of Lang's book "Algebra".

Let K/F be a separable extension of degree n. Recall that for $\alpha \in K$, $\mathrm{Tr}_{K/F}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha)$, where $\{\sigma_1, \ldots, \sigma_n\}$ is the set of all F-embeddings $K \to \Omega$ for an algebraic closed field Ω with $K \subset \Omega$. See HW9, Problem 8.

Problem 4. *Let K/F be a separable extension of degree n. View K as a vector space over F of dimension n. Consider the map*

$$\psi : K \times K \to F,$$

$$\psi(\alpha, \beta) = \mathrm{Tr}_{K/F}(\alpha \cdot \beta).$$

Show that ψ is a non-degenerate bilinear map.

Here is the definition of non-degenerate bilinear map. Let V be a vector space over a field F. A bilinear map $f : V \to V \to F$ is called non-degenerate if it satisfies one of the following equivalent conditions:

(1) Let $\mathcal{B} = \{\alpha_i\}_{1 \le i \le n}$ be a basis of V, then the matrix $[f]_{\mathcal{B}} := (f(\alpha_i, \alpha_j))_{1 \le i,j \le n}$ is invertible;
(2) For any $\alpha \in V$, if $f(\alpha, \beta) = 0$ for all $\beta \in V$, then we have $\alpha = 0$;
(3) For any $\beta \in V$, if $f(\alpha, \beta) = 0$ for all $\alpha \in V$, then we have $\beta = 0$.

See page 365 of Hoffman-Kunze.

Hint: Let $\mathcal{B} = \{\alpha_i\}_{1 \le i \le n}$ be a basis of K/F and let $\{\sigma_1, \dots, \sigma_k\}$ be the set of all F-embeddings $K \to \Omega$ into a fixed algebraically closed field Ω. Consider the matrix $[\psi]_{\mathcal{B}} = (\psi(\alpha_i, \alpha_j)) = (\mathrm{Tr}(\alpha_i \alpha_j)) = (\sum_k \sigma_k(\alpha_i)\sigma_k(\alpha_j))_{1 \le i,j \le n}$. Let A be the matrix $(\sigma_k(\alpha_i))_{1 \le i,k \le n} \in \mathrm{Mat}_{n \times n}(\Omega)$. Show that $[f]_\psi = AA^t$. If $\det([f]_\psi) = 0$, then $\det(A) = 0$, which means $AX = 0$ has a nontrivial solution in Ω^n. Then use Dedekind's theorem (last problem). Notice that each σ_i can be viewed as a group homomorphism $K^\times \to \Omega^\times$.

Problem 5. *Let K/F be a separable extension of degree n. Show that there exists an element $\alpha \in K$ such that $\mathrm{Tr}_{K/F}(\alpha) \neq 0$.*

This is a consequence of the last problem. If K/F is not separable, then $\mathrm{Tr}_{K/F}$ is indeed identically zero. We have seen one example in last HW.

2. Finite fields

Let $F = \mathbb{F}_q$ with $q = p^r$ for some r. Let K/F be a finite field extension. Recall that K/F is Galois and $\mathrm{Gal}(K/F)$ is a cyclic group of order $[K : F]$ generated by $\mathrm{Frob}_F : K \to K$ defined by $\mathrm{Frob}_F(x) = x^q$. For simplicity, we write $\sigma = \mathrm{Frob}_F$ and thus $\mathrm{Gal}(K/F) = \{\sigma^j, 0 \le j \le n-1\}$.

Problem 6. *Let $F = \mathbb{F}_q$ and K/F be a field extension of degree n. What are the intermediate fields E of $F \subset K$? Give the explicit bijections between the intermediate fields and the subgroup of* $\mathrm{Gal}(K/F)$.

Problem 7. *Let $F = \mathbb{F}_q$ with $q = p^r$ and let K/F be a finite extension of degree n. Given $\alpha \in K$, show that*

$$\mathrm{Tr}_{K/F}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}} = \sum_{j=0}^{n-1} \sigma^j(\alpha).$$

and

$$\mathrm{Nm}_{K/F}(\alpha) = \prod_{j=0}^{n-1} \alpha^{q^j} = \prod_{j=0}^{n-1} \sigma^j(\alpha).$$

Problem 8. *Let $F = \mathbb{F}_q$ and K/F be a finite field extension of degree n. Let $\alpha \in K$. Show that $\mathrm{Tr}_{K/F}(\alpha) = 0$ iff there exists an element $u \in K$ such that $\alpha = u - u^q$.*

One direction is easy. Conversely, suppose that $\mathrm{Tr}(\alpha) = 0$. Take $\beta \in K$ such that $\mathrm{Tr}_{K/F}(\beta) \neq 0$. Such a β exists by Problem 5. Then consider the element

$$u = \frac{1}{\mathrm{Tr}_{K/F}(\beta)}(\alpha\sigma(\beta) + (\alpha + \sigma(\alpha))\sigma^2(\beta) + \cdots + (\alpha + \sigma(\alpha) + \cdots + \sigma^{n-2}(\alpha))\sigma^{n-1}(\beta))$$

and prove $\alpha = u - u^q$.

Problem 9. *Let $F = \mathbb{F}_q$ with $q = p^r$ for some r. Given $\alpha \in F$. Show that the polynomial $f = x^p - x - \alpha \in F[x]$ is either irreducible or a product of linear factors. Moreover, show that f is irreducible iff* $\mathrm{Tr}_{F/\mathbb{F}_p}(\alpha) \neq 0$

Hint: Given a root u of f in some field extension, consider $u + c$ for $c \in \mathbb{F}_p$.

Problem 10. *Let $F = \mathbb{F}_q$ with $q = p^r$ for some r. Given $\alpha \in F$. Suppose the polynomial $f = x^p - x - \alpha \in F[x]$ is irreducible. Compute its Galois group G_f.*