Math 371, Spring 2013, PSet 3

Aaron Michael Silberstein

February 19, 2013

This problem set will be due Friday, March 1, 2013 at 1 pm in Matti's mailbox.

1 The group S_3

S_3 is the group of permutations on 3 elements. These problems should be review, and I am assuming you know about cycle notation. If not, check your textbook!

1. List the elements in S_3.
2. List the subgroups of S_3.
3. List the normal subgroups of S_3.
4. List the conjugacy classes of S_3.

2 The Group Algebra I

Let G be a finite group, and R a ring. We may define the **group algebra** to consist of formal sums

$$R[G] =_{\text{def}} \left\{ \sum_{g \in G} r_g g \right\}$$

where multiplication is given by

$$\left(\sum_{g \in G} r_g g \right) \left(\sum_{h \in G} r'_h h \right) = \sum_{\gamma \in G} \left(\sum_{gh = \gamma} r_g r'_h \right) \gamma.$$

From now on, we assume R is a commutative ring with identity.

1. Verify that $R[G]$ is a ring.

2. For which groups G is $R[G]$ commutative? Prove your assertion.

3. If $\varphi : G \to H$ is a homomorphism, prove that φ extends to a ring homomorphism $R[\varphi] : R[G] \to R[H]$.

4. The **center** of a non-commutative ring S is the set

$$Z(S) = \{z \in S \mid \forall\, s \in S, zs = sz\}\,.$$

Prove that $Z(S)$ is a ring.

5. If k is a field, write down a basis of $k[G]$ as a k-vector space. Write down a basis of $Z(k[G])$ as a k-vector space.

3 The General Cubic Extension

Let k be a field, and $k(\alpha_1, \alpha_2, \alpha_3)$ be the field of rational functions in three variables over k — that is, $k(\alpha_1, \alpha_2, \alpha_3)$ is the field of fractions of the polynomial ring $k[\alpha_1, \alpha_2, \alpha_3]$. Let

$$a_1 = \alpha_1 + \alpha_2 + \alpha_3; a_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3; \text{ and } a_3 = \alpha_1\alpha_2\alpha_3.$$

1. Let S_3 act on $k(\alpha_1, \alpha_2, \alpha_3)$ by ring homomorphisms by permuting the α_i's. Prove that the fixed field of $S^3, k(\alpha_1, \alpha_2, \alpha_3)^{S_3}$, is $k(a_1, a_2, a_3)$ (hint: last week's problem set!).

2. What is $\dim_{k(a_1,a_2,a_3)} k(\alpha_1, \alpha_2, \alpha_3)$? Write down a basis.

3. Let $K = k(a_1, a_2, a_3, \alpha_1)$. What is $\dim_{k(a_1,a_2,a_3)} K$? Prove that $\mathrm{Aut}(K/k(a_1, a_2, a_3))$ is trivial.

4. Let $f(x) = x^3 - a_1x^2 + a_2x + a_3$. Prove that $f(x)$ splits into a product of linear factors in $k(\alpha_1, \alpha_2, \alpha_3)$, but not in any subfield. We call $k(\alpha_1, \alpha_2, \alpha_3)$ a **splitting field** of f over $k(a_1, a_2, a_3)$.

4 The Cyclic Cubic Extension

Let k be a field, and let $\kappa(t) = t^3 - \xi$ be an irreducible polynomial. Let C_3 be the cyclic group of order 3.

1. Prove that k_κ (the Kronecker construction applied to $\kappa : k_\kappa = k[t]/(\kappa(t)))$ has a nontrivial automorphism fixing k if and only if k contains an element μ such that $\mu^3 = 1$ and $\mu \neq 1$ (that is, k **contains a cube root of unity**). What is $\mathrm{Aut}(k_\kappa/k)$?

2. Prove that $k[C_3] \simeq k[t]/(t^3-1)$. Prove that if k contains a cube root of unity μ,

$$k[C_n] \simeq \prod_{i=1}^{3} k[t]/(t-\mu^i) \simeq \prod_{i=1}^{3} k.$$

Let e_i be the element (guaranteed by the Chinese Remainder theorem) 1 (mod $(t-\mu^i)$) and 0 (mod $(t-\mu^j)$) for $i \neq j$, e_i. Write these out explicitly (that is, as sums of elements of C_3.

3. Prove that a field of characteristic 3 cannot contain a cube root of unity.

Let k be a field containing a cube root of unity, and let K/k be an extension of degree 3 (that is, $\dim_k K = 3$) with a nontrivial automorphism σ, fixing k elementwise. Then K is a $k[\langle\sigma\rangle]$-module — a module over the group ring over k of the group generated by σ.

1. Let M/L and L/K be field extensions. Prove that $\dim_K M = (\dim_L M)(\dim_K L)$.

2. Show that σ has order ≤ 3. Why can't it have order 2? Deduce that the order of σ is 3.

3. Prove that $\mathrm{Aut}(K/k) = C_3$; that is, it is generated by σ (hint: K must be gotten by the Kronecker construction on k for a polynomial of degree 3).

4. Prove that if a polynomial f is irreducible in $k[t]$ and has a root in K then it splits completely in K, and has degree 3 (hint: use the automorphism to write down the roots of f).

5. Prove that $e_i(K)$ must not be zero for i either 1 or 2; thus, there is an element $\xi \in K$ such that $\sigma(\eta) = \mu^i\eta$. Prove that $\eta^3 \in k, \sigma(\eta^2) = \mu^{2i}\eta^2$, and $K = k(\eta)$.

This is called **Hilbert's Satz 90 for Cubic Extensions**: if k contains a third root of unity, any cubic field extension K/k with a nontrivial automorphism σ is of the form $K[\sqrt[3]{\xi}]$ for some $\xi \in k$. If whenever f were cubic and k contained a cube root of unity, $k[t]/(f)$ had a nontrivial automorphism, we would immediately be able to write down a cubic formula like we wrote down a quadratic formula. However, from problem 3 of section 3, we see that we cannot be so naïve. We will use the structure of $k[S_3]$ to salvage this situation in next week's problem set.