Algebra 2: Problem Sheet 1

Robert Kropholler

January 31, 2018

Throughout F will denotes a field and $\mathbb{F}_p$ will denote the field with p elements.

1. Let $f(x) = x^3 + 9x + 6 \in \mathbb{Q}[x]$.
   (a) Show that this polynomial is irreducible.
   (b) Let α be a root of $f(x)$. Recall that $\{1, \alpha, \alpha^2\}$ is a basis for $\mathbb{Q}(\alpha)$. Find an expression for $\frac{1}{\alpha}$ in this basis.
   (c) Find an expression for $\frac{1}{1+\alpha}$.
2. Finish the proof of the tower law (Show that the set given in class is linearly independent.)
3. Let $D\colon F[x] \to F[x]$ be formal differentiation defined as follows
   $$D(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) = n a_n x^{n-1} n + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$$
   Show that this functions satisifes the following:
   (a) $D(af + bg) = aDf + bDg$ where $a, b \in F$.
   (b) $D(fg) = gDf + fDg$.
   (c) $D(f(g(x))) = DgDf(g(x))$.

   Let $a \in F$. Show that $(x-a)^2$ divides $f(x)$ iff $f(a) = Df(a) = 0$.

   Deduce that if f and Df are relatively prime, then f has no repeated roots in F.
4. Show that if $a \in \mathbb{Z}$ is divisible by p but not p^2, then $x^n - a$ is irreducible and has no repeated roots in any extension F of $\mathbb{Q}$.
5. Show that if m is a positive integer, then the polynomial $x^{p^m} - x$ has no repeated roots in any extension F of $\mathbb{F}_p$.

   Let
   $$L = \{\alpha \in F \mid \alpha^{p^m} = \alpha\},$$
   be the set of root of $x^{p^m} - x$ in F.

Show that L is a subfield of F. (Hint: Show that $(a+b)^p = a^p + b^p$ for all $a, b \in F$)

Let n be a positive integer dividing m. Show that $p^n - 1$ divides $p^m - 1$ in $\mathbb{Z}$. Show that in this case $x^{p^n} - x$ divides $x^{p^m} - x$.

6. Let F be a finite field show that $|F| = p^n$ for some prime p (Hint: Conside the prime subfield of F.)

7. Find the degree of the splitting fields of the following:

   (a) $x^3 - 1$ over $\mathbb{Q}$.

   (b) $x^3 - 2$ over $\mathbb{Q}$

   (c) $x^2 + 1$ over $\mathbb{F}_5$

   (d) $x^2 + 1$ over $\mathbb{F}_7$

8. Let $f(x) \in F[x]$ be of degree d. Show that the splitting field of $f(x)$ has degree $\leqslant d!$ over F.

9. Let $\bar{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q}\}$.

   Show that $\bar{\mathbb{Q}}$ is the union of all subfields of $\mathbb{C}$ which are finite extensions of $\mathbb{Q}$.

   Prove that $\bar{\mathbb{Q}}$ is a subfield of $\mathbb{C}$. (Hint: Consider the extension $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ for algebraic numbers α, β)

   Prove that $\bar{\mathbb{Q}}$ is not a finite extension of $\mathbb{Q}$.

10. (Optional) Show that the algebraic closure of a countable field is countable.