## Math 422/501: Problem set 6 (due 21/9/09)

### $\mathbb{Q}(\sqrt[3]{2})$

1. Let $K = \mathbb{Q}(\alpha)$ where $\alpha^3 = 2$. By Eisenstein's criterion ($p = 2$), $x^3 - 2 \in \mathbb{Q}[x]$ is irreducible. Without using the tools from abstract algebra:
   (a) Show by hand that $\{1, \alpha, \alpha^2\} \subset K$ is linearly independent over $\mathbb{Q}$.
   *Hint*: You may use the irreducibility of $x^3 - 2$.
   (b) Show by hand that $\{1, \alpha, \alpha^2\}$ is a basis for $K$.
   *Hint*: It is enough to show that $\{a + b\alpha + c\alpha^2\} \subset K$ is closed under addition and multiplication, and that each element has an inverse.
   – Conclude that $[K : \mathbb{Q}] = 3$.

2. (The hard way) Let $\beta \in K$ satisfy $\beta^3 = 2$.
   (a) Write $\beta = a + b\alpha + c\alpha^2$, and convert the equation $\beta^3 = 2 = 2 + 0\alpha + 0\alpha^2$ to a system of three non-linear equations in the three variables $a, b, c$.
   *Hint*: You need to use the fact that $\{1, \alpha, \alpha^2\}$ is a basis at some point.
   (b) Taking a clever linear combination of two of the equations, show that $a = 0$.
   (c) Now show that $b = 1$, $c = 0$, that is that $\beta = \alpha$.

3. (The easy way) Let $\beta \in K$ satisfy $\beta^3 = 2$ and assume that $\beta \neq \alpha$.
   (a) Let $\gamma = \beta/\alpha$ and show that $\gamma^3 = 1$.
   (b) Let $m(x) \in \mathbb{Q}[x]$ be the minimal polynomial of $\gamma$ over $\mathbb{Q}$. Show that $\deg m = 2$.
   *Hint*: Start by showing that $m$ is an irreducible factor of $x^3 - 1$.
   (c) Consider the field $\mathbb{Q}(\gamma) \subset K$. Show that $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 2$ and obtain a contradiction.
   *Hint:* $[K : \mathbb{Q}] = [K : \mathbb{Q}(\gamma)] \cdot [\mathbb{Q}(\gamma) : \mathbb{Q}]$.

### Prime fields and the characteristic

4. Let $K$ be a field.
   (a) Show that there is a unique ring homomorphism $\varphi : \mathbb{Z} \to K$.
   (b) Let $p \geq 0$ be such that $\mathrm{Ker}(\varphi) = (p)$. Show that either $p = 0$ or $p$ is prime.

   DEFINITION. We call $p$ the *characteristic* of $K$.

   (c) Let $K$ be a field of characteristic $p > 0$. Show that the image of $\varphi$ is the intersection of all subfields of $K$, and that it isomorphic to the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
   (d) Let $K$ be a field of characteristic zero. Show that there is a unique homomorphism $\mathbb{Q} \hookrightarrow K$ and conclude that the minimal subfield of $K$ is isomorphic to $\mathbb{Q}$.

5. (Finite fields)
   (a) Let $K$ be a finite field. Show that there exists a prime $p$ and a natural number $n$ so $|K| = p^n$.
   (b) Show that there exists a field of order 4.
   *Hint*: Construct an irreducible quadratic polynomial in $\mathbb{F}_2[x]$.
   (c) Show that there is a unique field of order 4.

REMARK. We will see that for each prime power there is a field of that order, unique up to isomorphism.

## Quadratic fields

Let $K$ be a field of characteristic not equal to 2. Write $K^\times$ for the multiplicative group of $K$, $(K^\times)^2$ for its subgroup of squares.

6. (Reduction to squares) Let $L/K$ be an extension of degree 2.
   (a) Show that there exists $\alpha \in L$ such that $K(\alpha) = L$. What is the degree of the minimal polynomial of $\alpha$?
   (b) Show that there exist $d \in K^\times$ such that $L : K$ is isomorphic to $K(\sqrt{d}) : K$.
   *Hint:* Complete the square.

7. (Classifying the extensions)
   (a) Assume that $d \in K^\times$ is not a square. Using the representation $K(\sqrt{d}) = \left\{a + b\sqrt{d} \mid a, b \in K\right\}$ show that $e \in K$ is a square in $K(\sqrt{d})$ iff $e = df^2$ for some $f \in K$. Where did you use the assumption about the characteristic?
   (b) Show that the extensions $K(\sqrt{d})$ and $K(\sqrt{e})$ are isomorphic iff $\frac{d}{e} \in (K^\times)^2$ (in general, the isomorphism will not make $\sqrt{d}$ to $\sqrt{e}$).
   *Hint:* Construct a $K$-homomorphism $K(\sqrt{e}) \to K(\sqrt{d})$. Why is it surjective? Injective?
   (c) Show that quadratic extensions of $K$ are in bijection with non-trivial elements of the group $K^\times/(K^\times)^2$.

8. (Applications)
   (a) Show that $\mathbb{R}$ has a unique quadratic extension.
   (b) Show that $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
   *Hint*: Show that $\sqrt{6} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ but that $\sqrt{2} + \sqrt{3} \neq a + b\sqrt{6}$ for any $a, b \in \mathbb{Q}$.

## Simple extensions

9. Let $K(\alpha) : K$ be a simple extension.
   (a) If $\alpha$ is algebraic, show that there are finitely many subfields $L$ of $K(\alpha)$ containing $K$.
   *Hint:* consider the minimal polynomial of $\alpha$ over $L$.
   (b) If $\alpha$ is transcendental, show that there are infinitely many intermediate fields $L$.

10. Let $L : K$ be an extension of fields with finitely many intermediate subfields.
    (a) Show that the extension is algebraic.
    (b) Show that the extension is *finitely generated*: there exists a finite subset $S \subset L$ so that $K = K(S)$.
    (c) Show that $L : K$ is finite.

11. Let $L : K$ be an extension of infinite fields with finitely many intermediate fields.
    (a) Given $\alpha, \beta \in L$ find $\gamma \in L$ so that $K(\alpha, \beta) = K(\gamma)$.
    *Hint*: Consider elements of the form $\gamma = \alpha + k\beta$ where $k \in K$.
    (d) Show that $L : K$ is a simple algebraic extension.

## Algebraicity

12. Let $M : L$ and $L : K$ be algebraic extensions of fields. Show that $M : L$ is algebraic.