# MATH 113 - HOMEWORK 7

**Not due**

**1.** Let $f, g \in \mathbf{Q}[x]$ and assume that $f$ is irreducible. If $f$ and $g$ share a common root in $\mathbf{C}$, prove that $f|g$.

**2.** *Algebraic Closures*

**(a)** Let $F$ be a finite field extension of $\mathbf{C}$. Prove that $F \cong \mathbf{C}$.

For the rest of the exercise, let $K \subseteq L$ be a fixed field extension.

**(b)** If $\alpha \in L - \{0\}$ is algebraic over $K$, prove that $\alpha^{-1}$ is algebraic over $K$ [Hint: What is $K(\alpha^{-1})$] .

**(c)** If $\alpha, \beta \in L$ algebraic over $K$. Prove that $\alpha + \beta$, $\alpha\beta$ are algebraic over $K$.

**(d)** Conclude that $\sqrt{2} + \sqrt[5]{14} - \sqrt[3]{2+5} + 4 \in \mathbf{R}$ is algebraic over $\mathbf{Q}$.

**3.** *Multiplicity of degree in towers:* Let $K \subseteq L$ and $L \subseteq M$ be field extensions and assume that $K \subseteq M$ is finite.

**(a)** Prove that $K \subseteq L$ and $L \subseteq M$ are finite extensions (Hint: This is just a statement about vector spaces).

**(b)** If $\{a_1, \ldots, a_n\}$ is a basis for $L$ over $K$ and $\{b_1, \ldots, b_m\}$ is a basis for $M$ over $L$, prove that $\{a_i b_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ is a basis for $M$ over $K$. Conclude that $[M : K] = [M : L][L : K]$.

**4.** For $\alpha$ given below, compute the minimal polynomial of $\alpha$ and find the degree of the extensions $\mathbf{Q}(\alpha)/\mathbf{Q}$.

**(a)** $\alpha = \sqrt{-3}$

**(b)** $\alpha = \sqrt{2} - \sqrt{10}$

**(c)** $\alpha = \sqrt{3} + i$

**5.** *Some automorphism (Galois) groups*

**(a)** Show that the only automorphism of $\mathbf{Q}(\sqrt[3]{2})$ is the identity i.e. $\mathrm{Aut}(\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}) \cong \{\mathrm{id}\}$ is trivial.

In the rest of the exercise you'll compute $\mathrm{Aut}(\mathbf{Q}(\sqrt{3}+i)/\mathbf{Q})$ (also see part **(e)**). Let $S = \mathrm{Hom}(\mathbf{Q}(\sqrt{3}+i), \mathbf{C})$ denote the set of embeddings of $\mathbf{Q}(\sqrt{3}+i)$ into $\mathbf{C}$.

**(b)** Show that $\mathbf{Q}(\sqrt{3}, i) = \mathbf{Q}(\sqrt{3}+i)$ and conclude that $\psi \in S$ is "determined" by $\psi(i)$ and $\psi(\sqrt{3})$.

**(c)** Prove that $\mathrm{Aut}(\mathbf{Q}(\sqrt{3}+i)/\mathbf{Q}) = S$ [Hint: What can $\psi(i)$, $\psi(\sqrt{3})$ be, for $\psi \in S$?].

**(d)** Prove that $\mathrm{Aut}(\mathbf{Q}(\sqrt{3}+\sqrt{i})/\mathbf{Q}) \cong (\mathbf{Z}/2\mathbf{Z})^2$ [Hint: Compute the order of $\psi \in \mathrm{Aut}(\mathbf{Q}(\sqrt{3}, i))$]

**(e)** [Bonus] Show that $\mathbf{Q}(\sqrt{3}, i)$ is a splitting field and conclude that $\mathrm{Gal}(\mathbf{Q}(\sqrt{3}, i)/\mathbf{Q}) \simeq (\mathbf{Z}/2\mathbf{Z})^2$ [Hint: Find *some* polynomial with roots $\sqrt{3}, i$...]

---

You don't need to know the following for the exam, but working through some of these problems might help you understand some of this material.

**Goal** Find an example of an algebraic extension that's NOT finite.

**x.** *Cyclotomic polynomials*

**(a)** Let $K$ be a field and $f \in K[x]$, for any $\alpha \in K$ we obtain a polynomial $f(x+\alpha) \in K[x]$ (what does this mean?). Prove that $f(x)$ is irreducible iff $f(x+\alpha)$ is irreducible.

For the rest of the question, let $p$ be a prime and let $f(x) = 1 + x + x^2 + \cdots + x^{p-1} \in \mathbf{Q}[x]$.

**(b)** Prove that the binomial coefficient $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ is divisible by $p$ for $1 \leq k \leq p-1$.

**(c)** Prove that $f(x+1) = \sum_{k=1}^{p} \binom{p}{k} x^{k-1}$ [Hint: Formally manipulate, $f(x) = \frac{x^p-1}{x-1}$]

**(d)** Prove that $f$ is irreducible.

**xx.** *Roots of unity and infinite algebraic extensions*

Throughout this question, $\zeta_n = e^{\frac{2\pi i}{n}}$ for $n \geq 1$ (recall that $e^{2\pi i} = 1$).

**(a)** Use **Problem x** to prove that the degree of $\mathbf{Q}(\zeta_p)$ over $\mathbf{Q}$ is $p-1$.

**(c)** For any $n \geq 1$, prove that the degree of $\mathbf{Q}(\zeta_n)$ over $\mathbf{Q}$ is finite.

**(d)** Let $\mathbf{Q}(\zeta_\infty) := \bigcup_{n \geq 1} \mathbf{Q}(\zeta_n) \subseteq \mathbf{C}$. Prove that $\mathbf{Q}(\zeta_\infty)$ is a subfield of $\mathbf{C}$.

**(e)** Prove that $\mathbf{Q}(\zeta_\infty)$ is algebraic but not finite over $\mathbf{C}$.

**Note** It's a deep theorem of algebraic number theory that $\mathbf{Q}(\zeta_\infty)$ is the maximal "abelian" extension of $\mathbf{Q}$. More precisely, if $K$ is an extension of $\mathbf{Q}$ with $\mathrm{Gal}(K, \mathbf{Q})$ abelian, then $K$ is a subfield of $\mathbf{Q}(\zeta_\infty)$; this is called the Kronecker-Weber Theorem. For example, since $\mathrm{Gal}(\mathbf{Q}(\sqrt{5}), \mathbf{Q}) \cong \mathbf{Z}/2\mathbf{Z}$, what I just said should imply that $\mathbf{Q}(\sqrt{5}) \subseteq \mathbf{Q}(\zeta_\infty)$. This can be seen explicitly from the (non-trivial) observation that $\sqrt{5} = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4$.