Math 504 **Homework 1** **Fall 2013**

(1) Let R be the ring of continuous functions $[0,1] \to \mathbb{R}$ with point-wise addition and multiplication. Prove that the set of functions vanishing at a point $x \in [0,1]$ is a maximal ideal in R—we denote it by $\mathfrak{m}_x$. If $\mathfrak{m}$ is a maximal ideal of R that is not equal to $\mathfrak{m}_x$ for any $x \in [0,1]$ show that there are a finite set of elements $f_1, \ldots, f_n$ in $\mathfrak{m}$ that have no common zero on $[0,1]$; by considering $f_0^2 + \cdots + f_1^2$ show there is no such $\mathfrak{m}$; i.e., the maximal ideals in R are the ideals $\mathfrak{m}_x$, $x \in [0,1]$.

(2) Factor $x^8 - 1$ and $x^{12} - 1$ in $\mathbb{Q}[x]$.

(3) If d and e are greatest common divisors of $\{a_1, \ldots, a_n\}$ in a domain R show that d and e are associates, i.e., unit multiples of each other.

(4) Let $k[x,y]$ be the polynomial ring on two variables with coefficients in the field k. Show that the ideal $k[x,y]_{\geq n} = \text{span}\{x^i y^j \mid i+j \geq n\}$ can be generated by $n+1$ elements but not by n elements. (Hint: think of degree.)

(5) Show that the ring of Gaussian integers, $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$, is a Euclidean domain with respect to the function $\delta : \mathbb{Z}[i] \to \mathbb{Z}$ defined by $\delta(x) := x\bar{x}$ where $\bar{x}$ denotes the complex conjugate of x.

(6) Factor 2, 3, and 5, in $\mathbb{Z}[i]$ as products of primes.

(7) Prove that a Euclidean domain is a PID.

(8) Let $k[x, x^{-1}]$ be the subring of $k(x)$ generated by x, x^{-1}, and k. Is $k[x, x^{-1}]$ a PID? Why?

(9) Let d be a square-free positive integer. Define the norm function $N : \mathbb{Z}[\sqrt{-d}] \to \mathbb{Z}$ by $N(a + b\sqrt{-d}) = a^2 + b^2 d$.
   (a) Establish some important properties of N.
   (b) Show that u is a unit in $\mathbb{Z}[\sqrt{-d}]$ if and only if $N(u) = 1$.
   (c) Show that the only units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$.
   (d) If $d > 1$ show that only units in $\mathbb{Z}[\sqrt{-d}]$ are ± 1.

(10) Find an irreducible element in $\mathbb{C}[x,y,z]/(xy - z^2)$ that is irreducible but not prime. Hint: think about homogeneous polynomials.

Math 504 **Homework 2** **Fall 2013**

(1) Show that the fields $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{7})$ are not isomorphic.
(2) Let $\mathbb{F}_{11}$ be the field with 11 elements. Let $K = \mathbb{F}_{11}(\alpha)$ where α is a root of $x^2 - 2$. Let $L = \mathbb{F}_{11}(\beta)$ where β is a root of $x^2 - 4x + 2$. Show there is an isomorphism $\Phi : K \to L$ that is the identity on $\mathbb{F}_{11}$.
(3) Let K/k be a degree-two field extension. If $\mathrm{char}(k) \neq 2$ show that $K = k(\alpha)$ where α is a root of a polynomial $x^2 - d$ for some $d \in k$. Show this fails in characteristic two.
(4) Let K/k be a degree-two field extension and suppose that $\mathrm{char}(k) = 2$. Show that $K = k(\alpha)$ where α is a root of a polynomial $x^2 + x + d$ for some $d \in k$.
(5) Let f be a polynomial of degree n in $k[x]$. Show that the images of $1, x, \dots, x^{n-1}$ in $k[x]/(f)$ form a basis for $k[x]/(f)$.
(6) Find the minimal polynomial of $\sqrt{3}+\sqrt{5}$ over the fields $\mathbb{Q}$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{10})$, and $\mathbb{Q}(\sqrt{15})$.
(7) Let f and g be non-zero polynomials in $k[x]$ and write z for $f(t)/g(t)$ which is an element in the field $k(x)$. Compute $[k(x) : k(z)]$.
(8) Let $\alpha = \frac{1}{2}(1 + \sqrt{5})$ denote the Golden ratio. You are used to writing numbers to base 10, or other integer bases. This problem is about base α. Let $a_n, a_{n-1}, a_{n-2}, \dots$ be an infinite sequence of numbers in $\{0, 1\}$ with the property that $a_i a_{i+1}$ is never equal to 11. We will write

$$\beta = a_n \dots \alpha_1 a_0 \bullet \alpha_{-1}\alpha_{-2} \dots$$

for

$$\beta = \sum_{j=-n}^{\infty} a_{-j}\alpha^{-j}$$

and call this the α-expansion for β.
  (a) Find the α-expansions for $2, 3, 4, 5$.
  (b) What is the number with α-expansion $0 \cdot 101010\dots$?
  (c) What is the number with α-expansion $0 \cdot 100100100\dots$?
(9) Let $\omega = e^{2\pi i/5}$. Find the minimal polynomial for $\omega^2 + \omega^3$ over $\mathbb{Q}$ and the degree of $\mathbb{Q}(\omega^2 + \omega^3)$ over $\mathbb{Q}$.
(10) A complex number is algebraic if it is the root of an irreducible polynomial with coefficients in $\mathbb{Q}$. If α and β are algebraic show that $\alpha + \beta$ and $\alpha\beta$ are also algebraic. Hint: use another characterization of algebraic numbers, and the formula $[K : L][L : k] = [K : k]$ for field extensions $k \subset L \subset K$.

Math 504 **Homework 3** **Fall 2013**

(1) Let $F = \mathbb{F}_2(x)$ be the field of rational functions over the field of order 2. Show that the extension $K = F(\sqrt[6]{x})$ of F is equal to $F(\sqrt{x}, \sqrt[3]{x})$. Show that $F(\sqrt[3]{x})$ is separable over F. Show that $F(\sqrt{x})$ is purely inseparable over F, i.e., the minimal polynomial of every element in $F(\sqrt{x})$ has only one root.

(2) Find the degree of a splitting field over $\mathbb{Q}$ for the following polynomials: $x^4 - 1$, $x^4 + 1$, $x^4 + 2$, $x^4 + 4$.

(3) Find the degree of a splitting field for $x^6 + 1$ over $\mathbb{Q}$ and $\mathbb{F}_2$.

(4) Show that the extension of $\mathbb{Q}$ generated by a root of $x^4 - 2$ is not normal. Deduce that a normal extension of a normal extension need not be normal.

(5) If a field of characteristic p has n distinct n^{th} roots of unity show that p does not divide n.

(6) Let K be a field and G the group of all automorphisms of K. Show that the invariant subfield K^G is perfect.

(7) Let x be transcendental over a field k. Show that $k(x)$ is a degree-six extension of $k(x)^G$ where G is the group generated by the automorphisms $x \mapsto x^{-1}$ and $x \mapsto 1 - x$. Show that $(x^2 - x + 1)^3/(x^2 - x)^2$ is in $k(x)^G$ and use that to compute the minimal polynomial of x over $k(x)^G$.

(8) Show that $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt{2} + \sqrt[3]{2})$.

(9) Find the smallest normal extension of $\mathbb{Q}$ that contains $\sin\left(\frac{\pi}{5}\right)$.

(10) Give an algebraic proof that every angle can be bisected by using a ruler and compass.

Math 504 **Homework 4** **Fall 2013**

In the following questions p is a prime number and $\xi_p = e^{2\pi i/p} \in \mathbb{C}$.
If q is a power of a prime we write $\mathbb{F}_q$ for the field with q elements.

(1) Using only the fact that $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$, show that $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{p^n}$ whenever m divides n.

(2) Let $\xi = \xi_p$. Let $R = \{\xi^i \mid i \in \mathbb{Z}\}$. Show that R is a ring with the operations
$$\xi^i \oplus \xi^j = \xi^{i+j} \qquad \text{and} \qquad \xi^i \odot \xi^j = \xi^{ij}.$$
Show that $R \cong \mathbb{F}_p$.

(3) Let p be a prime number. Let $\xi_p = e^{2\pi i/p}$ and $K = \mathbb{Q}(\xi)$. Show there is a group homomorphism $\Phi : \mathrm{Gal}(K/\mathbb{Q}) \to (R^\times, \odot)$ and hence an isomorphism $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{F}_p^\times$. Deduce that $\mathrm{Gal}(K/\mathbb{Q})$ is the cyclic group of order $p-1$.

(4) Let p be an odd prime and $\xi_p = e^{2\pi i/p}$. Explain why there is a field F such that $\mathbb{Q} \subset F \subset \mathbb{Q}(\xi_p)$ and $[F : \mathbb{Q}] = 2$. Why is $F = \mathbb{Q}(\sqrt{d})$ for some d? Find d.

(5) Take $p = 17$ above. Find all fields F such that $\mathbb{Q} \subset F \subset \mathbb{Q}(\xi_p)$. Each intermediate field is of the form $\mathbb{Q}(\alpha)$ for some α. Can you find a nice α for each F?

(6) [Knapp, Ex. 29, p. 537] Let $K/\mathbb{Q}$ be the splitting field of an irreducible polynomial of degree 3 and suppose that $\mathrm{Gal}(K/\mathbb{Q})$ is the symmetric group S_3. Does K contain the three cube roots of 1? Explain.

(7) Show that $\mathbb{F}_{16} = \mathbb{F}_4(\alpha)$ where α is a primitive 5^{th} root of 1 over $\mathbb{F}_2$. It might be helpful to write $\mathbb{F}_4 = \mathbb{F}_2(\beta)$ where $\beta \in \mathbb{F}_4 - \mathbb{F}_2$.

(8) If $\mathbb{F}_{16} = \mathbb{F}_4(\alpha)$ where α is a primitive 5^{th} root of 1 over $\mathbb{F}_2$ is there an element $\sigma \in \mathrm{Gal}(\mathbb{F}_16/\mathbb{F}_4)$ such that $\sigma(\alpha) = \alpha^2$? What about $\sigma(\alpha) = \alpha^3$?

(9) A question to think about. Is there a generalization of question 2? If so what? Give some explanation.

(10) Which questions were the most/least interesting? Can you think of an interesting question I could have asked but did not? Feel free to consult any books that might have an interesting question.

Math 504 **Homework 5** **Fall 2013**

(1) Let G be a group and N a normal subgroup. Show that G is solvable if and only if N and G/N are solvable.
(2) Compute the Galois group of $x^6 - 2x^3 - 1$ over $\mathbb{Q}$.
(3) Solve the equation $x^6 - x^5 + x^4 - x^3 + x^2 - x + 1 = 0$ by radicals. Hint: Think about $t = x + x^{-1}$.
(4) Let k be a subfield of $\mathbb{C}$ and let $K = k(\alpha, \beta)$ where $\alpha^2 = a \in k$ and $\beta^2 = b \in k$ and none of a, b, or ab, is a square in k. Prove that $\mathrm{Gal}(K/k) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
(5) Let $f \in k[x]$ be an irreducible polynomial where k is a subfield of $\mathbb{C}$. Suppose f has at least one root that is expressible in radicals. Show that all roots of f can be written in terms of radicals.
(6) Give an example of an extension K/k such that $[K : k] = n$ and a positive integer d dividing n such that there is no intermediate field $k \subset L \subset K$ with $[L : k] = d$.
(7) Let K/k be a Galois extension of degree n with Galois group G. Define the norm and trace maps $N_{K/k} : K \to k$ and $T_{K/k} : K \to k$ by

$$N(a) = \prod_{\sigma \in G} \sigma(a) \qquad \text{and} \qquad T(a) = \sum_{\sigma \in G} \sigma(a).$$

Suppose that the minimal polynomial of $a \in K$ is $\sum_{i=0}^{r} c_i x^i \in k[x]$. Show that
(a) the norm and trace do take values in k, and
(b) $N(a) = (-1)^n c_0^{n/r}$ and $T(a) = -\frac{n}{r} c_{r-1}$, and
(c) $N(a) = \det(F)$ and $T(a) = \mathrm{Trace}(F)$ where $F : K \to K$ is the k-linear map $F(b) := ab$. (Hint: companion matrix of the minimal polynomial.)

Math 504 **Homework 6** **Fall 2013**

(1) Let p be a prime number and G a non-abelian group with p^3 elements.
   (a) Show that $Z(G) \cong \mathbb{Z}_p$ and that $G/Z(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p$.
   (b) Show that every subgroup of G having p^2 elements contains $Z(G)$ and is a normal subgroup of G.
   (c) Show that G has a normal subgroup isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$ if $x^p = 1$ for all $p \in G$.

(2) Knapp's book, Chapter IV, problems 42, 43, 44, on p.202. You can assume the results in questions 40 and 41.

(3) Knapp's book, Chapter IV, problems 50, 51, 53, 54 on p.203.