Algebraic Number Theory
MA844 (aka MA743)
Spring 2014
HW #1

Field theory: Let L/K be an extension of fields. That is, L and K are both fields and K is a subfield of L. (Note that the symbol "/" in this context has nothing to do with quotients!)

(1) Verify that L is a K-vector space.

Since L is a K-vector space, we can consider the dimension of L over K. When this dimension is finite we denote it by $[L : K]$, and we say L/K is a *finite extension* of degree $[L : K]$.

(2) Let α be in some algebraic extension of K and set $L = K(\alpha)$. That is, L is the smallest field which contains both K and α. Explicitly, elements of L are all of the form $f(\alpha)/g(\alpha)$ where $f(x), g(x)$ are polynomials in $K[x]$.

(a) Consider the homomorphism

$$K[x] \longrightarrow K(\alpha)$$
$$f(x) \mapsto f(\alpha).$$

Let I_α be the kernel of this map. Since $K[x]$ is a PID, we can write $I_\alpha = (\pi_\alpha(x))$ where $\pi_\alpha(x)$ is a monic polynomial.

Verify that $\pi_\alpha(x)$ is an irreducible polynomial. We call this polynomial the *minimum polynomial of* α *over* K.

(b) We thus have an induced injective map:

$$K[x]/(\pi_\alpha(x)) \longrightarrow K(\alpha).$$

Verify that this map is an isomorphism.

(c) Conclude that $\{1, \alpha, \alpha^2, \dots, \alpha^{d-1}\}$ where $d = \deg(\pi_\alpha(x))$ is a basis of $K(\alpha)$ over K, and thus $[K(\alpha) : K]$ is the degree of the minimum polynomial of α over K.

(3) Compute the degree of each of the following fields:

(a) $\mathbb{Q}(\sqrt{d})$ for d a squarefree integer

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

(c) $\mathbb{Q}(e^{2\pi i/p})$ for p a prime number

(4) For a finite extension L/K, and $\alpha \in L$, consider the multiplication by α map:

$$m_\alpha : L \longrightarrow L$$
$$x \mapsto \alpha \cdot x$$

This map is clearly K-linear (check it!), and thus we can take the determinant and trace of this map. Define

$$N_{L/K}(\alpha) := \det(m_\alpha),$$

the norm of α from L to K, and

$$\mathrm{Tr}_{L/K}(\alpha) := \mathrm{trace}(m_\alpha),$$

the trace of α from L to K.

(a) Compute $N_{\mathbb{Q}(i)/\mathbb{Q}}(a + bi)$ and $\mathrm{Tr}_{\mathbb{Q}(i)/\mathbb{Q}}(a + bi)$.

(b) Compute $N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(a + b\sqrt{d})$ and $\mathrm{Tr}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(a + b\sqrt{d})$.

(c) Verify that

- $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha) \cdot N_{L/K}(\beta)$
- $\mathrm{Tr}_{L/K}(\alpha\beta) = \mathrm{Tr}_{L/K}(\alpha) + \mathrm{Tr}_{L/K}(\beta)$
- if $r \in K$, then $\mathrm{Tr}_{L/K}(r\alpha) = r\,\mathrm{Tr}_{L/K}(\alpha)$
- if $\alpha \in K$, then $N_{L/K}(\alpha) = \alpha^{[L:K]}$ and $\mathrm{Tr}_{L/K}(\alpha) = [L : K] \cdot \alpha$.

(d) Is it true that there exists an element $\alpha \in L$ such that $N_{L/K}(\alpha) \neq 0$? How about $\mathrm{Tr}_{L/K}(\alpha) \neq 0$?

(5) Consider $\mathbb{Q}(\alpha)$ where α is some algebraic element over $\mathbb{Q}$. Let M denote some algebraically closed field containing $\mathbb{Q}$ (e.g. $\mathbb{C}$).
  (a) How many field embeddings of $\mathbb{Q}(\alpha) \to M$ are there?
  (b) Consider the field $L = \mathbb{Q}(\sqrt[3]{2})$. Write down all embeddings of L into $\mathbb{C}$.
  (c) If we no longer assume that we are working over $\mathbb{Q}$, but instead consider $K(\alpha)$ mappings to M an algebraically closed field containing K where K is any field, does the answer to (a) change?
  (d) Consider $K = \mathbb{F}_p(t)$ and set $L = \mathbb{F}_p(t)(t^{1/p})$. That is, $L = \mathbb{F}_p(t)[X]/(X^p - t)$. Write down all embeddings of L into an algebraically closed field containing K.

(6) Returning to norm and trace, now consider the case of $L = K(\alpha)$ and simply write $N(\alpha)$ for $N_{K(\alpha)/K}(\alpha)$ and $\mathrm{Tr}(\alpha)$ for $\mathrm{Tr}_{K(\alpha)/K}(\alpha)$. Consider again the multiplication by α map $m_\alpha : K(\alpha) \to K(\alpha)$.
  (a) Write down the matrix for this map in terms of the basis $\{1, \alpha, \ldots, \alpha^{d-1}\}$ where $d = [K(\alpha) : K]$.
  (b) Show that the characteristic polynomial of m_α equals the minimum polynomial of α over K. (Hint: Use the Cayley-Hamilton theorem)
  (c) Let $\overline{K}$ denote a fixed algebraic closure of K. Show that

$$N(\alpha) = \prod_{\sigma : K(\alpha) \to \overline{K}} \sigma(\alpha)$$

  and

$$\mathrm{Tr}(\alpha) = \sum_{\sigma : K(\alpha) \to \overline{K}} \sigma(\alpha).$$

  Here σ is ranging over all embeddings of $K(\alpha)$ into $\overline{K}$.
  (d) If α is integral over K, show that $N(\alpha)$ and $\mathrm{Tr}(\alpha)$ are in $\mathcal{O}_K$.

Commutative algebra Let R be a commutative ring (with identity because my rings always have an identity).

(7) We say an ideal $\mathfrak{p} \subseteq R$ is a *prime ideal* if $\mathfrak{p}$ is a proper ideal and whenever $ab \in \mathfrak{p}$, then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Prove that $\mathfrak{p}$ is a prime ideal iff $R/\mathfrak{p}$ is an integral domain.

(8) We say an ideal $\mathfrak{m} \subseteq R$ is a *maximal ideal* if $\mathfrak{m}$ is a proper ideal and is not contained in any other proper ideals. Prove that $\mathfrak{m}$ is a maximal ideal iff $R/\mathfrak{m}$ is a field.

(9) We say $z \in R$ is a *zero divisor* if there exists $w \neq 0$ such that $zw = 0$. Is it true that the sum and product of zero divisors is again a zero divisor?

(10) We say that $u \in R$ is a *unit* if there exists $v \in R$ such that $uv = 1$.
  (a) Is it true that the sum and product of zero divisors is again a zero divisor?
  (b) Find all units in $\mathbb{Z}$.
  (c) Find all units in $\mathbb{Q}[x]$.
  (d) Find all units in $\mathbb{Z}[i]$.
  (e) Find all units in $\mathbb{Q}$.
  (f) Find all units in $\mathbb{Q}[x]/(x^2)$.

(11) We say x in R is *irreducible* if x is not a zero divisors nor a unit and whenever $x = ab$ with $a, b \in R$ then either a or b is a unit.
  (a) Is -3 irreducible in $\mathbb{Z}$?
  (b) Is 7 irreducible in $\mathbb{Q}$?
  (c) Is $1 + i$ irreducible in $\mathbb{Z}[i]$?
  (d) Is $1 + 3i$ irreducible in $\mathbb{Z}[i]$?
  (e) Is $1 + \sqrt{5}$ irreducible $\mathbb{Z}[\sqrt{5}]$?
  (f) Is x irreducible in $\mathbb{Q}[x]/(x^2)$?

(12) We say π in R is a *prime element* if the principal ideal (π) is a prime ideal.
  (a) Prove that prime elements are irreducible.
  (b) Is $1 + i$ a prime element of $\mathbb{Z}[i]$?

(c) Is $1+3i$ a prime element of $\mathbb{Z}[i]$?
(d) Is $1+\sqrt{-5}$ a prime element of $\mathbb{Z}[\sqrt{-5}]$?

(13) We say that x and y in R are *associates* if $x = yu$ with u a unit of R.
(a) Are $1+i$ and $1-i$ associates in $\mathbb{Z}[i]$?
(b) Are $1+2i$ and $1-2i$ associates in $\mathbb{Z}[i]$?
(c) Are $5+\sqrt{2}$ and $5-\sqrt{2}$ associates in $\mathbb{Z}[i]$?
(d) Let a, b, c, d be prime elements of R. If $ab = cd$ prove that either a and c are associates or a and d are associates.

(14) We say a ring is a PID if every ideal is a principal ideal. Prove that irreducible elements in a PID are prime elements.

(15) Is the following a counter-example to unique factorization into irreducibles in $\mathbb{Z}[i]$?

$$(1+3i)\cdot(1-3i) = 2\cdot 5$$

Explain.

Algebraic integers

(16) Let d be a square-free integer. Let $K = \mathbb{Q}(\sqrt{d})$. Determine the ring of integers $\mathcal{O}_K$.

(17) Let $K = \mathbb{Q}(\sqrt[3]{2})$. Show that $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$.

(18) We saw or at least we will see that unique factorization domains are always integrally closed. Explain why $\mathbb{Z}[2i]$ is not integrally closed (directly from the definitions) and then give an explicit counter-example to unique factorization in this ring.

(19) Let $C/B/A$ be extensions of rings. If C/B is an integral extension and B/A is an integral extension, prove that C/A is an integral extension.

(20) Let A be a domain. Show that the integral closure of the integral closure of A is simply the integral closure of A.