Math 538: Problem Set 1

Do a good amount of problems; choose problems based on what you already know and what you need to practice. Examples are important.

Review

1. (Rings) All rings are commutative with identity unless specified otherwise (in particular, every subring contains the identity element). Let R be a ring and let $P \lhd R$ be a proper prime ideal.
   (a) Suppose that P is of finite index in R. Show that P is a maximal ideal.
   (b) Suppose that S is a subring of R. Show that $P \cap S$ is a proper prime ideal of S.

2. (Field and Galois Theory) Let L/K be a finite separable extension of fields, and let $\alpha \in L$. Let M_α be the map of multiplication by α, thought of as a K-linear endomorphism of L.
   (a) Show that M_α is diagonalizable, and that its spectrum over a fixed algebraic closure $\bar{K}$ of K consists of the numbers $\{\iota(\alpha)\}_{\iota \in \mathrm{Hom}_K(L,\bar{K})}$.
   (b) Show that $\mathrm{Tr}^L_K\, \alpha = \mathrm{Tr}\, M_\alpha$, $N^L_K \alpha = \det M_\alpha$.

Quadratic fields

3. (The Gaussian Integers)
   (a) Show that $\mathbb{Z}[i]$ is a Euclidean domain, hence a UFD (hint: show that rounding the real and complex parts of $\frac{z}{w}$ gives a number $q \in \mathbb{Z}[i]$ so that $|z - qw| < |w|$)
   (b) Show that $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.
   (c) Let p be a rational prime and consider the ring $\mathbb{Z}[i]/p\mathbb{Z}[i]$ (verify that it has order p^2). Verify that the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}[i]$ induces an embedding $\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{Z}[i]/p\mathbb{Z}[i]$, and hence a homomorphism $\mathbb{F}_p[x]/(x^2+1) \to \mathbb{Z}[i]/p\mathbb{Z}[i]$ where x maps to $i + p\mathbb{Z}[i]$.
   (d) Show that this map is an isomorphism. Check that $\mathbb{F}_p[x]/(x^2+1)$ is a field iff $p \equiv 3\,(4)$ and obtain a different proof that a rational prime is inert in $\mathbb{Q}(i)$ iff it is 3 mod 4.

4. (The Eisenstein Integers) Let $\omega = \frac{-1+\sqrt{-3}}{2}$ be a primitive cube root of unity, $K = \mathbb{Q}(\omega)$,
   (a) Show that $\mathbb{Z}[\omega]$ is the set of algebraic integers in K.
   (b) Check that $N^K_{\mathbb{Q}}(a + b\omega) = a^2 - ab + b^2$.
   (c) Realizing $\mathbb{Z}[\omega]$ as a lattice in $\mathbb{C}$ let $\mathcal{F} = \{z \in \mathbb{C} \mid \forall \alpha \in \mathbb{Z}[\omega] : |z| \leq |z - \alpha|\}$ be the set of complex numbers closer to zero than to any other element of the lattice. Verify that:
      (i) $\mathcal{F}$ is closed, and is a polygon hence equal to the closure of its interior.
      (ii) $\mathbb{C} = \bigcup_{\alpha \in \mathbb{Z}[\omega]} \mathcal{F} + \alpha$.
      (iii) For any non-zero $\alpha \in \mathbb{Z}[\omega]$, $\mathcal{F} \cap (\mathcal{F} + \alpha) \subset \partial \mathcal{F}$ (hint: if z is in the intersection it is equally close to $0, \alpha$)..
   (d) Show that for any $z \in \mathcal{F}$, $|z| = \sqrt{Nz} < 1$. Conclude that $\mathbb{Z}[\omega]$ is a Euclidean domain, hence a UFD.
   (d) Show that $\mathbb{Z}[\omega]^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$.
   (e) Classify the primes of $\mathbb{Z}[\omega]$ following the argument for the Gaussian integers. To check which rational primes remain prime in this ring use both the argument from class (using congruence conditions to rule out $p = a^2 - ab + b^2$ in one case, and the cube root of unity mod p to show that p does factor in the other) and the argument from 3(d),(e) (examine the ring $\mathbb{Z}[\omega]/p\mathbb{Z}[\omega]$ to see if it is a field).

The following exercize is of central importance.

5. Let $K/\mathbb{Q}$ be a quadratic extension.
   (a) Verify for yourself that $K = \mathbb{Q}\left(\sqrt{d}\right)$ for a unique square-free integer $d \neq 1$. Fix such d from now on.
   (b) Show that $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d} \subset K$ is a subring generated by a $\mathbb{Q}$-basis of K (an "order"), and that all its elements are algebraic integers.
   (c) Let $a, b \in \mathbb{Q}$. Show that $a + b\sqrt{d}$ is an algebraic integer iff $2a, a^2 - db^2 \in \mathbb{Z}$, and that this forces $2b \in \mathbb{Z}$.
   (d) Show that $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$ unless $d \equiv 1\,(4)$, in which case $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{d}}{2} = \left\{ \frac{a+b\sqrt{d}}{2} \mid a, b \in \mathbb{Z}, a \equiv b\,(2)$
   (e) Show that if $d < -3$, $\mathcal{O}_K$ has no units except for ± 1.
   (f) Let p be an odd rational prime not dividing d. Find a representation of $\mathcal{O}_K/p\mathcal{O}_K$a-la 3(d) and conclude that $p\mathcal{O}_K$ is a prime ideal iff d is a square mod p. Now apply quadratic reciprocity to get a criterion for the splitting or primes.

   RMK In fact, it is possible to prove the law of quadratic reciprocity this way.

The following exercize is less important.

6. (The "other" quadratic extension) Let A detnote the ring $\mathbb{Q} \oplus \mathbb{Q}$, with pointwise addition and multiplication (this is the case $d = 1$ of problem 3).
   (a) Find a zero-divisor in A – it is not a field.
   (b) Show that the subring $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}$ is precisely the set of $x \in A$ which are integral over $\mathbb{Z}$. (Hint: find the minimal polynomial of $(a, b) \in A$).
   (c) Let $P \lhd \mathcal{O}$ be a prime ideal of finite index. Show that P is of the form $p\mathbb{Z} \oplus \mathbb{Z}$ or $\mathbb{Z} \oplus p\mathbb{Z}$ for a rational prime p (hint: consider the idempotents in $\mathcal{O}$).
   (d) Show that $\mathcal{O}$ has non-zero prime ideals of infinite index. In fact, find proper prime ideals P, Q such that $(0) \subsetneq P \subsetneq Q \subsetneq A$.

Number fields

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

Let $\mathbb{Q} \subset K \subset L$ be a number fields with rings of integers $\mathcal{O}_K, \mathcal{O}_L$ respectively.

8. (Units)
   (a) Let $\alpha \in \mathcal{O}_L$. Show that $\mathrm{Tr}^L_K \alpha, N^L_K \alpha \in \mathcal{O}_K$.
   (b) Show that $\varepsilon \in \mathcal{O}_L$ is a unit iff $N^L_K \alpha$ is a unit of $\mathcal{O}_K$.

9. (Ideals)
   (a) Let $\alpha \in \mathcal{O}_L$. Show that $N^L_K \alpha \in \alpha\mathcal{O}_L$.
   (b) Conclude that any non-zero ideal $\mathfrak{a} \lhd \mathcal{O}_L$ contains an ideal of the form $m\mathcal{O}_L$, $m \in \mathbb{Z} \setminus \{0\}$.
   (c) Show that every non-zero ideal of $\mathcal{O}_L$ is a free Abelian group of rank $n = [L : \mathbb{Q}]$.

Generalization: Orders in $\mathbb{Q}$-algebras

DEFINITION. Let R be a commutative ring. An (associative, unital) *R-algebra* is a (possibly non-commutative) unital ring A equipped with a ring homomorphism $f\colon R \to A$ whose image is central. Equivalently, A is an R-module equipped with an associative, unital product which is R-bilinear.

DEFINITION. Let A be a $\mathbb{Q}$-algebra. A subring $\mathcal{O} \subset A$ is an *order* of A if it is the free $\mathbb{Z}$-module generated by a $\mathbb{Q}$-basis of A.

10. Fix a finite-dimensional $\mathbb{Q}$-algebra A.
   (a) Show that A contains orders.
   (b) Let $\mathcal{O} \subset A$ be an order. Show that every $x \in \mathcal{O}$ is integral over $\mathbb{Z}$.
   (c) Suppose that A is commutative. Show that A has a unique maximal order.

11. Define the *trace* of $x \in A$ as the trace of left multiplication by x. Given $\{x_i\}_{i=1}^n \subset A$ let $D(x_1,\ldots,x_n) \in M_n(\mathbb{Q})$ be the matrix with i,j entry $\mathrm{Tr}(x_ix_j)$, $\Delta(x_1,\ldots,x_n) = \det D(x_1,\ldots,x_n)$.
   (a) Let $\mathcal{O} \subset A$ be an order. Show that $\mathrm{Tr}\,x \in \mathbb{Z}$ for all $x \in \mathcal{O}$.
   (b) Let $\{\omega_i\}_{i=1}^n \subset A$ be a $\mathbb{Q}$-basis. Show that for any $\{x_i\}_{i=1}^n \subset A$, $\Delta(x_1,\ldots,x_n) = (\det\alpha)^2\Delta(\omega_1,\ldots,\omega_n)$ where $\alpha \in M_n(\mathbb{Q})$ is the matrix such that $x_i = \sum_{k=1}^n \alpha_{ik}\omega_k$.
   COR Either $D = 0$ for all n-tuples (we say that the trace form is *degenerate*) or $D \neq 0$ for all bases (we say that the trace form is *non-degenerate*). We assume the second case from now on.
   (c) Let $\mathcal{O}$be an order with $\mathbb{Z}$-basis $\{\omega_i\}_{i=1}^n$. Show that the number $\Delta(\omega_1,\ldots,\omega_n)$ is a rational integer, independent of the choice of basis. Denote this $\Delta(\mathcal{O})$.
   (d) Suppose that $\mathcal{O} \subset \mathcal{O}'$ are two orders. Show that $\Delta(\mathcal{O}) = [\mathcal{O}' : \mathcal{O}]^2\Delta(\mathcal{O}')$.
   COR In a non-degenerate $\mathbb{Q}$-algebra every order is contained in a maximal order.
   (e) Construct a degenerate $\mathbb{Q}$-algebra without maximal orders.

REMARK. Note that this gives a a procedure for finding maximal orders in finite-dimensional $\mathbb{Q}$-algebras: find a $\mathbb{Q}$-basis containing 1_A. Scaling its elements gives an order $\mathcal{O}$, say of discriminant $\Delta(\mathcal{O})$. Let $\mathcal{O}'$ be order containing $\mathcal{O}$. Then $d = [\mathcal{O}' : \mathcal{O}] \leq \sqrt{\Delta(\mathcal{O})}$. It follows that $d\mathcal{O}' \subset \mathcal{O}$ so $\mathcal{O} \subset \mathcal{O}' \subset \frac{1}{d}\mathcal{O}$. Now $\mathcal{O}/d\mathcal{O} \simeq (\mathbb{Z}/d\mathbb{Z})^n$ where $n = \dim_{\mathbb{Q}} A$. It follows that the set of $\mathbb{Z}$-submodules of $\frac{1}{d}\mathcal{O}$ containing $\mathcal{O}$ is finite; it remains to check those one-by-one to see if any are orders.

12. Now suppose that A is an F-algebra where F is a number field. Let $\mathcal{O} \subset A$ be an order. Show that the $\mathcal{O}_F$-submodule of A generated by $\mathcal{O}$ is an order as well.
   COR Every maximal order of A is an $\mathcal{O}_F$-module.
   RMK In fact, every order of A which is an $\mathcal{O}_F$-module is a *free* $\mathcal{O}_F$-module. We may discuss this later.