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.

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 diagonable, 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 $\mathrm{Tr}_K^L \alpha = \mathrm{Tr}\, M_\alpha$, $N_K^L \alpha = \det M_\alpha$.

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 $a, b, c \in \mathbb{Z}$ be pairwise relatively prime and satisfy $a^2 + b^2 = c^2$. Show that $a + bi \in \mathbb{Z}[i]$ is of the form εz^2 for $z \in \mathbb{Z}[i]$, $\varepsilon \in \mathbb{Z}[i]^\times$ and obtain the classification of Pythagorean triples.
   (d) 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 $i + p\mathbb{Z}[i]$.
   (e) Show that this map is an isomorphism. Show 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 $N_{\mathbb{Q}}^K(a + b\omega) = a^2 - ab + b^2$.
   (c) Realizing $\mathbb{Z}[\omega]$ as a lattice in $\mathbb{C}$ let $\mathcal{F} = \{z \in \mathbb{C} \mid \forall \alpha \in \mathbb{Z}[\omega] : |z| \le |z - \alpha|\}$ 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.
   (e) Show that $\mathbb{Z}[\omega]^\times = \left\{\pm 1, \pm\omega, \pm\omega^2\right\}$.
   (continued)

(f) 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 exercise is of central importance.

5. Let $K/\mathbb{Q}$ be a quadratic extension.
   (a) Show that $K = \mathbb{Q}\left(\sqrt{d}\right)$ for a unique square-free integer $d \neq 1$.
   (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 $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{d}}{2} = \left\{ \frac{a+b\sqrt{d}}{2} \mid a, b \in \mathbb{Z},\, a \equiv b\,(2)\right.$
   (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(e) and conclude that $p\mathcal{O}_K$ is a prime ideal iff d is not 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 starting from this observation.

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 5).
   (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 $(0) \subsetneq P \subsetneq Q \subsetneq A$.

Cubic example

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