Problem Set 2.

1. Let K be a number field and $\mathcal{O}$ an order in K. Show that $\mathcal{O}$ is a unique factorization domain (UFD) if and only if it is a principal ideal domain (PID) by carrying out the following steps:
   a) Show that if R is a PID, then each irreducible element $\pi \in R$ generates a prime ideal.
   b) Show that if R is a UFD in which every nonzero prime ideal is a maximal ideal then all prime ideals are principal ideals.
   c) Show that if R is a UFD in which all prime ideals are principal that given $a, b \in R$ with only units as common factors, then there exist $m, n \in R$ such that $ma+nb = 1$.
   d) Use c) to show that an order in a number field which is a UFD must be a PID.
2. In class we showed that Galois group of the n–th cyclotomic field $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ is isomorphic to $(\mathbf{Z}/n\mathbf{Z})^*$, the group of units in the ring of integers modulo n and that the Frobenius element for primes p not dividing n is represented by the element $p \in (\mathbf{Z}/n\mathbf{Z})^*$. Use this for $n = 4$ to show that the Frobenius element at an odd prime p in the Gaussian field $\mathbf{Q}(\sqrt{-1})$ is trivial if and only if $p \equiv 1 \pmod 4$ and that this is the condition for -1 to be a square modulo such a prime.
3. Show that the number field $\mathbf{Q}(\sqrt{2})$ is the maximal real subfield of $\mathbf{Q}(\zeta_8)$ and show that the Frobenius element $Frob_p$ for an odd prime p restricts to the Frobenius element for the field $\mathbf{Q}(\sqrt{2})$. Show that whether 2 is a square modulo an odd prime p depends only on p modulo 8 by computing the Frobenius element at p for the quadratic field. Describe the set of odd primes p for which the Frobenius element is trivial, that is 2 is a square modulo p.
4. Show that the real subfield K of $\mathbf{Q}(\zeta_7))$ is obtained by adjoining a root α of $f(x) = x^3 + x^2 - 2x - 1$ (corrected the constant term to -1 on 9/17/19) to the rational field. Determine the Galois group of $K/\mathbf{Q}$ and Frobenius elements for primes $p \neq 7$. Use the order $\mathbf{Z}[\alpha] \subset K$ to determine the degrees of irreducible factors of $f(x)$ modulo p for all sufficiently large p.
5. Let K be the splitting field of $g(x) = x^3 - x - 1$. Show that $Gal(K/Q)$ contains elements of order 2 and 3 by reducing $g(x)$ modulo the first few primes. Show that K contains a unique quadratic subfield and determine the Frobenius elements for this subfield. Show that there is a congruence condition on primes p that determines when the Frobenius element at p has order 2.