Solve whichever problems you haven't seen before that interest you the most (suggestion: between 20 and 40 points' worth). Starred problems are especially recommended. Prepare to present 1-2 problems in class on the due date.

0.1 In-Lecture Exercises

0.1.1 Exercises from (Sep 19)

1. [2pts] Show that $x^n - 1 = \prod_{d|n} \Phi_d(x)$. [Hint: Group together the roots of unity of each order $d|n$.]
2. [2pts] Show that $\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(n/d)}$ where $\mu(n) = \begin{cases} 0 & \text{if } n \text{ is not squarefree} \\ (-1)^k & \text{if } n = p_1 \cdots p_k \text{ for distinct primes } p_i \end{cases}$ denotes the Möbius μ-function. Use this recurrence relation to calculate $\Phi_6(x)$ and $\Phi_{20}(x)$.
3. [1pt] For a prime p, show directly that $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible. [Hint: Use Eisenstein's criterion on $\Phi_p(x+1) = \frac{1}{x}[(x+1)^p - 1]$.]
4. [1pt] For any prime power p^d, show that $\Phi_{p^d}(x) = \Phi_p(x^{p^{d-1}})$. [Hint: Show both sides equal $\prod_{i=1}^{p-1}(x^{p^{d-1}} - \zeta_p^i)$.]
5. [3pts*] Let p be an odd prime. Show that $\mathbb{Q}(\zeta_p)$ contains a unique quadratic subfield and that it is $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$. [Hint: Use Galois theory for uniqueness, and discriminants to get the field itself.]
6. [3pts] Show that every quadratic field is a subfield of some cyclotomic field $\mathbb{Q}(\zeta_n)$. [Hint: Take a composite of $\mathbb{Q}(\zeta_8)$ and the $\mathbb{Q}(\zeta_p)$ for various p.]

   Remark: This problem is a special case of the Kronecker-Weber theorem: every number field K with abelian Galois group over $\mathbb{Q}$ is a subfield of some cyclotomic field.

0.1.2 Exercises from (Sep 25)

1. [1pt] For a prime p, show that $p = u(1 - \zeta_{p^d})^{\varphi(p^d)}$ where u is a unit in $\mathbb{Z}[\zeta_{p^d}]$.
2. [2pts] If D and E are relatively prime squarefree integers congruent to 1 modulo 4, show that the ring of integers of $\mathbb{Q}(\sqrt{D}, \sqrt{E})$ is $\mathbb{Z}[\frac{1+\sqrt{D}}{2}, \frac{1+\sqrt{E}}{2}]$, and compute an integral basis for it.
3. [3pts*] If $-D < -4$ is squarefree and $-D \equiv 2, 3 \pmod 4$, show that $\mathcal{O}_{\sqrt{-D}} = \mathbb{Z}[\sqrt{-D}]$ is not a unique factorization domain. [Hint: If D is odd, use $2 \cdot (1+D)/2 = (1+\sqrt{-D})(1-\sqrt{-D})$, and if D is even use $2 \cdot (D/2) = \sqrt{-D} \cdot (-\sqrt{-D})$.]

0.1.3 Exercises from (Sep 26)

1. [2pts] If R is an integral domain, show that the following conditions for R to be Noetherian are equivalent:
   (a) Every ideal of R is finitely generated.
   (b) Every ascending chain $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ of ideals of R is eventually constant (i.e., there exists N such that $I_n = I_N$ for all $n \geq N$).
   (c) Every nonempty collection S of ideals of R contains a maximal element (i.e., an ideal I such that if $J \in S$ has $I \subseteq J$ then $J = I$).
2. [1pt] Show that a finite integral domain is a field.

3. [3pts] Suppose S is an integral ring extension of the commutative ring R with 1 (i.e., every element of S is the root of a monic polynomial in $R[x]$).

   (a) Show that if Q is a prime ideal of S, then $P = Q \cap R$ is a prime ideal of R.

   (b) Show that if S is a domain then R is a field if and only if S is a field. [Hint: Use the monic polynomial satisfied by a nonzero element to construct an inverse for it.]

   (c) Show that an ideal Q of S is maximal in S if and only if $P = Q \cap R$ is maximal in R. [Hint: Note S/Q is an integral extension of R/P.]

4. [2pts] Suppose that R is a commutative ring with 1 and S is a ring containing R. Recall that the integral closure of R in S consists of the elements of S containing R, and R is integrally closed when its integral closure is just R itself.

   (a) Show that the integral closure of R in S is a subring of S containing R. [Hint: If s, t are integral over R, then $R[s]$ and $R[t]$ are finitely-generated R-modules, hence so is $R[s,t]$.]

   (b) Show that the integral closure of R in S is integrally closed in S. [Hint: Show that integrality is transitive.]

5. [1pt] Show that principal ideal domains are Dedekind domains. [Hint: Use the general fact that UFDs are integrally closed.]

0.1.4 Exercises from (Sep 30)

1. [1pt] If R is a Noetherian integral domain, show that fractional ideals of R are the same as finitely-generated R-submodules of K. [Hint: Put things over a common denominator.]

2. [1pt] Suppose P is a prime ideal of an integral domain and $IJ \subseteq P$ for some ideals I and J. Show that $I \subseteq P$ or $J \subseteq P$. (Note that this property is the ideal analogue of the prime divisibility property $p|ab$ implies $p|a$ or $p|b$.)

0.1.5 Exercises from (Oct 2)

1. [1pt] If I is a nonzero ideal of a Dedekind domain R, show that I can be written uniquely in the form $I = \prod_{P_i \text{ prime}} P_i^{a_i}$ where the product is taken over all prime ideals of R and the a_i are nonnegative integers only finitely many of which are positive.

2. [1pt] Show that the group of fractional ideals in a Dedekind domain is a free abelian group generated by the nonzero prime ideals.

3. [1pt] If A is any ideal in a Dedekind domain R, show that there are only finitely many ideals of R that contain A.

4. [1pt] For any ideals A and B in a Dedekind domain, show that $AB = (A+B)(A \cap B)$.

5. [2pts*] If I and J are ideals in a commutative ring with 1, show that $IJ \subseteq I \cap J$, and also that if $I + J = R$ then $IJ = I \cap J$.

0.1.6 Exercises from (Oct 3)

1. [2pts] Let R be an integral domain and let M be a maximal ideal of R. For any $d \geq 0$, show that M^d/M^{d+1} is an R/M-vector space.

2. [4pts*] Show that the prime ideals of $\mathbb{Z}[\sqrt{-2}]$ are as follows: the ideal $(\sqrt{-2})$, the ideals (p) where p is a prime congruent to 5 or 7 modulo 8, and the two ideals $(a + b\sqrt{-2})$ and $(a - b\sqrt{-2})$ where $a^2 + 2b^2 = p$ is a prime congruent to 1 or 3 mod 4.

0.2 Additional Exercises

1. [4pts] The famously unsolved inverse Galois problem asks whether every finite group G occurs as a Galois group over $\mathbb{Q}$. The goal of this problem is to show every finite *abelian* group is a Galois group over $\mathbb{Q}$.

   (a) For any $d \geq 2$, show that there exists a number field K, Galois over $\mathbb{Q}$, with Galois group $\mathbb{Z}/d\mathbb{Z}$. You may assume Dirichlet's theorem on primes in arithmetic progressions. [Hint: Choose any prime $p \equiv 1 \pmod{d}$ via Dirichlet's theorem and take an appropriate subfield of $\mathbb{Q}(\zeta_p)$.]

   (b) Let G be a finite abelian group. Prove that there exists a number field K, Galois over $\mathbb{Q}$, such that $\mathrm{Gal}(K/\mathbb{Q}) \cong G$. [Hint: Take a composite of fields as in (a).]

2. [10pts*] Let $n > 2$ and define $\theta = 2\cos(2\pi/n) = \zeta_n + \zeta_n^{-1}$.

   (a) Show that $\mathbb{Q}(\zeta_n)$ is a degree-2 extension of $\mathbb{Q}(\theta)$. Deduce that the extension $\mathbb{Q}(\theta)/\mathbb{Q}$ has degree $\varphi(n)/2$.

   (b) Show that the extension $\mathbb{Q}(\theta)/\mathbb{Q}$ is Galois and that its Galois group is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times/\{\pm 1\}$. [Hint: Show $\mathbb{Q}(\theta)$ is the fixed field of complex conjugation.]

   (c) Show that the Galois conjugates of θ are the numbers $2\cos(2\pi k/n)$ for $k \in \mathbb{Z}$. Deduce that $\mathbb{Q}(\theta)$ is a <u>totally real field</u>: every complex embedding of $\mathbb{Q}(\theta)$ lies inside $\mathbb{R}$.

   (d) For $k = \varphi(n)/2$, show that $\{1, \zeta_n, \theta, \theta\zeta_n, \theta^2, \theta^2\zeta_n, \ldots, \theta^{k-1}, \theta^{k-1}\zeta_n\}$ is an integral basis for $\mathbb{Z}[\zeta_n]$.

   (e) For $k = \varphi(n)/2$, show that $\{1, \theta, \theta^2, \ldots, \theta^{k-1}\}$ is an integral basis for $\mathcal{O}_{\mathbb{Q}(\theta)}$. Deduce that $\mathcal{O}_{\mathbb{Q}(\theta)} = \mathbb{Z}[\theta]$. [Hint: First explain why $\mathcal{O}_{\mathbb{Q}(\theta)} = \mathbb{R} \cap \mathbb{Z}[\zeta_n]$, and then use the basis for $\mathbb{Z}[\zeta_n]$ from (d).]

   (f) If $n = p$ is an odd prime, show that $\mathrm{disc}(\theta) = p^{(p-3)/2}$. [Hint: Compute $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\theta)$ directly, and then note $[N_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta)]^2 = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\theta)$. Finally note that $\sqrt{\mathrm{disc}(\theta)} \in \mathbb{Q}(\theta)$.]

3. [10pts*] The goal of this problem is to determine which imaginary quadratic integer rings $\mathcal{O}_{\sqrt{-D}}$ are Euclidean.

   (a) Show that $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\sqrt{2}]$, and $\mathbb{Z}[\sqrt{3}]$ are Euclidean with norm function $|N(a + b\sqrt{D})| = |a^2 - Db^2|$.

   (b) Suppose that $-D \equiv 1 \pmod{4}$. Prove that any $z \in \mathbb{C}$ differs from an element in $\mathcal{O}_{\sqrt{-D}}$ by a complex number whose norm is at most $(1+D)^2/(16D)$. [Hint: The elements of $\mathcal{O}_{\sqrt{-D}}$ form a lattice in $\mathbb{C}$. Use symmetry to reduce the distance calculation to one inside a triangle, and then show the largest distance occurs at the circumcenter.]

   (c) Show that $\mathcal{O}_{\sqrt{-D}}$ is a Euclidean domain for $-D = -3$, -7, and -11.

   From (a), (c), and exercise 0.1.2.3 above, the only remaining cases are for $-D \equiv 1 \pmod{4}$ and $-D \leq -15$. If R is an integral domain, we say an element $u \in R$ is a <u>universal side divisor</u> if it is not zero, not a unit, and every $x \in R$ can be written in the form $x = qu + z$ where z is either zero or a unit. Equivalently, u is a universal side divisor when every nonzero residue class modulo u is represented by a unit of R.

   (d) Suppose R is a Euclidean domain that is not a field. If u is a nonzero nonunit of R of minimal norm among nonzero nonunits in R (with respect to the norm function on R), show u is a universal side divisor.

   (e) Suppose $D < -3$. If u is a universal side divisor in $\mathcal{O}_{\sqrt{-D}}$, show that u must divide one of $x-1$, x, $x+1$ for any $x \in \mathcal{O}_{\sqrt{-D}}$.

   (f) Suppose $D < -11$. Show $\mathcal{O}_{\sqrt{-D}}$ has no universal side divisors and conclude that $\mathcal{O}_{\sqrt{-D}}$ is not Euclidean. [Hint: Apply (e) when $x = 2$ and $x = (1 + \sqrt{-D})/2$.]

   Remark: Here we see that the Euclidean imaginary quadratic rings are also norm-Euclidean (meaning that they are Euclidean with respect to the norm function). There do exist rings of integers that are Euclidean but not norm-Euclidean, and there also exist rings of integers that are not Euclidean but are k-stage Euclidean (meaning that the remainder bound holds but only after k stages of division).