HOMEWORK 1

Do at least 5 questions. Due September 30 at 11:59pm.

1. Let $d \in \mathbb{Z}$ be square free and $\neq 0, 1$. Show that the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[\sqrt{d}]$ if $d \not\equiv 1 \pmod 4$ and is $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if $d \equiv 1 \pmod 4$.

2. Let $A \subseteq B$ be integral domains with B integral over A. Prove that B is a field if and only if A is a field.

3. Let $n \geq 2$ and let ζ, ζ' be primitive nth roots of unity in some field extension of $\mathbb{Q}$.
(a) Show that $\frac{1-\zeta'}{1-\zeta}$ is an algebraic integer.
(b) Show that if n has at least two prime factors, then $1 - \zeta$ is a unit in $\mathbb{Z}[\zeta]$.

4. Let A be a UFD with fraction field F and let E/F be an extension of fields. Let $x \in E$ be algebraic over F with minimal polynomial $f \in F[t]$. Prove that x is integral over A if and only if $f \in A[t]$.

5. It can be shown that the ring of integers of $\mathbb{Q}(\sqrt[3]{2})$ is $\mathbb{Z}[\sqrt[3]{2}]$. Compute the discriminant of $\mathbb{Z}[\sqrt[3]{2}]$.

6. Let F be a number field of degree n over $\mathbb{Q}$ such that $\mathcal{O}_F = \mathbb{Z}[\alpha]$ for some $\alpha \in F$. (The basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is usually referred to as a *power basis* for F. Power bases don't always exist.) Let f be the minimal polynomial of α over $\mathbb{Q}$, and let $\alpha = \alpha_1, \ldots, \alpha_n$ be the roots of f. Show that the discriminant of F equals the discriminant of f, i.e.

$$d_F = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

7. Let $F(\alpha)/F$ be a finite separable extension of degree n generated by α, let $f \in F[t]$ be the minimal polynomial of α over F, and let f' be its derivative. Show that

$$d(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \operatorname{Nm}_{F(\alpha)/F}(f'(\alpha)).$$

8. Let A be a normal Noetherian domain with fraction field F. Let E/F be a finite separable extension and let B be the integral closure of A in E.
(a) Let $M \subset E$ be a finitely generated nonzero B-submodule of E. Prove that

$$M^* := \{x \in F : \operatorname{Tr}_{E/F}(xM) \subseteq A\}$$

is a also finitely generated B-submodule of E.
(b) Consider the case of $A = \mathbb{Z}$ and $M = \mathcal{O}_E$ the ring of integers in a number field E. Show that $\mathfrak{D}_{E/\mathbb{Q}} := \{x \in E : x\mathcal{O}_E^* \subseteq \mathcal{O}_E\}$ is an ideal in $\mathcal{O}_E$. This is called the *different* of the extension $E/\mathbb{Q}$.

9. Let $E/\mathbb{Q}$ be a quadratic extension. We use the notation and definitions of Question **8.**
(a) Compute $\mathcal{O}_E^*$.
(b) Compute the different $\mathfrak{D}_{E/\mathbb{Q}}$ of the extension $E/\mathbb{Q}$.

(c) Compute the ideal in $\mathbb{Z}$ generated by $\{\mathrm{Nm}_{E/\mathbb{Q}}(x) : x \in \mathfrak{D}_{E/\mathbb{Q}}\}$. Where have you seen this before?

10. Let $d \neq 0, 1$ be a squarefree integer, let $F = \mathbb{Q}(\sqrt{d})$, and let p be a prime number such that $p \nmid 2d$. Prove that $p\mathcal{O}_F$ is a prime ideal in $\mathcal{O}_F$ if and only if $x^2 \equiv d \pmod{p}$ has no solutions in $x \in \mathbb{Z}$. (Hint: Note that $\mathcal{O}_F/p\mathcal{O}_F$ is 2-dimensional over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.)

11. Prove that a Dedekind domain with only finitely many prime ideals is a principal ideal domain.

12. Let A be a Dedekind doamin.
  (a) Let $J \subseteq I$ be nonzero ideals in A. Prove there is $a \in I$ such that $I = J + (a)$.
  (b) Prove that any ideal in A can be generated by at most two elements.

13. Prove that a Dedekind domain is a UFD if and only if it is a PID.

14. Let A be a Dedekind domain.
  (a) Prove that for any ideals $J \subseteq I$ of A, there is an ideal H of A such that $J = IH$.
  (b) Prove that for any nonzero ideal I of A, there is a nonzero ideal H of A such that IH is principal.

15. Let I be an ideal of a Dedekind domain A. Prove that I is a direct summand of A^2 as an A-module. (Hint: Question **12.** above shows there is a surjection $f : A^2 \to I$. To show that I is a direct summand of A^2, it suffices to show there is an A-module map $s : I \to A^2$ such that $f \circ s = \mathrm{id}$. Question **14.** is useful for constructing s.)

16. Let A be a Dedekind domain and let S be a finite set of nonzero prime ideals of A. Prove that any element of $\mathrm{Cl}(A)$ can be represented by an ideal of A that is not divisible by any element in S.