Math 418: Takehome 1 due Wednesday, February 16, 2022.

Disclaimer, Terms, and Conditions: You may not discuss the exam with anyone except myself. You may *only* consult the following:

- The beloved(?) text, Dummit and Foote's *Abstract Algebra*.
- Your class notes and returned HW sets.
- My online class notes and HW solutions.

You can use any result in Chapters 7–12 and Sections 13.1–13.2 of Dummit and Foote, even if I didn't cover it in class. You can also use the result of any HW problem that was assigned, whether or not you did it.

Office hours: While discussion of these specific problems will be limited to clarifying their statements, I will be happy to answer any broader questions about the course material during my usual office hours (Monday and Tuesday from 1:30–2:30pm), extra office hour (Friday Feb 11, 10:00am), or by appointment.

1. Let F be a field. Consider the ring $R = F[[t]]$ of *formal power series* in t, namely things of the form

$$\sum_{n=0}^{\infty} a_n = a_0 + a_1 t + a_2 t^2 + \cdots \quad \text{where } a_n \in F.$$

Here "formal" means the above "sum" is really just an infinite list of elements of F; there's no notion of convergence involved. Elements of R are added term by term, and multiplication is as if they were polynomials. More precisely

$$\sum_{n=0}^{\infty} a_n t^n \times \sum_{n=0}^{\infty} b_n t^n = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) t^n$$

It is clear that R is a commutative ring with 1. It is different from the field of formal Laurent series $F((t))$ where a finite number of negative exponents of t are allowed.

(a) The units of R are precisely the α where the constant term $a_0 \neq 0$. For example, with $F = \mathbb{Q}$, the inverse of $1 - t$ is $1 + t + t^2 + t^3 + t^4 + \cdots$.

For the field $F = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, find the multiplicative inverse of $1 + t + t^2$.

(b) Prove that R is a Euclidean domain with respect to the norm $N(\alpha) = n$ if a_n is the first term of α that is non-zero. (If $F = \mathbb{C}$ and the power series converges near $t = 0$, then this norm is just the order of zero of the corresponding function at 0.)

(c) In the polynomial ring $R[x]$, prove that $x^n - t$ is irreducible.

2. Let $R = \mathbb{Z}[i]$.

   (a) Let $\pi \in R$ be irreducible. Consider the ideals $I_n = (\pi^n)$. Prove that $R/(\pi) \cong I_n/I_{n+1}$ as additive abelian groups. Hint: the isomorphism is multiplication by π^n.

   (b) Again for irreducible π, prove that $|R/(\pi^n)| = |R/(\pi)|^n$. Here $|\cdot|$ denotes the number of elements in a finite set. (This is a key step in proving that for *any* $\pi \in R$ that $|R/(\pi)| = N(\pi) = |\pi|^2$.)

   (c) For $\pi = 1 + i$, are $R/(\pi^3)$ and $\mathbb{Z}/8\mathbb{Z}$ isomorphic as rings?

3. Suppose F is a field with $\mathrm{char}(F) \neq 2$. Let α and β be elements of F, neither of which is a square in F.

   (a) Prove that $K = F(\sqrt{\alpha}, \sqrt{\beta})$ has degree 4 over F if $\alpha\beta$ is not a square in F.

   (b) What is $[K : F]$ when $\alpha\beta$ is a square in F? Prove your answer.

4. Suppose $K = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where α_i^2 is in $\mathbb{Q}$ for all i. Prove that $\sqrt[3]{7}$ is not in K.

5. Consider a field extension K/F where $[K : F] = n$. Recall from class on February 9 that for each $\gamma \in K$ we get an F-linear transformation $T_\gamma\colon K \to K$ defined by $T_\gamma(\alpha) = \gamma\alpha$. Let $M_n(F)$ denote the ring of $n \times n$ matrices with entries in F.

   (a) Let $A \in M_n(F)$ be the matrix of T_γ with respect to some basis $\mathcal{B} = \{\beta_1, \ldots, \beta_n\}$. Prove that γ is a root of the characteristic polynomial of A. (See Chapter 11 of Dummitt and Foote for a review of linear algebra. The characteristic polynomial is covered in Section 12.2.)

   (b) Part (a) lets us compute a monic polynomial in $F[x]$ of degree n that has γ as a root. Use this to find a monic polynomial in $\mathbb{Q}[x]$ of degree 3 satisfied by $\gamma = 1 + \sqrt[3]{2} + \sqrt[3]{4}$.