Assignment 2, due February 16 (before class starts).

Corrections

- February 14. Exercise 1 added and Exercise 3 removed.

Instructions

- Do not hand in a rough draft. Copy or type answers neatly and clearly. Points may be deducted for writing that is sloppy, has excessive cross-outs, or is hard to read.
- State facts precisely in clear language or notation. Put assertions in logical order. State clearly what the hypotheses and conclusions. Put the steps of an argument in logical order, including definitions. Points may be deducted for an incorrectly stated argument even if you seen to understand it. Clear mathematical exposition is an important goal for the class.
- Learn the Greek letters used in math. Learn their mathematical names and write them clearly.

Assigned Exercises, to hand in

1. Consider the ideal $I = (2, x) \subset \mathbb{Z}[x]$.
   (a) Characterize elements $f \in I$ in terms of its coefficients $a_0, \cdots, a_n$ (where $f(x) = a_0 + \cdots a_n x^n$).
   (b) Show that I is not a principal ideal.
   (c) Give an example of polynomials $f, g \in \mathbb{Z}$ so that there is no relation of the form $f = qg + r$ with $q, r \in \mathbb{Z}[x]$ and $\deg(r) < \deg(g)$ or $r = 0$.
   (d) Show that $\mathbb{Z}[x]$ is not a euclidean domain. *Warning.* This is not a trivial consequence of part (c). It is not enough to show that $\sigma(f) = \deg(f)$ does not work.
2. Let p be a rational prime that is also a Gaussian prime. Show that every $x + iy \in \mathbb{Z}[i]$ is equivalent to an element of the form $a + ib$ where $0 \leq a < p$ and $0 \leq b < p$, modulo the ideal $(p) \subset \mathbb{Z}[i]$. Use this to show that $\mathbb{F} = \mathbb{Z}[i]/(p)$ is a field with p^2 elements. *Hint.* You can prove $\mathbb{F}$ is a field by showing that (p) is a maximal ideal, or by finding an inverse for $\alpha = a + ib$ using an inverse mod p in $\mathbb{Z}$ for $n = \alpha\overline{\alpha}$.
3. (Exercise 5.3 of Chapter 12) Let $I \subset \mathbb{Z}[i]$ be the ideal generated by $3 + 4i$ and $4 + 7i$. Find $\alpha \in \mathbb{Z}[i]$ with $I = (\alpha)$. Such an α is a *generator* for I.

4. (Exercise 1.1 of Chapter 15) Suppose R is an integral domain ($xy = 0 \Longrightarrow x = 0$ or $y = 0$), $\mathbb{F} \subset R$ is a sub-ring that is a field. Suppose R is a vector space over $\mathbb{F}$ of finite dimension. Show that R is a field. *Hint.* This is a generalization of Exercise 1 of Assignment 1.

5. Suppose $\mathbb{F}$ is a finite degree extension of a field $\mathbb{K}$. Suppose $u_1, \cdots, u_n$ is a vector space basis of $\mathbb{F}$ as a vector space over $\mathbb{K}$. For any $\lambda \in \mathbb{F}$ the map $x \mapsto \lambda x$ is a linear transformation of this vector space. Let $A \in M_n(\mathbb{K}$ ($n \times n$ matrices with entries in $\mathbb{K}$) represent this linear transformation in the u_j basis. Show that λ is an eigenvalue of A. Find an example in which A has more than one eigenvalue in $\mathbb{F}$ and an example where λ is the only eigenvalue of A in $\mathbb{F}$.

Unassigned Exercises, for practice, not to hand in From the Chapter 12 exercises: 5.1, 5.2, from Chapter 15, exercise 2.1.
Also

1. Consider $f(x, y) = x - y^2$. Show that f is irreducible in $\mathbb{C}[x, y]$. Show that this implies that f is irreducible in any sub-field $\mathbb{F} \subset \mathbb{C}$.

2. Consider $f(x, y) = x^2 - y^2$. Show that f is irreducible in $\mathbb{Q}[x, y]$ but factors in in $\mathbb{C}[x, y]$.

3. Suppose $\mathbb{F} \subset A$, where $\mathbb{F}$ is a field and A is a ring. We say A extends $\mathbb{F}$. [Extension is not only for fields.] An element $\alpha \in A$ is *algebraic* if it satisfies a polynomial equation with coefficients in $\mathbb{F}$. The extension is algebraic if every element is algebraic. Otherwise it is transcendental, as for field extensions. An extension is *purely transcendental* if every $\alpha \notin \mathbb{F}$ is transcendental. Consider the quotient ring modulo the principal ideal

$$A = \mathbb{C}[x, y]/(x - y^2) .$$

   (a) Show that this is purely transcendental over $\mathbb{C}$.
   (b) Construct an extension that is transcendental but not purely transcendental.