PROBLEM SET 6

18.781 SPRING 2023

Due Monday, May 8. You may consult books, papers, and websites as long as you cite them and write up your solutions in your own words. Do not request answers on forums online. To get full points on a proof-based problem, *please write in complete sentences.*

Book. (Stillwell, *Elements of Number Theory*)

(1) 10.2.1–10.2.2
(2) 10.2.3–10.2.5
(3) 10.3.1–10.3.2
(4) 10.4.2–10.4.3
(5) 11.2.1–11.2.2
(6) 11.3.1–11.3.3
(7) 11.4.1–11.4.3
(8) 11.7.1–11.7.3
(9) 11.8.1–11.8.3

Non-Book. As usual, $\omega = e^{2\pi i/3} = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$.

Problem 1. Show that if F is a field and $I \subseteq F$ is a nonzero ideal, then $I = F$. *Hint:* $1 \in I$.

Problem 2. An *integral domain* is a ring R in which $1 \neq 0$ and the only divisor of 0 is 0. That is, if $ab = 0$, then either $a = 0$ or $b = 0$.

(1) Show that $\mathbf{Z}/m\mathbf{Z}$ is an integral domain if and only if m is prime or zero.
(2) Show that if R is an integral domain and $a \in R$ is nonzero, then the map $f_a : R \to R$ defined by $f_a(x) = ax$ is injective.
(3) Use part (2) to show that if R is a finite integral domain, then R is a field.
(4) Use part (3) to show that $\mathbf{Z}[i]/23\mathbf{Z}[i]$ and $\mathbf{Z}[\omega]/23\mathbf{Z}[\omega]$ are fields.

Problem 3. An *automorphism* of R is a ring isomorphism from R to itself.

(1) Show that if F is a field containing $\mathbf{Q}$, and f is an automorphism of F, then $f(a) = a$ for any $a \in \mathbf{Q}$. *Hint:* Do $a \in \mathbf{Z}$ first.
(2) Use part (1) to show that if $\zeta_n = e^{2\pi i/n}$ and f is an automorphism of

$$\mathbf{Q}(\zeta_n) = \{a_0 + a_1\zeta_n + \cdots + a_{n-1}\zeta_n^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in \mathbf{Q}\},$$

then f is determined by $f(\zeta_n)$.
(3) Use part (2) to show that the fields $\mathbf{Q}(i)$ and $\mathbf{Q}(\omega)$ each have two and only two automorphisms.
(4) Make a guess about the number of automorphisms of $\mathbf{Q}(\zeta_5)$. (More than two.) How about $\mathbf{Q}(\zeta_p)$ for prime $p > 5$?