Math 418, Spring 2025 – Homework 1

Due: Wednesday, January 29th, at 9:00am via Gradescope.

Instructions: Students should complete and submit all problems. Textbook problems are from Dummit and Foote, *Abstract Algebra, 3rd Edition.* All assertions require proof, unless otherwise stated. Typesetting your homework using LaTeX is recommended, and will gain you 1 bonus point per assignment.

1. **Dummit and Foote #7.1.3:** *Let R be a ring with identity and let S be a subring of R containing the identity. Prove that if u is a unit in S then u is a unit in R. Show by example that the converse is false.*

2. **Dummit and Foote #7.1.11:** *Prove that if R is an integral domain and $x^2 = 1$ for some $x \in R$ then $x = \pm 1$.*

3. **Dummit and Foote #7.2.1:** *Let $p(x) = 2x^3 - 3x^2 + 4x - 5$ and let $q(x) = 7x^3 + 33x - 4$. In each of parts (a), (b) and (c) compute $p(x)+q(x)$ and $p(x)q(x)$ under the assumption that the coefficients of the two given polynomials are taken from the specified ring (where the integer coefficients are taken mod n in parts (b) and (c)).*

   (a) $R = \mathbb{Z}$.

   (b) $R = \mathbb{Z}/2\mathbb{Z}$.

   (c) $R = \mathbb{Z}/3\mathbb{Z}$.

4. **Dummit and Foote #7.3.2:** *Prove that the rings $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ are not isomorphic.*

5. **Dummit and Foote #7.4.15:** *Let x^2+x+1 be an element of the polynomial ring $E = \mathbb{F}_2[x]$ and use the bar notation to denote passage to the quotient ring $\mathbb{F}_2[x]/(x^2+x+1)$.*

   (a) Prove that $\overline{E}$ has 4 elements: $\overline{0}, \overline{1}, \overline{x}$, and $\overline{x+1}$.

   (b) Write out the 4×4 addition table for $\overline{E}$ and deduce that the additive group $\overline{E}$ is isomorphic to the Klein 4-group.

   (c) Write out the 4×4 multiplication table for $\overline{E}$ and prove that $\overline{E}^{\times}$ is isomorphic to the cyclic group of order 3. Deduce that $\overline{E}$ is a field.

6. *Consider $R = \mathbb{Z}[\sqrt{-5}]$ with the (non-Euclidean) norm $N : R \to \mathbb{Z}_{\geq 0}$ given by $N(a) = |a|^2$ (Here, $|a|$ refers to the absolute value in $\mathbb{C}$). Note that $N(a \cdot b) = N(a)N(b)$.*

(a) Prove that $a \in R$ is a unit if and only if $N(a) = 1$. Find all the units in R.

(b) Recall that $r \in R$ is irreducible if whenever $r = ab$ then one of a or b is a unit. Use the norm to show that 2, 3, $1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are all irreducible elements of R

(c) Show that $2, 3, 1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are not unit multiples of one another, proving that R lacks unique factorization since $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

7. *Let R be an integral domain. Recall that g is a greatest common divisor of two elements $a, b \in R$ if g divides a and b, and if d divides a and b then d divides g.*

(a) Show that if g and g' are two gcds of $a, b \in R$, $g' = ug$ for some unit u.

(b) Let $R = \mathbb{Z}[\sqrt{-5}]$. Prove that 6 and $2 + 2\sqrt{-5}$ have no gcd. *(Hint: Use the fact that 2 and $1 + \sqrt{-5}$ are both common divisors of these elements)*