Math 418, Spring 2024 – Homework 1

Due: Wednesday, January 24th, 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 2 bonus points 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.

   Solution: Since $1_R \in S$, and by uniqueness of identity, $1_R = 1_S = 1$ is the identity in S. If u is a unit in S, then there exists $v \in S$ such that $uv = vu = 1$. Since $S \subseteq R$, $v \in R$, so u is a unit in R.

   On the other hand, if $R = \mathbb{Q}, S = \mathbb{Z}$, then S is subring of R containing the identity. However, 2 is a unit in R but not S.

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 $x = \pm 1$.

   Solution: Since $x^2 = 1$, $(x+1)(x-1) = x^2 - 1 = 0$. Since x is an integral domain, either $x + 1 = 0$ or $x - 1 = 0$, so $x = \pm 1$.

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) $R = \mathbb{Z}$.

   Solution: We simply do the usual polynomial addition and multiplication: $p(x) + q(x) = 9x^3 + 3x^2 + 37x - 9$ and $p(x)q(x) = 14x^6 - 21x^5 + 94x^4 - 142x^3 + 144x^2 - 181x + 20$.

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

   Solution: We reduce the expressions from the first part modulo 2: $p(x) + q(x) = x^3 + x^2 + x + 1$ and $p(x)q(x) = x^5 + x$.

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

   Solution: We reduce the expressions from the first part modulo 3: $p(x) + q(x) = x$ and $p(x)q(x) = 2x^6 + x^4 + 2x^3 + x + 2$.

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

   Proof. There are several approaches here. One way is to note that over an integral domain R, $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$ (Proof: if $p(x) = a_n x^n +$ (lower-degree terms) and $q(x) = b_m x^m +$ (lower-degree terms), then $p(x)q(x) = a_n b_m x^{n+m} +$ (lower-degree terms), and this coefficient is nonzero since R is an integral domain). Therefore, since all polynomials have nonnegative degrees, all units in $R[x]$ are units of R. In $\mathbb{Z}$ the units are $\{\pm 1\}$ while in $\mathbb{Q}[x]$ the units are $\mathbb{Q} \setminus \{0\}$. These have different cardinalities, so there cannot be an isomorphism $\mathbb{Z}[x] \to \mathbb{Q}[x]$ since such a map would need to biject the sets of units. $\square$

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 E has 4 elements: $\overline{0}, \overline{1}, \overline{x}$, and $\overline{x+1}$.

   Proof. If $e \in \overline{E}$, then e can be written as a degree-one polynomial since in $\overline{E}$, $x^2 = x + 1$, $x^3 = x(x+1) = x^2 + x = 1$, and so $x^{3k} = 1$, $x^{3k+1} = x$, $x^{3k+2} = x + 1$. Therefore, $E = \{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$ since these are the only degree-one polynomials over $\mathbb{F}_2$. On the other hand, these elements are distinct since their pairwise differences in E all have degree ≤ 1, so cannot be multiples of $x^2 + x + 1$ (since $\mathbb{F}_2$ is an integral domain; see reasoning from Problem 4). $\square$

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

   Solution: Addition table below. This is a group of order 4 which is not cyclic, so it is the Klein-4 group.

$+$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{x+1}$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{x+1}$	$\overline{0}$	$\overline{1}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{x}$	$\overline{1}$	$\overline{0}$

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

   Solution: Multiplication table below. Note that $\overline{E} \setminus \{\overline{0}\}$ consists of 3 elements, with (multiplicative) identity $\overline{1}$, and both $\overline{x}$ and $\overline{x+1}$ have inverses. Therefore, $\overline{E}^\times = \overline{E} \setminus \{\overline{0}\}$ is the cyclic group of order 3, and since every element of $\overline{E} \setminus \{\overline{0}\}$ is a unit, $\overline{E}$ is a field. [In fact, the multiplicative group of a finite field is always cyclic.]

$*$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{x+1}$	$\overline{1}$
$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{1}$	$\overline{x}$

6. Consider $R = \mathbb{Z}[\sqrt{-5}]$ with the (non-Euclidean) norm $N : R \to \mathbb{Z}_{\geq 0}$ given by $N(a) = |a|^2$. 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.

   Proof. Suppose a is a unit. Then

   $$1 = N(1) = N(a \cdot a^{-1}) = N(a)N(a^{-1})$$

   Since $N(a)$ and $N(a^{-1})$ are positive integers, the equality above forces $N(a) = 1$. Conversely suppose $N(a) = 1$. If $a = x + y\sqrt{-5}$, then

   $$N(a) = x^2 + 5y^2 = 1.$$

   This forces $y = 0$ and $x = \pm 1$. So a is a unit. In particular, the same argument shows that the units of R are $\{1, -1\}$. □

   (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

   Proof. Consider $2 \in R$. Suppose $2 = (x_1 + y_1\sqrt{-5})(x_2 + y_2\sqrt{-5})$. Taking norms both sides

   $$4 = (x_1^2 + 5y_1^2)(x_2^2 + 5y_2^2) = x_1^2x_2^2 + 5(\cdots)$$

   This has solution $x_1 = \pm 1; y_1 = 0; x_2 = \pm 2; y_2 = 0$ or vice versa, showing that 2 is irreducible.
   Next, consider $1+\sqrt{-5}$. Suppose $1+\sqrt{-5} = (x_1+y_1\sqrt{-5})(x_2+y_2\sqrt{-5})$. Taking norms both sides

   $$6 = (x_1^2 + 5y_1^2)(x_2^2 + 5y_2^2) = x_1^2x_2^2 + 5(x_1^2y_2^2 + x_2^2y_1^2 + 5y_1^2y_2^2).$$

   Since 6 is squarefree, the only solutions are $x_1 = \pm 1; y_1 = 0; x_2 = \pm 1; y_2 = \pm 1$ or vice versa, showing that $1 + \sqrt{-5}$ is irreducible.
   Similar arguments work for the other two cases. □

(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 $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$.

Proof. By part (a) the only units are ± 1, so the first statement follows by inspection. The example given shows that R lacks unique factorization since both factorizations are into irreducibles, but the two factorizations are not the same up to rearrangement and/or units. $\square$

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.

Proof. Since g and g' are both gcds of a and b, they divide each other; say $g = ug'$, $g' = vg$. Then $uv = vu = 1$, so u and v are inverses and therefore units in R. $\square$

(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)*

Proof. We have $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ and $2+2\sqrt{-5} = 2(1+\sqrt{-5})$, so 2 and $1+\sqrt{-5}$ are common divisors of 6 and $2+2\sqrt{-5}$. If g is a gcd of 6 and $2+2\sqrt{-5}$, then both 2 and $1+\sqrt{-5}$ divide g. Since $N(ab) = N(a)N(b)$ for all $a, b \in \mathbb{Z}[\sqrt{-5}]$, we have $4 = N(2)|N(g)$ and $6 = N(1+\sqrt{5})|N(g)$, and also $N(g)|N(6) = 36$ and $N(g)|N(2+2\sqrt{-5}) = 24$. This means that $N(g) = 12$, but this is impossible since a simple check shows that there are no nonnegative integers a and b such that $|a+b\sqrt{-5}| = a^2+5b^2 = 12$. $\square$