MATH 4000/6000 – Homework #5
posted March 26, 2025; due March 28, 2025

You can observe a lot by just looking. – Yogi Berra

Assignments are expected to be neat and stapled. **Illegible work may not be marked**. Starred problems (*) are required for those in MATH 6000 and extra credit for those in MATH 4000.

In this assignment, "ring" always means "commutative ring."

0. (UNDERSTANDING CHECKS; NOT TO TURN IN!) Let $\phi\colon R \to S$ be a ring homomorphism. Show that ϕ is one-to-one if and only if $\ker(\phi) = \{0_R\}$. (This should remind you of linear algebra!)

1. Decide whether each of the following polynomials is irreducible in $F[x]$ for the given field F. Justify your answers.
   (a) $f(x) = x^2 + \bar{1}$, $F = \mathbb{Z}_5$,
   (b) $f(x) = x^2 + \bar{1}$, $F = \mathbb{Z}_{19}$,
   (c) $f(x) = x^3 + x + \bar{1}$, $F = \mathbb{Z}_2$,

2. Decide whether each of the following polynomials is irreducible in $\mathbb{Q}[x]$. Justify your answers.
   (a) $f(x) = 3x^3 - 210x + 1$,
   (b) $f(x) = 6x^3 - 2x^2 + 21x - 7$,
   (c) $f(x) = x^5 - 3x + 6$,

3. (Proving irreducibility by reduction mod p)
   (a) Suppose $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is a polynomial with integer coefficients and degree $n \geq 1$. Suppose p is a prime not dividing a_n and that the polynomial
   $$g(x) = \overline{a_n}x^n + \overline{a_{n-1}}x^{n-1} + \cdots + \overline{a_0} \in \mathbb{Z}_p[x],$$
   obtained by reducing all coefficients mod p, is irreducible in $\mathbb{Z}_p[x]$. Prove that $f(x)$ is irreducible in $\mathbb{Q}[x]$.
   Hint. By Gauss's lemma, it is enough to show that $f(x)$ does not factor as a product of nonconstant polynomials with *integer* coefficients.
   (b) Using the result of (a), prove that $5001x^3 - 3001x + 10000001$ is irreducible in $\mathbb{Q}[x]$.

4. Let $\phi\colon R \to S$ be a homomorphism. Show that $\phi(R) = \{\phi(r) : r \in R\}$ is a subring of S, by using the criterion of Problem 1 from the last assignment.

5. (a) Show that the "squaring map" $f\colon R \to R$ given by $f(r) = r^2$ is **not** a homomorphism for the ring $R = \mathbb{Q}$ but is a homomorphism for $R = \mathbb{Z}_2[x]$.
   (b) (generalizing the second part of a) Let p be a prime number, and R be a commutative ring in which $\underbrace{1 + 1 + 1 + \cdots + 1}_{p \text{ times}} = 0$.
   Show that the "pth power map" $g\colon R \to R$ defined by $g(r) = r^p$ is a homomorphism.

6. Let R be a ring. Recall that if $x_1, \ldots, x_n$ are elements of R, then (by definition)
   $$\langle x_1, \ldots, x_n \rangle = \{r_1x_1 + \cdots + r_nx_n : \text{all } r_i \in R\}.$$
   In other words, $\langle x_1, \ldots, x_n \rangle$ is the set of all R-linear combinations of $x_1, \ldots, x_n$. Prove that for any given $x_1, \ldots, x_n \in R$, the set $\langle x_1, \ldots, x_n \rangle$ is an ideal of R by directly verifying the three defining properties of an ideal.

7. Let R be an integral domain. Show that if $a, b \in R$, then $\langle a \rangle = \langle b \rangle$ if and only if $a = u \cdot b$ for some unit $u \in R$. (Make sure your argument also handles the case when one of a or b is zero.)

8. (gcds as generators of ideals) Let R be a ring in which every ideal is principal. That is, every ideal of R has the form $\langle r \rangle$ for some $r \in R$.

   Let $x_1, \dots, x_n \in R$. Since $\langle x_1, \dots, x_n \rangle$ is an ideal of R, there is some $d \in R$ with $\langle x_1, \dots, x_n \rangle = \langle d \rangle$. Prove that d divides all of $x_1, \dots, x_n$ and that if e is any element of R dividing all of $x_1, \dots, x_n$, then $e \mid d$.

9. Let F be a field. Prove that if I is any ideal of $F[x]$, then $I = \langle f(x) \rangle$ for some $f(x) \in F[x]$.

   Imitate the proof from class for the analogous claim in $\mathbb{Z}$.

10. Let R be a ring, not the zero ring.

    (a) Prove that if $I \subseteq R$ is an ideal and $1 \in I$, then $I = R$.

    (b) Prove that $a \in R$ is a unit if and only if $\langle a \rangle = R$.

    (c) Prove that R is a field if and only if the only ideals in R are $\langle 0 \rangle$ and R.

11. (*; **MATH 6000 problem**) By a Gaussian prime, we mean a nonzero element $\pi \in \mathbb{Z}[i]$ that is (a) not a unit and (b) has the property that whenever $\pi = \alpha\beta$ with $\alpha, \beta \in \mathbb{Z}[i]$, either α or β is a unit. (You should be able to check, using what you know about $\mathbb{Z}[i]$ from the last assignment, that this agrees with the definition of primes in $\mathbb{Z}[i]$ given in class.)

    (a) Let p be a prime number (a prime in the ordinary integers!). Show that if $p = a^2 + b^2$ for some integers a, b, then p is **not** a prime in $\mathbb{Z}[i]$.

    (b) Conversely, show that if p is a prime number that cannot be written in the form $a^2 + b^2$ for any integers a and b, then p is prime in $\mathbb{Z}[i]$.

    Hint. If $p = \alpha\beta$, what can you say about the norms of α, β?

    (c) Show that every prime number p dividing $2^{10000} + 1$ is **not** prime in $\mathbb{Z}[i]$.

    Hint 1. In the last homework set, you proved the Gaussian division algorithm. A now familiar reasoning process leads to the Gaussian prime analogue of Euclid's lemma, which may be assumed for this problem: If π is a Gaussian prime and $\pi \mid \alpha\beta$, then π divides α or $\pi \mid \beta$. Hint 2. $2^{10000} + 1$ factors in $\mathbb{Z}[i]$ as a difference of squares.

12. (*; **MATH 6000 problem**) Let $R = \mathbb{Z}[x]$, and let I be the set of elements of R with even constant term. Show that I is an ideal of R but that I is not principal: there is no $f(x) \in \mathbb{Z}[x]$ with $I = f(x)\mathbb{Z}[x]$.