MATH 4000/6000 – Homework #6

posted April 16, 2025; due April 25, 2025

Many who have never had occasion to learn what mathematics is confuse it with arithmetic, and consider it a dry and arid science. In reality, however, it is the science which demands the utmost imagination.
– Sofia Kovalevskaya

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.

0. (UNDERSTANDING CHECKS; NOT TO TURN IN!)
   (a) Suppose $\phi\colon R \to S$ is a ring isomorphism. Prove that R is the zero ring $\Longleftrightarrow$ S is the zero ring. Remember that a ring is called the zero ring when its additive identity 0 is the same as its multiplicative identity 1; equivalently (as shown in class), when the ring has a unique element.
   (b) Let R be a commutative ring, and let I be an ideal of R. Prove that R/I is the zero ring if and only if $I = R$.
1. Prove that isomorphism defines an equivalence relation on rings. That is:
   (a) $R \cong R$ for all rings R.
   (b) For all rings R and S, if $R \cong S$, then $S \cong R$.
   (c) For all rings R, S, and T, if $R \cong S$ and $S \cong T$, then $R \cong T$.

   You should use standard facts about bijections from MATH 3200: the inverse of a bijection is a bijection, and the composition of two bijections is a bijection.
2. Let A be a ring. We say that A satisfies condition (N) if
   $$A \text{ contains a nonzero element which squares to } 0. \tag{N}$$
   For example, $\mathbb{Z}_4$ satisfies condition (N), since $2^2 = 0$ in $\mathbb{Z}_4$ while $2 \neq 0$. However, $\mathbb{Z}_5$ does not satisfy condition (N).

   Give a careful proof that if R and S are rings for which $R \cong S$, then R satisfies condition (N) if and only if S satisfies condition (N).
3. Use the Euclidean algorithm and backtracking to find $X(x), Y(x) \in \mathbb{Z}_5[x]$ with
   $$(x^2+3)X(x) + (x^3 - 3x - 2)Y(x) = 1 \quad \text{in } \mathbb{Z}_5[x].$$
   Use this to compute the inverse of $\alpha^2 + 3$ in $R = \mathbb{Z}_5[x]/\langle x^3 - 3x - 2\rangle$, where (as usual) we write $\alpha = \overline{x}$. Express your answer in the form $a_0 + a_1\alpha + a_2\alpha^2$, where $a_0, a_1, a_2 \in \mathbb{Z}_5$.
4. Using the Fundamental Homomorphism Theorem, show:
   (a) $R/\langle 0\rangle \cong R$ for each commutative ring R,
   (b) $R[x]/\langle x\rangle \cong R$ for each nonzero commutative ring R.

   Suggestions. For (a), find an onto homomorphism from R to R with kernel $\langle 0\rangle$. For (b), find an onto homomorphism from $R[x]$ to R with kernel $\langle x\rangle$.

For the following sequence of problems we need some new terminology. Let F and K be fields, and suppose F is a subring of K. In this case, we say F is a subfield of K. For each $\beta \in K$, there is an "evaluate at β" homomorphism from $F[x]$ to K defined by

$$\begin{aligned} \mathrm{ev}_\beta : F[x] &\to K \\ f(x) &\mapsto f(\beta). \end{aligned}$$

That is, ev_β takes a polynomial with F-coefficients and evaluates at $x = \beta$ to get an element of K. Note that $\mathrm{ev}_\beta(1) = 1$. Furthermore, if you add two polynomials and then plug in β, you get the same result as if you plugged in β first and then added the results in K. Similarly for multiplication. So ev_β is a homomorphism, as claimed.

We define the image of ev_β by $F[\beta]$. That is,

$$F[\beta] = \{f(\beta) : f(x) \in F[x]\}.$$

Since the image of a homomorphism is always a subring, we know that $F[\beta]$ is a subring of K.

5. Suppose F is a subfield of K and $\beta \in K$.

   (a) Explain why $F \subseteq F[\beta]$.

   (b) Show that $F[\beta]$ is a domain.

   (c) Take as known that the real number $\pi = 3.1415\ldots$ is not a root of any nonconstant polynomial $f(x) \in \mathbb{Q}[x]$.[1] From (a) and (b) — taking $F = \mathbb{Q}, K = \mathbb{R}$, and $\beta = \pi$ — we know that $\mathbb{Q}[\pi] = \{f(\pi) : f(x) \in \mathbb{Q}[x]\}$ is a subring of $\mathbb{R}$ and in fact an integral domain. Show that $\mathbb{Q}[\pi]$ is *not* a field.

   Hint. Both (a) and (b) admit one-line solutions. For (c), show that π has no multiplicative inverse in $\mathbb{Q}[\pi]$.

6. Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. Then $f(x)$ has no root in $\mathbb{Q}$, but $f(x)$ has the root $\sqrt[3]{2} \in \mathbb{R}$. Let $\mathrm{ev}_{\sqrt[3]{2}} : \mathbb{Q}[x] \to \mathbb{R}$ be the evaluation at $\sqrt[3]{2}$ map, and let $\mathbb{Q}[\sqrt[3]{2}]$ be the image in $\mathbb{R}$ of $\mathrm{ev}_{\sqrt[3]{2}}$.

   (a) Show that $\ker(\mathrm{ev}_{\sqrt[3]{2}}) = \langle x^3 - 2\rangle$.

   Hint. Earier results from class (which?) imply that $\ker(\mathrm{ev}_{\sqrt[3]{2}}) = \langle m(x)\rangle$ for some $m(x) \in \mathbb{Q}[x]$. On the other hand, it is obvious that $x^3 - 2 \in \ker(\mathrm{ev}_{\sqrt[3]{2}})$ (make sure you see why). Hence, $m(x) \mid x^3 - 2$. Go from there.

   (b) Deduce from (a) and the Fundamental Homomorphism Theorem that $\mathbb{Q}[x]/\langle x^3 - 2\rangle \cong \mathbb{Q}[\sqrt[3]{2}]$. Explain why this implies that $\mathbb{Q}[\sqrt[3]{2}]$ is a field.

7. (continuation) Find $(2 + \sqrt[3]{2} + \sqrt[3]{4})^{-1}$ in $\mathbb{Q}[\sqrt[3]{2}]$. Express your answer in the form $c_0 + c_1\sqrt[3]{2} + c_2(\sqrt[3]{2})^2$, where $c_0, c_1, c_2 \in \mathbb{Q}$.

8. Use the Fun. Homomorphism Theorem to show that $\mathbb{Q}[x]/\langle x^2 - 1\rangle \cong \mathbb{Q} \times \mathbb{Q}$. Is $\mathbb{Z}_2[x]/\langle x^2 - 1\rangle$ isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$? Justify your answers.

   Hint for the first part: Consider the homomorphism from $\mathbb{Q}[x]$ to $\mathbb{Q} \times \mathbb{Q}$ given by $f(x) \mapsto (f(1), f(-1))$. What is the image? What is the kernel?

[1] This is a celebrated theorem of Lindemann (1882): *π is transcendental*. We also know that $e = 2.71828\ldots$ is transcendental (Hermite, 1873). But it remains an open querstion to decide whether or not $e + \pi$ is transcendental.

9. (***; MATH 6000 problem**) Let F and K be fields with F a subfield of K. An element $\beta \in K$ is said to be algebraic over F if β is a root of some nonconstant polynomial in $F[x]$.

   (a) Suppose $\beta \in K$ is algebraic over F. Prove that β is the root of an *irreducible* polynomial $p(x) \in F[x]$.

   (b) Prove that the evaluation map $\mathrm{ev}_\beta : F[x] \to K$ has kernel $\langle p(x) \rangle$ for the polynomial $p(x)$ of part (a). Deduce that $F[x]/\langle p(x) \rangle \cong F[\beta]$ and conclude that $F[\beta]$ is a field.

10. (***; MATH 6000 problem**) Let R be a commutative ring. An ideal I of R is called a maximal ideal if I is a proper subset of R and there is no ideal J with

$$I \subsetneq J \subsetneq R.$$

In other words, I is a maximal ideal of R if I is a proper ideal of R not strictly contained in another proper ideal of R.

   (a) Suppose that I is a maximal ideal of R. Let a be an element of R not belonging to I. Prove that every element of R has the form $ax + b$ for some $x \in R$ and some $b \in I$.

   (b) Suppose that I is a maximal ideal of R. Show that R/I is a field.

   (c) Prove the converse of (b): If R is a commutative ring and I is an ideal of R for which R/I is a field, then I is a maximal ideal of R. (Throughout this problem you may assume the result of Problem 0 that R/I is the zero ring if and only if $I = R$.)