JOSEPH OKONOBOH
MATHEMATICS
CAL STATE LONG BEACH

MATH 444, SPRING 2015
SECTION 1 (5562)
HW #11, DUE: 2015, APRIL 27

1. Consider the veracity or falsehood of each of the following statements. For bonus, argue for those that you believe are true while providing a counterexample for those that you believe are false.

   1. $\mathbb{Z}(\sqrt{2})$ is a UFD.
   2. If $\alpha : R \to S$ is a ring homomorphism, then it is one-to-one if the only $r \in R$ satisfying $\alpha(r) = 0$ is $r = 0$.
   3. Every integral domain is a field.
   4. If every element of a ring is an idempotent, then the ring is commutative.
   5. The group of units of $\mathcal{M}_2(\mathbb{Z}_3)$ has 56 elements.

   Solution.

   1. False.
   2. True.
      Proof. Let $\alpha : R \to S$ be a ring homomorphism with a trivial kernel. Suppose $\alpha(a) = \alpha(b)$. Then it follows that $\alpha(a - b) = \alpha(a) - \alpha(b) = 0$. Since the kernel of α is trivial, we must have that $a - b = 0$; that is, $a = b$. Thus α is injective. $\square$
   3. False.
      Counterexample. $\mathbb{Z}$ is an integral domain, but it is not a field.
   4. False.
      Counterexample. Consider the set
      $$S = \left\{ \begin{pmatrix} 1 & b \\ 0 & 0 \end{pmatrix} : b \in \mathbb{Z} \right\} \cup I_2 \cup \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$
      Define $A + B = 0$ for all $A, B \in S$. We can easily show that S is closed under the usual multiplication, so that S is a ring. Notice that every element of S is idempotent, but S is not commutative because
      $$\begin{pmatrix} 1 & 7 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 3 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 7 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 7 \\ 0 & 0 \end{pmatrix}$$
   5. False. A matrix is in $\mathcal{M}_2(\mathbb{Z}_3)$ if and only if its row vectors are linearly independent. But the number of matrices in $\mathcal{M}_2(\mathbb{Z}_3)$ with linearly independent rows is
      $$(3^2 - 1)(3^2 - 3) = 48,$$
      so that $|\mathcal{M}_2(\mathbb{Z}_3)| = 48$.

2. Let $A = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ be an element of $\mathbb{Z}(\sqrt{2})$. Suppose that $\det A$ is even. Show there is an element of $\mathbb{Z}(\sqrt{2})$ whose determinant is $\frac{1}{2}\det A$. **Hint.** Find an element of determinant 2 and show that you can divide A by it.

Proof. Since $\det A$ is even, we have that $\det A = 2k = a^2 - 2b^2$ for some integer k. Now we have that $a^2 = 2b^2 + 2k = 2(b^2 + k)$, so that a^2—and thus a—is even. Let $B = \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}$. Solving the equation $A = BX$ where $X = \begin{pmatrix} x & y \\ 2y & x \end{pmatrix}$ will result in $x = a - b$ and $y = b - a/2$. Since a is even, it follows that $a/2$ is an integer, so that y is an integer. Thus $X \in \mathbb{Z}(\sqrt{2})$. Hence

$$2k = \det A = \det(BX) = \det(B)\det(X) = 2\det(X),$$

so that $\det X = k = \frac{1}{2}\det A$, as desired. □

3. **On Factoring.**

(1) Give all irreducible cubics over $\mathbb{Z}_2$.

(2) Factor $p(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ completely in $\mathbb{Z}_2[x]$.

(3) How many monic quadratics are there in $\mathbb{Z}_3[x]$?

(4) Find all irreducible monic quadratics over $\mathbb{Z}_3$.

(5) Factor $q(x) = x^6 + x^3 - x^2 - x$ completely in $\mathbb{Z}_3[x]$.

(6) Consider the mod function from $\mathbb{Z}$ to $\mathbb{Z}_3$, and its natural extension to a homomorphism from $\mathbb{Z}[x]$ to $\mathbb{Z}_3[x]$ that mods out the coefficients, for example $5x$ goes to $2x$. Find the image under this homomorphism of the polynomial

$$h(x) = x^6 + 9x^5 + 21x^4 + 37x^3 + 53x^2 + 29x + 15.$$

(7) Do the same as in (6) except now one mods out 2.

(8) Use parts (2) and (5) to discuss the possible factorization of $h(x)$. For example, does it have any integer roots? Or is it irreducible etc. Discuss as much as you can.

Solution.

(1) The irreducible cubics over $\mathbb{Z}_2$ are:

$$x^3 + x + 1 \text{ and } x^3 + x^2 + 1.$$

(2) $p(x) = (x^3 + x + 1)(x^3 + x^2 + 1)$.

(3) There are 9 monic quadratics in $\mathbb{Z}_3[x]$.

(4) The irreducible monic quadratics over $\mathbb{Z}_3[x]$ are:

$$x^2 + 1, x^2 + x + 2, \text{ and } x^2 + 2x + 2.$$

(5) $q(x) = x(x + 1)(x + 2)^2(x^2 + x + 2)$.

(6) The image of $h(x)$ under this homomorphism is:

$$x^6 + x^3 + 2x^2 + 2x.$$

(7) The image of $h(x)$ under this homomorphism is:

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.$$

(8) From (2), we know that $h(x)$ mod 2 doesn't have a root in $\mathbb{Z}_2[x]$; thus $h(x)$ doesn't have a root in $\mathbb{Z}$ by Homework 10 Problem 1.2. That is $h(x)$ has no linear factors, and by extension, no quintic factor. Although we know from (5) that $h(x)$ mod 3 is not irreducible in $\mathbb{Z}_3[x]$, we cannot conclude that $h(x)$ is not irreducible in $\mathbb{Z}$ (Homework 10 Problem 1.4).

4. **On Factorization.**

(1) Find the complete factorization of $x^5 - 1$ in $\mathbb{Q}[x]$.

(2) Find real numbers a and b such that

$$(x^2 + ax + 1)(x^2 + bx + 1) = x^4 + x^3 + x^2 + x + 1.$$

(3) Find the complete factorization of $x^5 - 1$ in $\mathbb{R}[x]$.

(4) Find the complete factorization of $x^5 - 1$ in $\mathbb{C}[x]$.

(5) Find the complete factorization of $x^5 - 1$ in $\mathbb{Z}_{11}[x]$.

(6) Find the complete factorization of $x^5 - 1$ in $\mathbb{Z}_{31}[x]$.

(7) Find the complete factorization of $x^{10} - 1$ in $\mathbb{Q}[x]$.

Solution.

(1) In $\mathbb{Q}[x]$, we have $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$.

(2) Solving the equation

$$(x^2 + ax + 1)(x^2 + bx + 1) = x^4 + x^3 + x^2 + x + 1,$$

for real numbers a and b, we shall get

$$a = \frac{1+\sqrt{5}}{2} \text{ and } b = \frac{1-\sqrt{5}}{2}.$$

(3) In $\mathbb{R}[x]$, we have $x^5 - 1 = (x-1)\left(x^2 + \frac{1+\sqrt{5}}{2}x + 1\right)\left(x^2 + \frac{1-\sqrt{5}}{2}x + 1\right)$.

(4) In $\mathbb{C}[x]$, we have

$$x^5 - 1 = (x-1)(x-(A+Bi))(x-(A-Bi))(x-(C+Di))(x-(C-Di)),$$

where $A = \dfrac{-1-\sqrt{5}}{4}$, $B = \dfrac{1}{2}\sqrt{\dfrac{5-\sqrt{5}}{2}}$, $C = \dfrac{\sqrt{5}-1}{4}$, and $D = \dfrac{1}{2}\sqrt{\dfrac{5+\sqrt{5}}{2}}$.

(5) In $\mathbb{Z}_{11}[x]$, we have

$$x^5 - 1 = (x+2)(x+6)(x+7)(x+8)(x+10).$$

(6) In $\mathbb{Z}_{31}[x]$, we have

$$x^5 - 1 = (x+15)(x+23)(x+27)(x+29)(x+30).$$

(7) In $\mathbb{Q}[x]$, we have $x^{10} - 1 = (x-1)(x+1)(x^4 - x^3 + x^2 - x + 1)(x^4 + x^3 + x^2 + x + 1)$.