JOSEPH OKONOBOH
MATHEMATICS
CAL STATE LONG BEACH

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) There is a field with 16 elements.

(2) In $\mathbb{Z}[\sqrt{7}]$, $\begin{pmatrix} 9 & 4 \\ 28 & 9 \end{pmatrix}$ is a prime.

(3) The polynomial $x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ where a is odd, b is even and c is odd, is always irreducible over $\mathbb{Z}$.

(4) $\mathbb{Z}[\sqrt{-5}]$ is a UFD.

(5) In $\mathbb{Z}[\sqrt{7}]$, $\begin{pmatrix} 8 & 3 \\ 21 & 8 \end{pmatrix}$ is a unit.

Solution.

(1) True.

Example. Let $F = \mathbb{Z}_2[x]/(x^4 + x + 1)$. That is, F consists of the polynomials in $\mathbb{Z}_2[x]$ mod $x^4 + x + 1$. Thus F is the set of all polynomials of degree less than 4 with coefficients in $\mathbb{Z}_2[x]$, so that $|F| = 16$. Addition and multiplication in F are carried out mod $x^4 + x + 1$. It is clear that F is a commutative ring. Since

$$\begin{aligned} 1 \cdot 1 &= 1 \\ x(x^3 + 1) &= 1 \\ (x + 1)(x^3 + x^2 + x) &= 1 \\ x^2(x^3 + x^2 + 1) &= 1 \\ (x^2 + 1)(x^3 + x + 1) &= 1 \\ (x^2 + x)(x^2 + x + 1) &= 1 \\ x^3(x^3 + x^2 + x + 1) &= 1 \\ (x^3 + x^2)(x^3 + x) &= 1, \end{aligned}$$

it follows that every nonzero element of F has a multiplicative inverse, so that F is a field.

(2) True. It follows immediately since the determinant is a prime that is also co-prime with 7.

(3) True.

Proof. Let $p(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$, where b is even and a and c are odd. Suppose to the contrary that $p(x)$ is not irreducible. Then it follows that $p(x)$ must have a root, say $x_0 \in \mathbb{Z}$. So $0 = p(x_0) = {x_0}^3 + a{x_0}^2 + bx_0 + c$. That is, $x_0(-{x_0}^2 - ax_0 - b) = c$. This says that x_0 is a divisor of c. Then since c is odd, it must be the case that x_0 is also odd. But then we must have that ${x_0}^3$ is odd, $a{x_0}^2$ is odd, and bx_0 is even, so that ${x_0}^3 + a{x_0}^2 + bx_0 + c$ is odd, a contradiction since ${x_0}^3 + a{x_0}^2 + bx_0 + c = 0$ is even. Thus $p(x)$ is irreducible. $\square$

(4) False.
Proof. First we want to show that the elements

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, B = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}, C = \begin{pmatrix} 1 & 1 \\ -5 & 1 \end{pmatrix}, \text{ and } D = \begin{pmatrix} 1 & -1 \\ 5 & 1 \end{pmatrix}$$

are irreducible in $\mathbb{Z}[\sqrt{-5}]$. We shall only show that A and C are irreducible since the arguments for B and D are similar. Suppose $A = A_1 A_2$. Then it follows that

$$4 = \det(A) = \det(A_1)\det(A_2).$$

Observe that since we are in $\mathbb{Z}[\sqrt{-5}]$, it is impossible for the determinant of any matrix to be 2. Moreover, since the determinant of every matrix is nonnegative, we must have that either A_1 or A_2 has determinant of 1, so that one of A_1 and A_2 is a unit. Thus A is irreducible. Now suppose $C = C_1 C_2$. Then it follows that

$$6 = \det(C) = \det(C_1)\det(C_2).$$

No matrix has determinat 2 or 3 in $\mathbb{Z}[\sqrt{-5}]$. Thus one of C_1 or C_2 must be a unit, and it follows that C is irreducible. Since the units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1, it follows that none of the irreducibles above are associates. It follows immediately that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD because we have the following two distinct factorizations into irreducibles:

$$\begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ -5 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 5 & 1 \end{pmatrix}.$$

□

(5) True. Since the determinant of the matrix in question is 1, it is a unit.

2. In a previous homework we encountered the integral domain R of 2×2 matrices of the form $A = \begin{pmatrix} a & b \\ -b & a-b \end{pmatrix}$ where $a, b \in \mathbb{Z}$. Do the following:

(1) Prove that no element of R can have a negative determinant.

(2) Find a nontrivial unit.

(3) Find all units. Give an argument for your answer.

(4) Find an element whose determinant is a prime.

(5) Decide whether $\begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$ is irreducible or not. If not factor it into irreducibles.

(6) Do the same for $\begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}$.

(7) Do the same for $\begin{pmatrix} 34 & 41 \\ -41 & -7 \end{pmatrix}$.

(8) Show that the element $A = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ is a prime by showing that if $MN \equiv 0 \bmod A$, then either $M \equiv 0 \bmod A$ or $N \equiv 0 \bmod A$.

Solution.

(1) **Proof.** Let $A = \begin{pmatrix} a & b \\ -b & a-b \end{pmatrix} \in R$. Since

$$\det(A) = a(a-b) + b^2 = \left(a - \frac{b}{2}\right)^2 + \frac{3}{4}b^2 \geq 0,$$

it follows that no element of R can have a negative determinant. □

(2) A nontrivial unit in R is $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$.

(3) Let $A = \begin{pmatrix} a & b \\ -b & a-b \end{pmatrix} \in R$ be a unit. It follows by (1) that

$$1 = \det(A) = a^2 + b^2 - ab;$$

thus we want integers a and b such that $a^2 + b^2 - ab = 1$. By completing the square we get that

$$a^2 + b^2 - ab = 1 \text{ iff } a = \frac{b}{2} \pm \sqrt{\frac{4 - 3b^2}{4}}.$$

For the discrimant to be nonnegative, we must have that $b = 0$ or $|b| = 1$. It follows that (a, b) is an integral solution of $a^2 + b^2 - ab = 1$ iff

$$(a, b) \in \{(-1, 0), (1, 0), (0, 1), (1, 1), (0, -1), (-1, -1)\}.$$

Thus the group of units is

$$\left\{ I, -I, \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \right\}.$$

(4) The element $\begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix}$ has determinant 3.

(5) The matrix $\begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$ is not irreducible since we have the following factorization into irredcibles:

$$\begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} -1 & -2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ -2 & -1 \end{pmatrix}.$$

The factors in the factorization above are irreducible since their determinants are prime.

6. Let $B = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}$. Claim that B is irreducible.

Proof. Suppose $B = XY$. Then it follows that

$$25 = \det(B) = \det(X)\det(Y).$$

Now suppose that $\det(X) = 5$. Then if we have that $X = \begin{pmatrix} x & y \\ -y & x-y \end{pmatrix}$, it follows that $x^2 - xy + y^2 = 5$. That is

$$x = \frac{y}{2} \pm \sqrt{\frac{20-3y^2}{4}}.$$

By observing the discrimant, we see that y can only take on values 0, 1, and 2. But x is not an integer for any of these values. Thus no matrix in R exists with determinant 5. It follows that one of X and Y must have determinant 1, so that this matrix is a unit; thus B is irreducible in R. $\square$

7. The matrix $\begin{pmatrix} 34 & 41 \\ -41 & -7 \end{pmatrix}$ is not irreducible since we have the following factorization into irredcibles:

$$\begin{pmatrix} 34 & 41 \\ -41 & -7 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 4 & 1 \\ -1 & 3 \end{pmatrix}\begin{pmatrix} 7 & 3 \\ -3 & 4 \end{pmatrix}.$$

The factors in the factorization above are irreducible since their determinants are prime.

8. **Proof.** Suppose $MN \equiv 0 \bmod A$. That is, $AX = MN$ for some matrix $X \in R$. Thus

$$4\det(X) = \det(A)\det(X) = \det(AX) = \det(MN) = \det(M)\det(N).$$

We can then conclude that the determinants of M and N cannot be both odd. So suppose without loss that $\det(M) = 2k$ for some integer k. Now if

$$M = \begin{pmatrix} x & y \\ -y & x-y \end{pmatrix},$$

then $x^2 - xy + y^2 = 2k$. If x and y are both odd, then $x^2 - xy + y^2$ will also be odd, a contradiction. If x is odd and y is even (or vice-versa), then $x^2 - xy + y^2$ will again be odd. Thus the only viable option is that x and y are both even. Now write $x = 2k_1$ and $y = 2k_2$ for some integers k_1 and k_2. Since $X' = \begin{pmatrix} k_1 & k_2 \\ -k_2 & k_1 - k_2 \end{pmatrix} \in R$ and since $AX' = M$, it follows that $M \equiv 0 \bmod A$, so that A is prime. $\square$

3. **On Nilpotent Elements.**

1. Let R be a ring. An element $m \in R$ is called nilpotent if $m^k = 0$ for some positive integer k. Let $r = 1 + m + m^2 + \cdots + m^{k-1}$. Show r is invertible by finding its inverse.

(2) Exemplify (1) by using the matrix $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$.

Solution.

(1) We have

$$\begin{aligned} rm &= (1 + m + m^2 + \cdots + m^{k-1})m \\ &= m + m^2 + \cdots + m^{k-1} + m^k \\ &= m + m^2 + \cdots + m^{k-1} \\ &= r - 1, \end{aligned}$$

so that $r(1 - m) = 1$. Similarly

$$\begin{aligned} mr &= m(1 + m + m^2 + \cdots + m^{k-1}) \\ &= m + m^2 + \cdots + m^{k-1} + m^k \\ &= m + m^2 + \cdots + m^{k-1} \\ &= r - 1, \end{aligned}$$

so that $(1 - m)r = 1$. We have thus shown that the multiplicative inverse of r is $1 - m$. Thus r is invertible.

(2) Let $B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$. A quick computation will show us that the smallest positive integer k for which $B^k = 0$ is 3. Thus if $r = I + B + B^2 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, we have that

$$r(I - B) = r \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} = I,$$

so that r is invertible.

BONUS. Consider the integral domain $R = \mathbb{Z}[\sqrt{3}]$. Let $A = \begin{pmatrix} 5 & 3 \\ 9 & 5 \end{pmatrix}$. Decide if (1)-(4) are irreducible or not. Argue your case.

(1) A.

(2) $\begin{pmatrix} 19 & 11 \\ 33 & 19 \end{pmatrix}$.

(3) $\begin{pmatrix} 34 & 20 \\ 60 & 34 \end{pmatrix}$.

(4) $\begin{pmatrix} 362 & 209 \\ 627 & 362 \end{pmatrix}$.

(5) Factor $\begin{pmatrix} 69 & 0 \\ 0 & 69 \end{pmatrix}$ into irreducibles.

(6) Show that A is prime by showing that R_A is a field. **Hint.** Show that if $M \in R$ has even determinant, then $A \mid M$, and if M has odd determinant, then $A \mid (M - I)$.

(7) Find a nontrivial common divisor of $\begin{pmatrix} 89 & 53 \\ 159 & 89 \end{pmatrix}$ and $\begin{pmatrix} 86 & 48 \\ 144 & 86 \end{pmatrix}$, and show why it is a common divisor.

(8) Find the greatest common divisor of $\begin{pmatrix} 89 & 53 \\ 159 & 89 \end{pmatrix}$ and $\begin{pmatrix} 86 & 48 \\ 144 & 86 \end{pmatrix}$, and give reasons.

(9) Find the lcm of $\begin{pmatrix} 89 & 53 \\ 159 & 89 \end{pmatrix}$ and $\begin{pmatrix} 86 & 48 \\ 144 & 86 \end{pmatrix}$.

More Bonus. Argue every element is a product of irreducibles in R.

Hard Bonus. Argue every irreducible is prime.

Solution.

(1) Since the determinant of A is 1, it follows that A is a unit so that A is not irreducible.

(2) This matrix is irreducible since its determinant is a prime.

(3) Not irreduible since (use idea in (6) to continually factor A out of the given matrix)

$$\begin{pmatrix} 34 & 20 \\ 60 & 34 \end{pmatrix} = A^2 \begin{pmatrix} -8 & 5 \\ 15 & -8 \end{pmatrix}.$$

(4) This matrix is not irreducible since it is a unit.

(5)

$$\begin{pmatrix} 69 & 0 \\ 0 & 69 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 23 & 0 \\ 0 & 23 \end{pmatrix}$$

(6) **Proof.** We want to first prove the hint. So suppose $M = \begin{pmatrix} m & n \\ 3n & m \end{pmatrix}$ has even determinant. Observe that if m and n have different parities, then the determinant of M must be odd. Thus m and n must either be both odd or both even. Now we want to find a matrix $B = \begin{pmatrix} a & b \\ 3b & a \end{pmatrix} \in R$ such that $BA = X$. Solving the equation $BA = X$ for a and b will give us the following:

$$a = -\frac{1}{2}(5m - 9n)$$
$$b = \frac{1}{2}(3m - 5n).$$

But since m and n have the same parities, it follows that $5m - 9n$ and $3m - 5n$ are even so that a and b are integers. Thus $B \in R$ and $A \mid M$. Now suppose that

M has an odd determinant. Thus m and n have different parities. So suppose first that m is even and n is odd. Thus it follows that $m-1$ is odd, so that $M-I$ has an even determinant and so is divisible by A. Similarly if m is odd and n is even, then $m-1$ must be even so that $M-I$ has an even determinant and thus is also divisible by A. Thus we have proven the hint. Now consider $R/(A)$ (the set of elements in $\mathbb{Z}[\sqrt{3}]$ mod A). Let $C \in R$. If $\det(C)$ is even, then $C = AX'$ for some $X' \in R$. This means that $C \equiv 0 \bmod A$. Now if $\det(C)$ is odd, then $C - I = AX''$ for some $X'' \in R$. Thus $C \equiv I \bmod A$. Hence $R/(A) = \{\mathbf{0}, I\}$, which is clearly a field, where $\mathbf{0}$ is the additive inverse and I is the multiplicative inverse. Now we are ready to show that A is prime. Suppose for some $S, T \in R$, A divides ST, so that $AY = ST$ for some $Y \in R$. Viewing this equation $AY = ST$ in $R/(A)$, we must have that $ST = AY = \mathbf{0}Y = \mathbf{0}$. Since $R/(A)$ is a field, it must be an integral domain. Hence $ST = \mathbf{0}$ implies that $S = \mathbf{0}$ or $T = \mathbf{0}$. That is A divides S or A divides T, so that A is prime. $\square$

7 Since the determinants of both matrices in question are even, then we know from 6 that they are both divisible by A. Thus A is a common divisor of both matrices.