

MATH 415  
Modern Algebra I

**Lecture 30:**  
**Review for Exam 2.**

## Topics for Exam 2

*Basic theory of rings and fields:*

- Rings and fields
- Integral domains
- Modular arithmetic
- Rings of polynomials
- Factorization of polynomials

Fraleigh/Brand: Sections 22–28

## Sample problems

**Problem 1.** Let  $M$  be the set of all  $2 \times 2$  matrices of the form  $\begin{pmatrix} n & k \\ 0 & n \end{pmatrix}$ , where  $n$  and  $k$  are rational numbers. Under the operations of matrix addition and multiplication, does this set form a ring? Does  $M$  form a field?

**Problem 2.** Let  $L$  be the set of the following  $2 \times 2$  matrices with entries from the field  $\mathbb{Z}_2$ :

$$A = \begin{pmatrix} [0] & [0] \\ [0] & [0] \end{pmatrix}, \quad B = \begin{pmatrix} [1] & [0] \\ [0] & [1] \end{pmatrix},$$
$$C = \begin{pmatrix} [1] & [1] \\ [1] & [0] \end{pmatrix}, \quad D = \begin{pmatrix} [0] & [1] \\ [1] & [1] \end{pmatrix}.$$

Under the operations of matrix addition and multiplication, does this set form a ring? Does  $L$  form a field?

## Sample problems

**Problem 3.** Prove that for a ring with unity, commutativity of addition follows from the other axioms.

**Problem 4.** Find a direct product of cyclic groups that is isomorphic to  $G_{16}$  (multiplicative group of all invertible elements of the ring  $\mathbb{Z}_{16}$ ).

**Problem 5.** Determine the last two digits of  $303^{303}$ .

**Problem 6.** Find all integer solutions of the equation  $21x - 32y = 4$ .

## Sample problems

**Problem 7.** Find all integer solutions of the equation  $2x + 3y + 5z = 7$ .

**Problem 8.** Solve the equation  $2x^{100} + x^{71} + x^{29} = 0$  over the field  $\mathbb{Z}_{11}$ .

**Problem 9.** Factor a polynomial  $p(x) = x^3 - 3x^2 + 3x - 2$  into irreducible factors over the field  $\mathbb{Z}_7$ .

**Problem 10.** Factor a polynomial  $p(x) = x^4 + x^3 - 2x^2 + 3x - 1$  into irreducible factors over the field  $\mathbb{Q}$ .

**Problem 1.** Let  $M$  be the set of all  $2 \times 2$  matrices of the form  $\begin{pmatrix} n & k \\ 0 & n \end{pmatrix}$ , where  $n$  and  $k$  are rational numbers. Under the operations of matrix addition and multiplication, does this set form a ring? Does  $M$  form a field?

The set  $M$  is closed under matrix addition, taking the negative, and matrix multiplication as

$$\begin{aligned} \begin{pmatrix} n & k \\ 0 & n \end{pmatrix} + \begin{pmatrix} n' & k' \\ 0 & n' \end{pmatrix} &= \begin{pmatrix} n+n' & k+k' \\ 0 & n+n' \end{pmatrix}, \\ -\begin{pmatrix} n & k \\ 0 & n \end{pmatrix} &= \begin{pmatrix} -n & -k \\ 0 & -n \end{pmatrix}, \\ \begin{pmatrix} n & k \\ 0 & n \end{pmatrix} \begin{pmatrix} n' & k' \\ 0 & n' \end{pmatrix} &= \begin{pmatrix} nn' & nk' + kn' \\ 0 & nn' \end{pmatrix}. \end{aligned}$$

Also, the multiplication is commutative on  $M$ . The associativity and commutativity of the addition, the associativity of the multiplication, and the distributive law hold on  $M$  since they hold for all  $2 \times 2$  matrices. Thus  $M$  is a commutative ring.

**Problem 1.** Let  $M$  be the set of all  $2 \times 2$  matrices of the form  $\begin{pmatrix} n & k \\ 0 & n \end{pmatrix}$ , where  $n$  and  $k$  are rational numbers. Under the operations of matrix addition and multiplication, does this set form a ring? Does  $M$  form a field?

The ring  $M$  is not a field since it has zero-divisors (and zero-divisors do not admit multiplicative inverses).

For example, the matrix  $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in M$  is a divisor of zero as

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

**Problem 2.** Let  $L$  be the set of the following  $2 \times 2$  matrices with entries from the field  $\mathbb{Z}_2$ :

$$A = \begin{pmatrix} [0] & [0] \\ [0] & [0] \end{pmatrix}, \quad B = \begin{pmatrix} [1] & [0] \\ [0] & [1] \end{pmatrix}, \quad C = \begin{pmatrix} [1] & [1] \\ [1] & [0] \end{pmatrix}, \quad D = \begin{pmatrix} [0] & [1] \\ [1] & [1] \end{pmatrix}.$$

Under the operations of matrix addition and multiplication, does this set form a ring? Does  $L$  form a field?

First we build the addition and multiplication tables for  $L$  (meanwhile checking that  $L$  is closed under both operations):

+		A	B	C	D
A		A	B	C	D
B		B	A	D	C
C		C	D	A	B
D		D	C	B	A

×		A	B	C	D
A		A	A	A	A
B		A	B	C	D
C		A	C	D	B
D		A	D	B	C

Analyzing these tables, we find that both operations are commutative on  $L$ ,  $A$  is the additive identity element, and  $B$  is the multiplicative identity element. Also,  $B^{-1} = B$ ,  $C^{-1} = D$ ,  $D^{-1} = C$ , and  $-X = X$  for all  $X \in L$ . The associativity of addition and multiplication as well as the distributive law hold on  $L$  since they hold for all  $2 \times 2$  matrices. Thus  $L$  is a field.



**Problem 3.** Prove that for a ring with unity, commutativity of addition follows from the other axioms.

Suppose  $R$  is a set with two operations, addition and multiplication, that satisfies all axioms of a ring with unity except, possibly, commutativity of addition. We need to show that addition is commutative anyway:  $x + y = y + x$  for all  $x, y \in R$ . Let us simplify  $(1 + 1)(x + y)$  in two different ways:

$$\begin{aligned}(1 + 1)(x + y) &= 1(x + y) + 1(x + y) = (x + y) + (x + y), \\(1 + 1)(x + y) &= (1 + 1)x + (1 + 1)y \\ &= (1x + 1x) + (1y + 1y) = (x + x) + (y + y).\end{aligned}$$

Hence  $(x + y) + (x + y) = (x + x) + (y + y)$ . It follows that  $(-x) + (x + y) + (x + y) + (-y) = (-x) + (x + x) + (y + y) + (-y)$ ,  $(-x + x) + (y + x) + (y + (-y)) = (-x + x) + (x + y) + (y + (-y))$ ,  $0 + (y + x) + 0 = 0 + (x + y) + 0 \implies y + x = x + y$ .

*Remark.* The same argument proves that for a vector space, commutativity of vector addition follows from the other axioms.

**Problem 4.** Find a direct product of cyclic groups that is isomorphic to  $G_{16}$  (multiplicative group of all invertible elements of the ring  $\mathbb{Z}_{16}$ ).

A congruence class  $[a]_{16}$  is invertible in  $\mathbb{Z}_{16}$  if and only if  $a$  is coprime with 16, that is, if  $a$  is odd. There are 8 congruence classes in  $G_{16}$ :  $[1]$ ,  $[3]$ ,  $[5]$ ,  $[7]$ ,  $[9]$ ,  $[11]$ ,  $[13]$ ,  $[15]$ .

Classification of finite abelian groups implies that  $G_{16}$  is isomorphic to  $\mathbb{Z}_8$ ,  $\mathbb{Z}_4 \times \mathbb{Z}_2$  or  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ . These three groups are distinguished by orders of their elements:  $\mathbb{Z}_8$  has elements of order 1, 2, 4 and 8;  $\mathbb{Z}_4 \times \mathbb{Z}_2$  has elements of order 1, 2 and 4;  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$  has only elements of order 1 and 2.

Let us find orders for all elements of  $G_{16}$ .

$[1]$  has order 1.

$[3]^2 = [9]$ ,  $[3]^4 = [9]^2 = [81] = [1]$ , hence  $[3]$  has order 4.

$[5]^2 = [25] = [9]$ ,  $[5]^4 = [9]^2 = [1]$ , hence  $[5]$  has order 4.

$[7]^2 = [49] = [1]$ , hence  $[7]$  has order 2.

$[9]^2 = [1]$ , hence  $[9]$  has order 2.

$[11]^2 = [-5]^2 = [5]^2 = [9]$ , hence  $[11]$  has order 4.

$[13]^2 = [-3]^2 = [9]$ , hence  $[13]$  has order 4.

$[15]^2 = [-1]^2 = [1]$ , hence  $[15]$  has order 2.

We conclude that  $G_{16} \cong \mathbb{Z}_4 \times \mathbb{Z}_2$ .

**Problem 5.** Determine the last two digits of  $303^{303}$ .

The last two digits form the remainder under division by 100. We know that  $\phi(100) = 40$ . It follows from Euler's Theorem that  $3^{40} \equiv 1 \pmod{100}$ . Then

$$[303^{303}] = [303]^{303} = [3]^{303} = [3]^{40 \cdot 7 + 23} = ([3]^{40})^7 [3]^{23} = [3]^{23}.$$

$$\text{We have } [3]^2 = [9], [3]^3 = [9][3] = [27], [3]^4 = [27][3] = [81],$$

$$[3]^5 = [81][3] = [43], [3]^6 = [43][3] = [29],$$

$$[3]^7 = [29][3] = [87], [3]^8 = [87][3] = [61],$$

$$[3]^9 = [61][3] = [83], [3]^{10} = [83][3] = [49],$$

$$[3]^{11} = [49][3] = [47], [3]^{12} = [47][3] = [41],$$

$$[3]^{13} = [41][3] = [23], [3]^{14} = [23][3] = [69],$$

$$[3]^{15} = [69][3] = [7], [3]^{16} = [7][3] = [21],$$

$$[3]^{17} = [21][3] = [63], [3]^{18} = [63][3] = [89],$$

$$[3]^{19} = [89][3] = [67], [3]^{20} = [67][3] = [1],$$

Finally,  $[3]^{23} = [3]^3 = [27]$  so that  $303^{303} = \dots 27$ .

*Remark.* It turns out that  $G_{100} \cong \mathbb{Z}_{20} \times \mathbb{Z}_2$ . Therefore the order of each element of the group  $G_{100}$  is a divisor of 20.

**Problem 5.** Determine the last two digits of  $303^{303}$ .

*Alternative solution:* The last two digits form the remainder under division by 100. First let us find the remainders under division by 25 and 4. We have  $\phi(25) = 25 - 5 = 20$  and  $\phi(4) = 4 - 2 = 2$ . It follows from Euler's Theorem that  $303^{20} \equiv 1 \pmod{25}$  and  $303^2 \equiv 1 \pmod{4}$ . Then

$$\begin{aligned} [303^{303}]_{25} &= [303]_{25}^{303} = [303]_{25}^{20 \cdot 15 + 3} = ([303]_{25}^{20})^{15} [303]_{25}^3 \\ &= [303]_{25}^3 = [3]_{25}^3 = [3^3]_{25} = [27]_{25} = [2]_{25}, \end{aligned}$$

$$\begin{aligned} [303^{303}]_4 &= [303]_4^{303} = [303]_4^{2 \cdot 151 + 1} = ([303]_4^2)^{151} [303]_4 \\ &= [303]_4 = [3]_4. \end{aligned}$$

Since  $303^{303} \equiv 2 \pmod{25}$ , the remainder of  $303^{303}$  under division by 100 is among the four numbers  $2$ ,  $27 = 2 + 25$ ,  $52 = 2 + 25 \cdot 2$ , and  $77 = 2 + 25 \cdot 3$ . We pick the one that has remainder 3 under division by 4. That's 27.

**Problem 6.** Find all integer solutions of the equation  $21x - 32y = 4$ .

An integer  $y$  is a part of an integer solution  $(x, y)$  of the equation if and only if it is a solution of the linear congruence  $-32y \equiv 4 \pmod{21}$ . Since  $-32 \equiv 10 \pmod{21}$ , this is equivalent to  $10y \equiv 4 \pmod{21}$ . Further, we can cancel the common factor 2 on both sides of the congruence (since 2 is coprime with 21):  $10y \equiv 4 \pmod{21} \iff 5y \equiv 2 \pmod{21}$ . To solve the latter linear congruence, we need to find the multiplicative inverse of 5 modulo 21. This is  $-4$  as  $-4 \cdot 5 = -20 \equiv 1 \pmod{21}$ . Hence

$$5y \equiv 2 \pmod{21} \iff y \equiv -4 \cdot 2 \equiv -8 \pmod{21}.$$

In other words,  $y = -8 + 21k$  for some  $k \in \mathbb{Z}$ . The corresponding value of  $x$  can be found from the equation:  $x = (4 + 32y)/21 = (4 + 32(-8 + 21k))/21 = -12 + 32k$  (it should be integer as well). Thus the general integer solution is  $x = -12 + 32k$ ,  $y = -8 + 21k$ , where  $k \in \mathbb{Z}$ .

**Problem 7.** Find all integer solutions of the equation  $2x + 3y + 5z = 7$ .

Let us rewrite the equation as  $2x + 3y = c(z)$ , where  $c(z) = 7 - 5z$ , and consider  $c(z)$  an integer parameter.

If  $(x, y)$  is an integer solution, then  $x$  is a solution of the congruence  $2x \equiv c(z) \pmod{3}$ . Then  $4x \equiv 2c(z) \pmod{3}$  and  $x \equiv 2c(z) \pmod{3}$ . Conversely, if  $x = 2c(z) + 3k$ , where  $k \in \mathbb{Z}$ , then we can find  $y$  from the equation,  $y = (c(z) - 2x)/3 = -c(z) - 2k$ , and it is also an integer. All this can be done for any integer value of  $z$ .

Thus the general integer solution of the original equation is

$$z = m,$$

$$x = 2c(m) + 3k = 3k - 10m + 14,$$

$$y = -c(m) - 2k = -2k + 5m - 7,$$

where  $k$  and  $m$  are arbitrary integers.

**Problem 8.** Solve the equation  $2x^{100} + x^{71} + x^{29} = 0$  over the field  $\mathbb{Z}_{11}$ .

The equation is equivalent to

$$x^{29}(2x^{71} + x^{42} + 1) = 0.$$

Hence  $x = 0$  or  $2x^{71} + x^{42} + 1 = 0$ . By Fermat's Little Theorem,  $x^{10} = 1$  for any nonzero  $x \in \mathbb{Z}_{11}$ .

Since 0 is not a solution of the equation  $2x^{71} + x^{42} + 1 = 0$ , this equation is equivalent to  $2x + x^2 + 1 = 0 \iff (x + 1)^2 = 0 \iff x = -1$ .

Thus the solutions are  $x = 0$  and  $x = 10$  (note that  $-1 \equiv 10 \pmod{11}$ ).



**Problem 9.** Factor a polynomial  $p(x) = x^3 - 3x^2 + 3x - 2$  into irreducible factors over the field  $\mathbb{Z}_7$ .

A quadratic or cubic polynomial is irreducible if and only if it has no zeros. Indeed, if such a polynomial splits into a product of two non-constant polynomials, then at least one of the factors is linear. This implies that the original polynomial has a zero.

Let us look for the zeros of  $p(x)$ :  $p(0) = -2$ ,  $p(1) = -1$ ,  $p(2) = 0$ . Hence  $p(x)$  is divisible by  $x - 2$ :

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

Now let us look for the zeros of the polynomial  $q(x) = x^2 - x + 1$ . Note that values 0 and 1 can be skipped this time. We obtain  $q(2) = 3$ ,  $q(3) = 7 \equiv 0 \pmod{7}$ . Hence  $q(x)$  is divisible by  $x - 3$ :  $x^2 - x + 1 = (x - 3)(x + 2)$ .

Thus  $x^3 - 3x^2 + 3x - 2 = (x - 2)(x - 3)(x + 2)$  over the field  $\mathbb{Z}_7$ .

**Problem 10.** Factor  $p(x) = x^4 + x^3 - 2x^2 + 3x - 1$  into irreducible factors over the field  $\mathbb{Q}$ .

Possible rational zeros of  $p$  are 1 and  $-1$ . They are not zeros. Hence  $p$  is either irreducible over  $\mathbb{Q}$  or else it is factored as

$$x^4 + x^3 - 2x^2 + 3x - 1 = (ax^2 + bx + c)(a'x^2 + b'x + c').$$

Since  $p \in \mathbb{Z}[x]$ , one can show that the factorization (if it exists) can be chosen so that all coefficients are integer.

Additionally, we can assume that  $a \geq 0$  (otherwise we could multiply each factor by  $-1$ ). Equating the corresponding

coefficients of the left-hand side and the right-hand side, we obtain  $aa' = 1$ ,  $ab' + a'b = 1$ ,  $ac' + bb' + a'c = -2$ ,

$bc' + b'c = 3$  and  $cc' = -1$ . The first and the last equations imply that  $a = a' = 1$ ,  $c = 1$  or  $-1$ , and  $c' = -c$ . Then

$b + b' = 1$  and  $bb' = -2$ , which implies  $\{b, b'\} = \{2, -1\}$ .

Finally,  $c = -1$  if  $b = 2$  and  $c = 1$  if  $b = -1$ . We can check that indeed

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