M E T U
Department of Mathematics

<table>
<tr><td colspan="2" align="center">Abstract Algebra
Final Exam</td></tr>
<tr><td>Code : Math 367
Acad. Year : 2015
Semester : Fall
Instructor : Küçüksakallı

Date : Jan 19, 2016
Time : 13:30
Duration : 120 minutes</td><td>Last Name :
Name :
Student No. :
Signature :
<hr>7 QUESTIONS ON 4 PAGES
100 TOTAL POINTS</td></tr>
</table>

1	2	3	4	5	6	7	8		

1. (25pts) For each of the following polynomials, determine whether it is an irreducible element of the indicated integral domain.

- $a(x) = 2x + 2 \in \mathbb{Z}[x]$.

  Not irreducible. Because $a(x) = 2 \cdot (x + 1)$ but 2 and $x + 1$ are not units in $\mathbb{Z}[x]$.

- $b(x) = x^2 + 2x + 4 \in \mathbb{Z}_5[x]$.

  Irreducible. Because $b(x)$ has no roots in $\mathbb{Z}_5[x]$ and $\deg(b) \leq 3$.

- $c(x) = x^3 + 4x^2 + 6x + 4 \in \mathbb{Q}[x]$.

  Not irreducible. Because $c(x) = (x + 2) \cdot (x^2 + 2x + 2)$.

- $d(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$

  Irreducible. We have $d(x + 1) = x^4 + 5x^3 + 10x^2 + 10x + 5$ and Eisenstein's criteria with $p = 5$ implies that $d(x+1)$ is irreducible in $\mathbb{Q}[x]$. As a result $d(x)$ is irreducible in $\mathbb{Q}[x]$ as well.

- $e(x) = x^5 + x + 1 \in \mathbb{Z}_2[x]$.

  Not irreducible. Because $e(x) = (x^2 + x + 1) \cdot (x^3 + x^2 + 1)$ in $\mathbb{Z}_2[x]$.

2 (18pts) Let $n \geq 2$ be an integer and $I_n = \{f \in \mathbb{Z}[x] \mid f(0) \text{ is divisible by } n\}$.

- Show that $I_n = \langle x, n \rangle$ in $\mathbb{Z}[x]$.

  Pick $f(x) \in \langle x, n \rangle$. Then $f(x) = xg(x) + nh(x)$ for some $g, h \in \mathbb{Z}[x]$. It follows that $f(0) = nh(0)$ where $h(0) \in \mathbb{Z}$. We have $n|nh(0)$ and $f(x) \in I_n$. Conversely pick $f(x) \in I_n$. Then $f(0) = nk$ for some $k \in \mathbb{Z}$. The polynomial $f(x) - nk$ is divisible by x and as a result $f(x) - nk = xg(x)$ for some $g \in \mathbb{Z}[x]$. Therefore $f(x) = xg(x) + nk$ and it is an element of $\langle x, n \rangle$.

- If I_n is a prime ideal of $\mathbb{Z}[x]$ then show that n is prime in $\mathbb{Z}$.

  Suppose that $n|ab$. It follows that $ab \in I_n$. If I_n is a prime ideal, then either $a \in I_n$ or $b \in I_n$. As a result either $a = a(0)$ is divisible by n or $b = b(0)$ is divisible by n. We conclude that n is a prime element of $\mathbb{Z}$.

- If n is prime in $\mathbb{Z}$ then show that I_n is a prime ideal of $\mathbb{Z}[x]$.

  Suppose that $f(x)g(x) \in I_n$. It follows that $f(0)g(0)$ is divisible by n. If n is a prime element in $\mathbb{Z}$, then either $f(0)$ is divisible by n or $g(0)$ is divisible by n. We conclude that $f(x) \in I_n$ or $g(x) \in I_n$. Therefore I_n is a prime ideal of $\mathbb{Z}[x]$.

3. (7pts) Show that $\mathbb{Z}[x]/\langle x^2+1 \rangle$ and $\mathbb{Z}[\sqrt{2}]$ are not isomorphic as rings.

Assume otherwise and let $f : \mathbb{Z}[x]/\langle x^2+1 \rangle \to \mathbb{Z}[\sqrt{2}]$ be an isomorphism of rings. If $\alpha = x + \langle x^2+1 \rangle$, then $-\alpha^2 = 1 + \langle x^2+1 \rangle$ is the identity element of $\mathbb{Z}[x]/\langle x^2+1 \rangle$. It follows that $f(-\alpha^2) = 1$, where 1 is the identity element of $\mathbb{Z}[\sqrt{2}]$. On the other hand, $f(-\alpha^2) = -f(\alpha)^2$ by the properties of a ring homomorphism. It follows that $f(\alpha)^2 = -1$. This is a contradiction because $f(\alpha)$ is an element of $\mathbb{Z}[\sqrt{2}]$ and its square cannot be negative.

4. (13pts) Find all maximal ideals in $\mathbb{Z}_{360}$.

The ring $R = \mathbb{Z}_{360}$ is a principal ideal ring and each ideal is of the form $I = \langle [n] \rangle$ for some integer n. Without loss of generality we can assume that $n|360$ because

$$\langle [n] \rangle = \langle [\gcd(n, 360)] \rangle.$$

Consider the map $f : \mathbb{Z}_{360} \to \mathbb{Z}_n$ given by the formula $f([x]) = [x]$. It is well defined since $n|360$. Moreover it is a homomorphism of rings. We have $\mathrm{Ker}(f) = \langle [n] \rangle$. The first isomorphism theorem implies that $R/\langle [n] \rangle \cong \mathbb{Z}_n$. The ideal $I = \langle [n] \rangle$ is maximal if and only R/I is a field. We know that $\mathbb{Z}_n$ is a field if and only if p is prime. Thus the ideals $\langle [2] \rangle, \langle [3] \rangle$ and $\langle [5] \rangle$ are the only maximal ideals of R.

5a. (6pts) What is the smallest positive integer n such that there are exactly **three** nonisomorphic Abelian groups of order n. Name the three groups.

$$n = 8, \qquad A_1 = \mathbb{Z}_8, \qquad A_2 = \mathbb{Z}_4 \times \mathbb{Z}_2, \qquad A_3 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

5b. (6pts) What is the smallest positive integer n such that there are exactly **four** nonisomorphic Abelian groups of order n. Name the four groups.

$$n = 36, \quad A_1 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3, \quad A_2 = \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3, \quad A_3 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9, \quad A_4 = \mathbb{Z}_4 \times \mathbb{Z}_9.$$

6. (13pts) Show that every Euclidean domain is a principal ideal domain.

This is Theorem 15.1.9 in your textbook

7. (12pts) Consider the binary operation $*$ on the set of integers defined by $a*b = a+b-4$.

- Show that $(\mathbb{Z}, *)$ is a group.

  The binary operation is associative because $(a*b)*c = a+b+c-8 = a*(b*c)$ for all integers a, b, c and the binary operation $+$ is associative. The identity element exists because $a * 4 = a = 4 * a$ for every $a \in \mathbb{Z}$. For each element $a \in \mathbb{Z}$, let $a^{-1} = 8 - a$. Then $a*a^{-1} = 4 = a^{-1}*a$, we conlude that each element a has an inverse. Therefore $(\mathbb{Z}, *)$ is a group.

- Show that the groups $(\mathbb{Z}, *)$ and $(\mathbb{Z}, +)$ are isomorphic.

  Define $f : \mathbb{Z} \to \mathbb{Z}$ by the formula $f(x) = x+4$. The map f is a group homomorphism from $(\mathbb{Z}, +)$ to $(\mathbb{Z}, *)$ because

$$\begin{aligned} f(a+b) &= a+b+4 \\ &= (a+4)+(b+4)-4 \\ &= f(a)+f(b)-4 \\ &= f(a)*f(b). \end{aligned}$$

  It is easy to see that f is one-to-one and onto. Thus f is an isomorphism of groups and the groups $(\mathbb{Z}, *)$ and $(\mathbb{Z}, +)$ are isomorphic.