MATH 113 – MIDTERM

Name: Answers /70

July 25, 2013

(1) (20 points) Decide whether the following statements are **T**rue or **F**alse. Circle the right answer. You don't need to justify your answers.

T **F:** $\langle \mathbb{N}, + \rangle$ is a group. no inverse

T **F:** $\mathbb{Q}^+$ is a subgroup of $\langle \mathbb{R}^*, \cdot \rangle$, where $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.

T **F:** $\langle \mathbb{Q}, + \rangle$ and $\langle \mathbb{Q}^+, \cdot \rangle$ are isomorphic. $\forall a \exists b \, (b + b = a)$ in $\mathbb{Q}$ but not $\forall a \exists b \, (b \cdot b = a)$ in $\mathbb{Q}^+$

T **F:** $\langle \mathbb{Z}_{\leq 3}[x], + \rangle$ and $\langle \mathbb{Z}^4, + \rangle$ are isomorphic, where $\mathbb{Z}_{\leq 3}[x]$ is the set of polynomials with integer coefficients and degree at most 3.

T **F:** $\mathbb{Z}_{24} \times \mathbb{Z}_5$ and $\mathbb{Z}_8 \times \mathbb{Z}_{15}$ are isomorphic. $\cong \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

T **F:** S_4 has a subgroup isomorphic to $\mathbb{Z}_8$

all $\sigma \in S_4$ have order 1, 2, 3 or 4

T **F:** Every integral domain is a field. $\mathbb{Z}$ isn't

T **F:** If R is a subring of F, both with unity, then R and F have the same characteristic.

$F = \mathbb{Z}_{12}$

$R = \{4, 8, 0\}$

T **F:** $\mathbb{Z}_{25}$ is a field.

$5 \cdot 5 = 0$ in $\mathbb{Z}_{25}$

T **F:** $\mathbb{Q}[i] = \{ai + b : a, b \in \mathbb{Q}\}$ is a sub-field of $\mathbb{C}$.

(2) (9 points)

Find all the solutions to the following equations. You don't need to justify.

(a) $3x = 7$ in $\mathbb{Z}_8$.

one solution because $\gcd(3,8)=1$

$x=5$

(b) $3x = 7$ in $\mathbb{Z}_9$.

no solution because $\gcd(3,9)=3$ and $3 \nmid 7$

(c) $8x = 4$ in $\mathbb{Z}_{12}$.

4 solutions because $d=\gcd(8,12)=4$ and $4 \mid 4$

$x=2$
$x=5$
$x=8$
$x=11$

(3) (12 points)

Consider $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ as additive groups.

(a) Prove that every element of $\frac{\mathbb{Q}}{\mathbb{Z}}$ has finite order.

(b) Find an element in $\frac{\mathbb{R}}{\mathbb{Z}}$ which has infinite order.

(c) Show that $\frac{\mathbb{R}}{\mathbb{Z}}$ and $\frac{\mathbb{R}}{\mathbb{Q}}$ are not isomorphic.

(a) Every element of $\frac{\mathbb{Q}}{\mathbb{Z}}$ is of the Form $\frac{p}{q}+\mathbb{Z}$ where $p, q \in \mathbb{Z}$, $q \neq 0$

then $\underbrace{\left(\frac{p}{q}+\mathbb{Z}\right) + \dots + \left(\frac{p}{q}+\mathbb{Z}\right)}_{q \text{ times}} = p+\mathbb{Z} = \mathbb{Z}$

identity of $\frac{\mathbb{Q}}{\mathbb{Z}}$

(b) Let $r = \pi$, e or any irrational number

then For no $n \in \mathbb{N}$ $\underbrace{r+r+\dots+r}_{n} \in \mathbb{Z}$

(c) In $\frac{\mathbb{R}}{\mathbb{Z}}$ there is an element of order 2 namely $\frac{1}{2}+\mathbb{Z}$

In $\frac{\mathbb{R}}{\mathbb{Q}}$ there is no element of order 2 because if $(a+\mathbb{Q})+(a+\mathbb{Q}) = \mathbb{Q}$ then $2a \in \mathbb{Q}$ but then $a \in \mathbb{Q}$ and $a+\mathbb{Q} = \mathbb{Q}$

the identity

(4) (10 points)
Consider the following operation on the set $\mathbb{R}^+ = \{r \in \mathbb{R} : r > 0\}$:

$$a * b = a^{\log(b)}.$$

Show that $\langle \mathbb{R}^+, \cdot, * \rangle$ is a field. (You may skip the associativity and distributivity properties. You'll get partial credit for proving parts of this.)

- We know that $(\mathbb{R}^+, \cdot)$ is an abelian group.
- $*$ is commutative because

$$a * b = a^{\log b} = e^{\log(a) \cdot \log(b)} = e^{\log(b) \cdot \log(a)}$$
$$= b^{\log(a)} = b * a$$

- $*$ has an identity, namely e (or 10 if you ~~also~~ were using base 10)

because $e * \cancel{a} = e^{\log a} = a$

$$a * e = a^{\log(e)} = a^1 = a$$

- ~~$*$~~ Every $a \neq 0_{\mathbb{R}} = 1$ has a $*$-inverse given by $e^{\frac{1}{\log(a)}}$ because

$$\cancel{a *}\ e^{\frac{1}{\log(a)}} * a = \left(e^{\frac{1}{\log(a)}}\right)^{\log(a)} = e^{\frac{\log(a)}{\log(a)}} = e$$

(5) (9 points)

Let G be an abelian group and let $H = \{(a,a,a) : a \in G\}$. Show that H is a normal subgroup of $G \times G \times G$ and that

$$\frac{G \times G \times G}{H} \cong G \times G.$$

– H is a subgroup because

- if $(a,a,a), (b,b,b) \in H$ then $(a,a,a)\cdot(b,b,b) = (ab,ab,ab) \in H$
- $1_{G\times G\times G} = (1,1,1) \in H$
- if $(a,a,a) \in H$, then $(a,a,a)^{-1} = (a^{-1}, a^{-1}, a^{-1}) \in H$

– Since G is abelian, so is $G\times G\times G$, so H is normal.

– Consider $\phi : G\times G\times G \to G\times G$ given by $\phi(a,b,c) = (ac^{-1}, bc^{-1})$

- ϕ is a homomorphism because

$$\begin{aligned}\phi(a_1,b_1,c_1)\cdot\phi(a_2b_2c_2) &= (a_1c_1^{-1}, b_1c_1^{-1})\cdot(a_2c_2^{-1}, b_2c_2^{-1}) \\ &= (a_1c_1^{-1}a_2c_2^{-1}, (b_1c_1^{-1}b_2c_2^{-1}) = \\ &= (a_1a_2(c_1c_2)^{-1}, b_1b_2(c_1c_2)^{-1}) \\ &= \phi((a_1b_1c_1)(a_2b_2c_2))\end{aligned}$$

- ϕ is onto because given $(x,y) \in G\times G$, $(x,y) = \phi(x,y,e)$
- $\ker(\phi) = H$ because

$$(a,b,c) \in \ker(H) \Leftrightarrow (ac^{-1}, bc^{-1}) = (e,e) \Leftrightarrow \begin{matrix} ac^{-1} = e \\ bc^{-1} = e \end{matrix} \Leftrightarrow \begin{matrix} a = c \\ b = c \end{matrix}$$

$$\Leftrightarrow a = b = c \Leftrightarrow (a,b,c) \in H$$

Therefore, by the fundamental theorem of homomorphism

$$\frac{G\times G\times G}{H} \cong G\times G$$

(6) (10 points)
In a field F, we say that b is a *cubic root of* a, if $b^3 = a$.
(a) Show that a^{11} is a cubic root of a for every $a \in \mathbb{Z}_{17}$.
(b) Show that if $p \equiv 2 \pmod 3$, then every element of $\mathbb{Z}_p$ has a cubic root.
(c) Show that if $p \equiv 1 \pmod 3$, the 1 has more than one cubic root in $\mathbb{Z}_p$. (Hint: you may use the fact that on any finite abelian group G, if q is prime and q divides $|G|$, then G has an element of order q.)
(d) Show that if $p \equiv 1 \pmod 3$, then some element of $\mathbb{Z}_p$ does not have a cubic root.

(a) By Fermat's little theorem $a^{16} \equiv 1 \pmod p$

So $(a^{11})^3 = a^{33} = a^{16} \cdot a^{16} \cdot a \equiv a \pmod p$

(b) By Fermat's little theorem, $a^{p-1} \equiv 1 \pmod p \quad \forall a \not\equiv 0 \pmod p$

Let $k = \frac{2p-1}{3}$. Since $p \equiv 1 \pmod 3$, we know $\frac{2p-1}{3} \in \mathbb{Z}$

So

$(a^k)^3 = a^{3k} = a^{2p-1} = a^{p-1} \cdot a^{p-1} \cdot a \equiv a \pmod p$

when $a \not\equiv 0 \pmod p$

If $a \equiv 0 \bmod p$, then $0^3 \equiv 0 \pmod p$.

In any case a^k is a cubic root of a

(c) $|\mathbb{Z}_p^*| = p-1$ and $3 \mid p-1$, so there is $a \in \mathbb{Z}_p^*$

such that ~~3 | ord~~ $\operatorname{ord}(a) = 3$

Therefore $a \neq 1$ and $a^3 = 1$

So a and 1 are both cubic roots of 1

(d) Since every element has at most one cube, and 1 has at least 2 cubic roots, Some other element must have none.

$\boxed{\text{The function } a \mapsto a^3 \text{ is not bijective}}$