Kang-Li Cheng
ksc66

Math 4330 Homework Set 1

Due Friday, Sept. 4, 2015

Keith Dennis Malott 524 255-4027 **math4330@rkd.math.cornell.edu**

TA: Gautam Gopal Krishnan 120 Malott Hall gk379@cornell.edu

Problems marked by $\boxed{\text{box}}$ or $\boxed{\star}$ are more challenging and may be turned in anytime during the semester. There will be several such problems assigned during the term. Please turn in *separately* from routine assignments – if incorrect or incomplete, they will be returned to you to complete correctly. Final deadline is Monday, Nov. 30, no exceptions.

Do the following problems from the handouts:

Fields 1

Fields 5

Fields 6

Fields 10

Fields 11

Fields 12

Fields 13

Fields 14

Fields 17

66/90

1. Construct field F with 9 elements

$F_9 = F_3[\beta]$ Consider $\mathbb{Z}_3$ and the quadratic polynomial $f(x) = x^2+1$.

Multiplication table on back.

10

+	1	2	x	x+1	x+2	2x	2x+1	2x+2
1	2	0	x+1	x+2	x	2x+1	2x+2	2x
2	0	1	x+2	x	x+1	2x+2	2x	2x+1
x	x+1	x+2	2x	2x+1	2x+2	0	1	2
x+1	x+2	x	2x+1	2x+2	2x	1	2	0
x+2	x	x+1	2x+2	2x	2x+1	2	0	1
2x	2x+1	2x+2	0	1	2	x	x+1	x+2
2x+1	2x+2	2x	1	2	0	x+1	x+2	x
2x+2	2x	2x+1	2	0	1	x+2	x	x+1

5. $\sigma: F_1 \to F_2$ and preserves addition, multiplication, and is nontrivial, then

2 σ is a homomorphism because such a map is surjective and injective.

$\sigma(a) = \sigma(a) \leftrightarrow a = a$ $\sigma(1) = 1$.

X $\sigma: \mathbb{R} \to \mathbb{C}$

$\alpha \mapsto \alpha$

is not surjective.

Show any homomorphism between 2 fields is one to one.

6. $\sigma(a) = \sigma(b) \to a = b$

We know that ker(σ) is an ideal and ker(σ) is either all of F or empty.

Then σ is 1 to 1. If ker(σ) is all of F, then σ is the zero map.

7

Use only what has been done in class.

10. Let $\sigma: F_1 \to F_2$ be a homomorphism, F_1 and F_2 are fields.

Show σ induces an isomorphism between their prime subfields, and characteristics of F_1 and F_2 are the same.

4 Suppose F is a field and $\phi: \mathbb{Z} \to F$ is an injective map. So $\sigma: \mathbb{Q} \to F$ is an induced map. Since $\phi: \mathbb{Z} \to F$ factors through all prime fields of F, we know

$F' = \mathbb{Q}$ or $F' = F_p$.

In the case that $\mathbb{Z} \to F$ is not injective, we have a map $F_p \to F$

Incomplete proof.

$\times$	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
1	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$x+2$
$x+1$	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$x+2$	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
$2x$	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
$2x+2$	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

11. Frobenius map is a homomorphism
We verify the 3 properties from definition of homomorphism.

$\sigma: F \to F,\ \sigma(x) = x^p$

$$\underline{\sigma(a+b)} = (a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i}$$

10 For $1 \leq i \leq p-1$ $\binom{p}{i} = \dfrac{p!}{i!(p-i)!} \to \underbrace{\sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} = 0}_{\text{Mention } p \text{ divide } \binom{p}{i}.}$

So $(a+b)^p = a^p + b^p = \sigma(a) + \sigma(b)$

$$\underline{\sigma(1) = 1^p = 1}$$

$$\sigma(a \cdot b) = (ab)^p = a^p b^p = \sigma(a) \cdot \sigma(b)$$

Multiplication is associative and commutative.

12. A field is called perfect if it has characteristic 0 or Frobenius homomorphism is an automorphism.

9 Any finite field is perfect.

Why is char $F \neq 0$?

Proof: Let F be a finite field and $\underline{\text{char}(F) = p}$. Now $\sigma: F \to F$ is an injection of a finite set into a finite set so σ must be a bijection $\to$ σ is surjective. $\square$

13. $Q[\sqrt{2}]$ - set of all numbers in $\mathbb{C}$ that can be written in the form $a+b\sqrt{2}$, $a,b \in Q$.

a) $Q[\sqrt{2}]$ is the smallest subfield of C which contains $\sqrt{2}$.

$Q[\sqrt{2}]$ is a field from the result of "Fields 14."

Any field F that contains Q and $\sqrt{2}$ contains $b\sqrt{2}$ and $a+b\sqrt{2}$, $a,b \in Q$, by definition of a field. Therefore $Q(\sqrt{2}) \subseteq F$.

$Q(\sqrt{2})$ is strictly larger than Q.

b) Describe all $\operatorname{aut}(Q(\sqrt{2}))$

The only two automorphisms are $\sigma : Q(\sqrt{2}) \to Q(\sqrt{2})$ mapping to $\{a+b\sqrt{2}\}$ and $\{a-b\sqrt{2}\}$.

another mapping to

7

Why?

c) $Q[\sqrt{d}]$ is the smallest subfield of C which contains $\sqrt{d}$ except when d is a perfect square.

The smallest subfield is Q when d is a perfect square.

$\sqrt{d} \in Q$.

14. Show $Q(\sqrt{p}) = \{ a + b\sqrt{p} \mid a, b \in Q \}$ is a subfield of R.

We verify that $Q(\sqrt{p})$ satisfies the definition.

1) $0 + 0\sqrt{p} \in Q(\sqrt{p})$

2) $a + b\sqrt{p},\ c + d\sqrt{p} \in Q(\sqrt{p})$, $a + b\sqrt{p} + c + d\sqrt{p} = a + c + (b + d)\sqrt{p} \in Q(\sqrt{p})$.

3) $(a + b\sqrt{p})(c + b\sqrt{b}) = ac + (ad + bc)\sqrt{b} + bdp \in Q(\sqrt{b})$

4) $-(a + b\sqrt{b}) = -a + (-b)\sqrt{p} \in Q(\sqrt{p})$

5) $(a + b\sqrt{p})^{-1} = \left(\frac{a}{a^2 - pb^2}\right) + \left(\frac{-b}{a^2 - pb^2}\right)\sqrt{p} \in Q(\sqrt{p})$

7

What is $Q(\sqrt{2}) \cap Q(\sqrt{p})$, where p is any odd prime?

$a + b\sqrt{2}$ The intersection will be just Q.

$a + b\sqrt{p}$ Prove it.

17. a) Any automorphism of $\mathbb{Q}$ is Trivial.

Let ϕ be an automorphism of $\mathbb{Q}$, $\phi \in Aut(\mathbb{Q})$. Let $p/q \in \mathbb{Q}$. We write $\frac{p}{q}$ as $\frac{\sum_{i=1}^{p} 1_i}{\sum_{i=1}^{q} 1_i}$

Then $\phi\left(p/q\right) = \frac{p\,\phi(1)}{q\,\phi(1)} = p/q$. So any automorphism of $\mathbb{Q}$ must be the trivial one.

b) Any automorphism of $\mathbb{R}$ is trivial

Let ϕ be an automorphism of $\mathbb{R}$, $\phi \in Aut(\mathbb{R})$.

Let $x \in \mathbb{R}$, $x > 0$. Then $\exists\ y \in \mathbb{R}$, $y = x^2$. $\phi(x) = \phi(y^2) > 0$.

Suppose $m < n$, so $n - m > 0$. Then $\phi(n) - \phi(m) = \phi(n-m) > 0$ and $\phi(m) < \phi(n)$.

1° This shows that ϕ must be strictly increasing.

Let $y, z \in \mathbb{Q}$ s.t. $y < x < z$. Then $y < \phi(x) < z \rightarrow \phi(x) = x$ because we can find $z - y$ small enough.

Any order preserving aut must be the identity?