

Math 392 Homework 5 = Midterm review questions SOLUTIONS

1. Define the function $f : \mathbb{Z}[i] \rightarrow \mathbb{Z}_2$ by $f(x + iy) = [x + y]$ for all $x, y \in \mathbb{Z}$.

(i) Prove carefully that f is a ring homomorphism.

(ii) What is the *kernel* of f ?

(iii) Is f any of: onto, 1-1, isomorphism?

(iv) Define $g : \mathbb{Z}[i] \rightarrow \mathbb{Z}_3$ by $g(x + iy) = [x + y]$ for all $x, y \in \mathbb{Z}$. Is g a ring homomorphism? Explain your answer carefully.

(i) *First, $f(1) = [1]$. Second, $f((x + iy) + (u + iv)) = f((x + u) + i(y + v)) = [x + u + y + v]$ and $f(x + iy) + f(u + iv) = [x + y] + [u + v] = [x + y + u + v]$. So it is additive. Finally, $f((x + iy)(u + iv)) = f((xu - yv) + i(xv + yu)) = [xu - yv + xv + yu] = [xu + xv + yu + yv]$ and $f(x + iy)f(u + iv) = [x + y][u + v] = [xu + xv + yu + yv]$. So it is multiplicative. Hence it is a ring homomorphism.*

(ii) *$\ker f$ is the set of all $x + iy$ such that $x + y$ is even. Hence it is the set of all $x + iy$ such that either x, y are both odd integers or x, y are both even integers. That is a good enough answer.*

But you can do a little better: $\mathbb{Z}[i]$ is a Euclidean domain so every ideal is principal. So we should be able to write $\ker f = (z)$ for some Gaussian integer z . I claim that $\ker f = (1 + i)$. To prove this note that $1 + i$ is in $\ker f$. Now consider $(1 + i)(a + ib) = (a - b) + i(a + b)$. Given $x + iy$ with x, y both odd or both even, set $a = (x + y)/2$ and $b = (y - x)/2$. Note that a, b are definitely both integers by the assumption on x, y . Hence $a + ib \in \mathbb{Z}[i]$. Hence, $(a - b) + i(a + b) = x + iy$ belongs to $(1 + i)$. This shows that $(1 + i) = \ker f$.

(iii) *f is onto but not 1-1 so it is not an isomorphism.*

(iv) *NO! e.g. $g(i^2) = g(-1) = [-1]$ while $g(i)^2 = [1]^2 = [1]$. So it is not multiplicative.*

2. (i) What is an *ideal*?

(ii) Prove that the kernel of a ring homomorphism is an ideal.

(iii) Which of the following subsets of \mathbb{Z}_{15} are ideals?

(a) $\{[0]\}$.

(b) $\{[1]\}$.

(c) $\{[0], [1], [2], \dots, [14]\}$.

(d) $\{[0], [5], [10]\}$.

(e) $\{[0], [4], [8], [12]\}$.

(iv) Let I be an ideal of a ring R . Prove that $I = R$ if and only if I contains a unit of R .

(i) *An ideal of R is a non-empty subset of R such that $a, b \in I \Rightarrow a + b \in I$ and $a \in I, b \in R \Rightarrow ab \in I$.*

(ii) *Let $f : R \rightarrow S$ be a ring homomorphism. Remember $\ker f = \{a \in R \mid f(a) = 0\}$. Obviously, $f(0) = 0$ so $0 \in \ker f$ so $\ker f$ is non-empty. Suppose $a, b \in \ker f$, i.e. $f(a) = f(b) = 0$. Then, $f(a + b) = f(a) + f(b) = 0 + 0 = 0$, so $a + b \in \ker f$. Finally suppose $a \in \ker f$ and $b \in R$. Then, $f(ab) = f(a)f(b) = 0f(b) = 0$, so $ab \in \ker f$. Hence $\ker f$ is an ideal.*

(iii) (a) YES (b) NO (c) YES (d) YES (e) NO.

3. (i) I want to define a function $f : \mathbb{Z}_7 \rightarrow \mathbb{Z}_6$ by setting $f(n + (7)) = n + (6)$ for all $n \in \mathbb{Z}$. Explain why I cannot do this.

(ii) Instead, define $f : \mathbb{Z}_{42} \rightarrow \mathbb{Z}_6$ by setting $f(n + (42)) = n + (6)$ for all $n \in \mathbb{Z}$. Explain why I can do this.

(i) *This is not well-defined. For instance, $1 + (7) = 8 + (7)$. If you choose the former representation, the rule for f gives the output $1 + (6)$. If you choose the latter representation the rule for f gives the output $8 + (6) = 2 + (6) \neq 1 + (6)$.*

(ii) *We just need to check that it is well-defined. Suppose $n + (42) = n' + (42)$, i.e. $42|(n - n')$. Then since $6|42$ we get that $6|(n - n')$. Hence $n + (6) = n' + (6)$. So the rule is well-defined independent of the choice of representatives.*

4. Let $R = \mathbb{Z}_2[x]/(x^3 + x + 1)$.

(i) How many elements does R have? List them.

(ii) Is R an integral domain and/or a field? Explain.

(iii) Calculate the multiplicative inverse of the elements $x + (x^3 + x + 1)$ and $x^2 + (x^3 + x + 1)$ in R .

(i) *8 elements. They are*

$$\bar{0}, \bar{1}, \bar{x}, \bar{x} + \bar{1}, \bar{x}^2, \bar{x}^2 + \bar{1}, \bar{x}^2 + \bar{x}, \bar{x}^2 + \bar{x} + \bar{1}.$$

(ii) *Note $x^3 + x + 1$ has no roots in \mathbb{Z}_2 . Hence since it is a cubic it is irreducible. Hence R is a field and an integral domain.*

(iii) *Euclidean algorithm. First:*

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

Reducing modulo $x^3 + x + 1$ gives $0 = x(x^2 + 1) + 1$. Hence, $\bar{x}^{-1} = \overline{x^2 + 1}$.

Second:

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

Then

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

Hence,

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

Reducing modulo $x^3 + x + 1$ gives $\bar{1} = \bar{x}^2(\bar{1} + \bar{x} + \bar{x}^2)$. Hence the inverse of \bar{x}^2 is $\bar{1} + \bar{x} + \bar{x}^2$.

5. Suppose F is a field and $f(x) \in F[x]$.

(i) What is a *splitting field* for $f(x)$ over F ?

(ii) Is $\mathbb{Q}[\sqrt{2} + \sqrt{3}] \subset \mathbb{R}$ a splitting field for the polynomial $(x^2 - 2)(x^2 - 3)$ over \mathbb{Q} ? Explain.

(iii) Show that the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over \mathbb{Q} is $(x^4 - 10x^2 + 1)$.

(iii) Use the isomorphism theorem to prove that $\mathbb{Q}[x]/(x^4 - 10x^2 + 1) \cong \mathbb{Q}[\sqrt{2} + \sqrt{3}]$.

(iv) Construct a splitting field for the polynomial $(x^2 - 2)(x^2 - 3)$ over \mathbb{Z}_7 .

(i) *It means a field extension K of F such that $f(x)$ factorizes as a product of linear factors in $K[x]$ but $f(x)$ does not factorize as a product of linear factors in $L[x]$ for any field L with $F \subseteq L \subsetneq K$.*

(ii) To get a splitting field, we have to adjoin all the roots of the polynomial. So $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ is a splitting field. We need to show that $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$. Obviously $\sqrt{2} + \sqrt{3} \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ so $\mathbb{Q}[\sqrt{2} + \sqrt{3}] \subseteq \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Conversely, we need to show that $\sqrt{2}$ and $\sqrt{3}$ both belong to $\mathbb{Q}[\sqrt{2} + \sqrt{3}]$. Well,

$$\frac{1}{2}(\sqrt{2} + \sqrt{3})^3 - \frac{9}{2}(\sqrt{2} + \sqrt{3}) = \frac{1}{2}(2\sqrt{2} + 6\sqrt{3} + 9\sqrt{2} + 3\sqrt{3} - 9\sqrt{2} - 9\sqrt{3}) = \sqrt{2}.$$

This shows that $\sqrt{2}$ belongs to $\mathbb{Q}[\sqrt{2} + \sqrt{3}]$, then you get at once that $\sqrt{3}$ does too. Hence, $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$ and it is the splitting field.

(iii) Note that

$$\begin{aligned}(\sqrt{2} + \sqrt{3})^0 &= 1, \\(\sqrt{2} + \sqrt{3})^1 &= \sqrt{2} + \sqrt{3}, \\(\sqrt{2} + \sqrt{3})^2 &= 5 + 2\sqrt{6}, \\(\sqrt{2} + \sqrt{3})^3 &= 9\sqrt{2} + 11\sqrt{3}, \\(\sqrt{2} + \sqrt{3})^4 &= 49 + 20\sqrt{6}.\end{aligned}$$

Hence $(\sqrt{2} + \sqrt{3})^4 - 10(\sqrt{2} + \sqrt{3})^2 + 1 = 49 + 20\sqrt{6} - 50 - 20\sqrt{6} + 1 = 0$. So $\sqrt{2} + \sqrt{3}$ is a root of $x^4 - 10x^2 + 1$. Now suppose that $x^4 - 10x^2 + 1$ is NOT the minimal polynomial. Then there is a monic polynomial $m(x)$ of degree < 4 with $\sqrt{2} + \sqrt{3}$ a root.

Could $m(x)$ be of degree 1? NO because $\sqrt{2} + \sqrt{3}$ is not rational.

Could $m(x)$ be of degree 2? Well then it would be $x^2 + ax + b$ and $(\sqrt{2} + \sqrt{3})^2 + a(\sqrt{2} + \sqrt{3}) + b = 0$ would imply that $5 + b + 2\sqrt{6} + a\sqrt{2} + a\sqrt{3} = 0$ hence equating coefficients that $a = 0, b = -5 - 2\sqrt{6}$ which is NOT rational. So NO.

Finally could $m(x)$ be of degree 3? In that case it would be $x^3 + ax^2 + bx + c$ and $(\sqrt{2} + \sqrt{3})^3 + a(\sqrt{2} + \sqrt{3})^2 + b(\sqrt{2} + \sqrt{3}) + c = 9\sqrt{2} + 11\sqrt{3} + 5a + 2a\sqrt{6} + b\sqrt{2} + b\sqrt{3} + c = 3a\sqrt{6} + (b+9)\sqrt{2} + (b+11)\sqrt{3} + (c+5a) = 0$. Equating coefficients gives $b+9 = b+11 = 0$ a contradiction. So NO.

Therefore our polynomial of degree 4 must be the minimal polynomial.

(iii) Consider the evaluation homomorphism $\mathbb{Q}[x] \rightarrow \mathbb{Q}[\sqrt{2} + \sqrt{3}], f(x) \mapsto f(\sqrt{2} + \sqrt{3})$. It is onto and the kernel is $(x^4 - 10x^2 + 1)$ since that is the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over \mathbb{Q} . Hence by the isomorphism theorem, $\mathbb{Q}[x]/(x^4 - 10x^2 + 1) \cong \mathbb{Q}[\sqrt{2} + \sqrt{3}]$.

(iv) Note $(x^2 - 2) = (x - 3)(x + 3)$ in $\mathbb{Z}_7[x]$, so to get a splitting field for $(x^2 - 2)(x^2 - 3)$ over \mathbb{Z}_7 we just need a splitting field for $x^2 - 3$. But $x^2 - 3$ is irreducible over \mathbb{Z}_7 , so $\mathbb{Z}_7[x]/(x^2 - 3)$ is a field. It consists of all polynomials of the form $a + b\bar{x}$ for $a, b \in \mathbb{Z}_7$, and $\bar{x}^2 = 3$. The constant ones give a subfield \mathbb{Z}_7 . of $\mathbb{Z}_7[x]/(x^2 - 3)$, and $\mathbb{Z}_7[x]/(x^2 - 3)$ IS the splitting field we were after.