Homework 2.

(1) Let F be a field. Show that a polynomial $p(x) \in F[x]$ of degree n has at most n roots in F.

Pf Let us prove the above by induction. First, suppose $p(x)$ has degree 1. Then $p(x) = a_0 + a_1 x = (x + a_0 a_1^{-1}) a_1$ where $a_0, a_1 \in F$ and $a_1 \neq 0$, and has only one root, $-a_0 a_1^{-1}$. ✓

Now suppose that polynomials in $F[x]$ of degree $n-1$ have at most $n-1$ roots in F, and consider $p(x) \in F[x]$ of degree n with some root $\alpha \in F$, i.e. $p(\alpha) = 0$. (If $p(x)$ has no root, then we are done) Then by Division with Remainder, $p(x) = (x-\alpha) q(x)$, where $q(x) \in F[x]$ of degree $n-1$. Then the roots of $p(x)$ are α and the roots of $q(x)$. There cannot be any other root because $\beta - \alpha \neq 0$ and $q(\beta) \neq 0$ for any $\beta \in F$ different from α and the roots of $q(x)$. Now we know that $q(x)$ has at most $n-1$ roots, so $p(x) = (x-\alpha) q(x)$ has at most n roots, namely, those of $q(x)$ and α!

why can you do this?

4

We can do this because the coeff ring F is a field.

Thus by induction, a polynomial $p(x) \in F[x]$ of degree n has at most n roots in F.

$\square$

(2) Let R be a ring. The whole ring R is an ideal of itself, called the unit ideal. Show that if an ideal I contains a unit, then it is the unit ideal.

Pf Let $u \in I$ denote this unit. By definition $u^{-1} \in R$, so $u \cdot u^{-1} = 1 \in I$. Then $1 \cdot r \in I$ for all $r \in R$, meaning that $I \supset 1 \cdot R = R$. We know that $I \subset R$. Thus $I = R$. Therefore, if an ideal I contains a unit, then it is the unit ideal. ✓

5

$\square$

(3) Let R be a ring and let $a, b \in R$. Show that $(a) = (b)$ if and only if $a = ub$ for some unit $u \in R$.

Pf ($\Rightarrow$) Suppose $(a) = (b)$, then $a \in (b)$, so $a = b \cdot r$ for some $r \in R$. Similarly, $b \in (a)$, so $b = a \cdot s$ for some $s \in R$. Then $a = (a \cdot s) \cdot r = asr$, so $sr = 1$. Then r has an inverse $r^{-1} = s \in R$. So $a = r \cdot b$

5 where $r \in R$ is a unit.

($\Leftarrow$) Suppose $a = ub$ for some unit $u \in R$. Then

$$(a) = aR = (ub)R \underset{\substack{\uparrow \\ \text{commutative}}}{=} (bu)R \underset{\substack{\uparrow \\ \text{associative}}}{=} b(uR) \underset{\substack{\uparrow \\ \text{unit ideal is the} \\ \text{whole ring (Problem \#2)}}}{=} bR = (b)$$

Therefore, $(a) = (b) \iff a = ub$ for some unit $u \in R$. $\square$

(4) Every non-zero ring has at least two ideals, the zero ideal and the unit ideal. Show that a non-zero ring is a field if and only if it has no other ideals.

Pf ($\Rightarrow$) Let I be a nonzero ideal of a field F, and let α be a nonzero element of I. Since F is a field, α has an inverse $\alpha^{-1} \in F$, i.e. α is a unit. Then I contains a unit, α, and hence I is the unit

5 ideal. ($\because$ If an ideal contains a unit, then it is the unit ideal, from Problem #2). So F has no other ideals besides (0) and (1).

($\Leftarrow$) Suppose that a non-zero ring R has no other ideals besides (0) and (1). Choose any nonzero element $\alpha \in R$, then $(\alpha) = (1)$ because $(\alpha) \neq (0)$. Then $1 \in (\alpha)$, so $1 = \alpha \cdot r$ for some $r \in R$, i.e. α has an inverse $\alpha^{-1} = r \in R$. Now α was an arbitrary nonzero element of R, so every nonzero element of R has a multiplicative inverse, i.e. R is a field. $\square$

(5) Show that the characteristic of a field is a prime number.

Pf Let F denote a field and φ the unique homomorphism $\mathbb{Z} \longrightarrow F$ defined by $\varphi(m) = 1 + \cdots + 1$ (m terms). Then $\ker \varphi = n\mathbb{Z}$ for some $n \in \mathbb{N}$ ($\because$ kernel is a subgroup). Suppose n is not prime, i.e. suppose $a \in \mathbb{N}$ divides n, $a \neq 1$ and $a \neq n$. Then $\varphi(n) = \varphi(a \cdot \frac{n}{a}) = \varphi(a)\varphi(\frac{n}{a})$. And since neither a nor $\frac{n}{a}$ is in the kernel ($n\mathbb{Z}$) neither $\varphi(a)$ nor $\varphi(n/a)$ is zero. Also, since $\varphi(a), \varphi(n/a) \in F$ a field, they have inverses $(\varphi(a))^{-1}$ and $(\varphi(n/a))^{-1}$, respectively. So $\varphi(a)\varphi(n/a)$ has inverse $(\varphi(n/a))^{-1}(\varphi(a))^{-1}$, meaning that $\varphi(a)\varphi(n/a) \neq 0$. But $\varphi(a)\varphi(n/a) = \varphi(n) = 0$, a contradiction. Thus, n is a prime number, and the characteristic of a field is a prime number. ✓

where $\frac{n}{a} \in \mathbb{Z}$

5

$\square$

(6) Ch.11: 3.12. Let I and J be ideals of a ring R. Prove that the set $I+J$ of elements of the form $x+y$, with x in I and y in J, is an ideal. This ideal is called the sum of the ideals I and J.

Pf Suppose $z, z' \in I+J$. Then $z = x+y$ and $z' = x'+y'$ for some $x, x' \in I$ and $y, y' \in J$. Then $z+z' = x+x'+y+y'$. We know that $x+x' \in I$ and $y+y' \in J$, so

$$z+z' = (x+x')+(y+y') \in I+J, \checkmark$$

hence $I+J$ is closed under addition.

Now consider the same $z = x+y \in I+J$ and take any $r \in R$. Then $rz = r(x+y) = rx+ry$ ($\because$ distributive law). We know that $rx \in I$ and $ry \in J$, so $rz = rx+ry \in I+J$.

Therefore, $I+J$ is an ideal. ✓

5

$\square$

(7) Ch. 11. 4.3 Identify the following rings.

(a) $\mathbb{Z}[x]/(x^2-3,\ 2x+4)$.

Sol. Let us consider the ideal $(x^2-3,\ 2x+4)$. We see that

5

$$2(x^2-3) + (2-x)(2x+4) = 2x^2-6+(4x+8-2x^2-4x) = 2$$

So $2 \in (x^2-3,\ 2x+4)$, and hence $(x^2-3,\ 2x+4) = (x^2+1,\ 2)$.

Then

$$\mathbb{Z}[x]/(x^2-3,\ 2x+4) \cong \mathbb{Z}[x]/(x^2+1,\ 2)$$
$$\cong \left(\mathbb{Z}[x]/(2)\right)/(x^2+1)$$
$$\cong \mathbb{F}_2[x]/x^2+1$$
$$\cong \mathbb{F}_2[i] \checkmark$$

which has four elements $0,\ 1,\ i,\ 1+i$

(b) $\mathbb{Z}[i]/(2+i) \cong \left(\mathbb{Z}[x]/(x^2+1)\right)/(2+x)$

$$\cong \mathbb{Z}[x]/(x^2+1,\ x+2)$$

we see that $(2-x)(x+2)+(x^2+1) = 5$, so $5 \in (x^2+1,\ x+2)$ also.

Then

$$\mathbb{Z}[i]/(2+i) \cong \mathbb{Z}[x]/(x+2,\ 5) \checkmark$$
$$\cong \left(\mathbb{Z}[x]/(x+2)\right)/(5)$$
$$\cong \mathbb{Z}/(5)$$
$$\cong \mathbb{F}_5 \checkmark$$

(continued)

(c) $\mathbb{Z}[x]/(6, 2x-1)$.

We see that $6\cdot x - 3(2x-1) = 3$, so

$3 \in (6, 2x-1)$ also.

Hence $(6, 2x-1) = (3, 2x+2)$, and thus

$$\mathbb{Z}[x]/(6, 2x-1) \cong \mathbb{Z}[x]/(3, 2x+2)$$
$$\cong (\mathbb{Z}[x]/(3))/(2x+2)$$
$$\cong \mathbb{Z}_3[x]/(2x+2)$$
$$\cong \mathbb{Z}_3[x]/(-(x+1))$$
$$\cong \mathbb{F}_3$$

(d) $\mathbb{Z}[x]/(2x^2-4, 4x-5)$

First, $-8(2x^2-4)+(4x+5)(4x-5) = 7 \in (2x^2-4, 4x-5)$.

So $(2x^2-4, 4x-5) = (4x+2, 7)$.

Then $\mathbb{Z}[x]/(2x^2-4, 4x-5) \cong \mathbb{Z}[x]/(4x+2, 7)$

Since $2 \in \mathbb{Z}_7$ is a unit

$(4x+2) = (8x+4) = (x+4)$

$$\cong (\mathbb{Z}[x]/(7))/(4x+2)$$

So $\mathbb{F}_7[x]/(4x+2) = \mathbb{F}_7[x]/(x+4) \cong \mathbb{F}_7$

The last iso. is via eval at -4.

$$\cong \underline{\mathbb{F}_7[x]/(4x+2)}$$
$$\cong \cdots ?$$

(e) $\mathbb{Z}[x]/(x^2+3, 5) \cong (\mathbb{Z}[x]/(5))/(x^2+3)$

$$\cong \mathbb{F}_5[x]/(x^2+3)$$
$$\cong \mathbb{F}_5[x]/(x^2-2)$$
$$\cong \mathbb{F}_5[\sqrt{2}]$$

(8) Ch. 11 4.4 Are the rings $\mathbb{Z}[x]/(x^2+7)$ and $\mathbb{Z}[x]/(2x^2+7)$ isomorphic?

Sol No.

Pf We know that $\mathbb{Z}[x]/(x^2+7) \cong \mathbb{Z}[\sqrt{7}]$. Now consider a homomorphism

$$\varphi : \mathbb{Z}[x]/(2x^2+7) \longrightarrow \mathbb{Z}[\sqrt{7}].$$

Then φ must send 0 to 0 and 1 to 1, and x to some $a+b\sqrt{7} \in \mathbb{Z}[\sqrt{7}]$ such that

5

$$\varphi(2x^2+7) = \varphi(2)(\varphi(x))^2 + \varphi(7) = 0$$

But $2(a+b\sqrt{7})^2+7 = 2(a^2+2ab\sqrt{7}+7b^2)+7$

$$= 2a^2+14b^2+7+2ab\sqrt{7}$$

which cannot equal zero with $a, b \in \mathbb{Z}$ because $2a^2+14b^2+7$ is a positive integer while $2ab\sqrt{7}$ is either zero or non-integer (irrational.) ✓ $\square$

(9) Ch. 11: 5.2 Let a be an element of a ring R. If we adjoin an element α with the relation $\alpha = a$, we expect to get a ring isomorphic to R. Prove that this is true.

2

Pf

By the ~~first~~ Isomorphism Theorem, we have the new ring $R' = R[\alpha]$ with kernel $(\alpha - a) \cong R[\alpha]/(\alpha - a)$

kernel of what map? $\overset{?}{\cong} R.$ $\square$

Consider the map $R[x] \xrightarrow{\varphi} R$ which is identity on R and sends x to α. Then $x-\alpha \in \operatorname{Ker}\varphi$. So $(x-\alpha) \subset \operatorname{Ker}\varphi$. Suppose $p(x) \in \operatorname{Ker}(\varphi)$. Then, as $(x-\alpha)$ is monic, we can write

$$p(x) = (x-\alpha)q(x) + r \quad , r \in R$$

By substituting $x = \alpha$, we get $r=0$. So $p(x) \in \cancel{\text{Ker}}\ (x-\alpha)$.

Thus $\operatorname{Ker}\varphi = (x-\alpha)$. Since φ is surjective, first iso. thm gives $R[x]/(x-\alpha) \cong R$