Abstract Algebra - Hw #10 Solns

Joe Cutrone

B1 1. p.278 #4

a) Just prove general statement: Let $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, $b = p_1^{\beta_1} \cdots p_n^{\beta_n}$, $c = p_1^{\gamma_1} \cdots p_n^{\gamma_n}$ (where some indices can be zero)

$a | bc \Rightarrow \alpha_i \le \beta_i + \gamma_i$

$\frac{a}{(a,b)} \Big| c = p_1^{\alpha_1 - \min\{\alpha_1 - \beta_1\}} \cdots p_n^{\alpha_n - \min\{\alpha_n - \beta_n\}}$ iff $\alpha_i - \min\{\alpha_i, \beta_i\} \le \gamma_i$

b) Let $a, b \in \mathbb{Z} - \{0\}$, $ax + by = N$. This is the same as finding all solutions to $ax \equiv N \bmod b$

Suppose (x_0, y_0) is a solution. Assume $g = (a,b) | N$ (else no solutions)

multiply $ax + by = N$ by N/g: $\frac{ax_0N}{g} + \frac{by_0N}{g} = N$

$\therefore x \equiv \frac{x_0 N}{g} \bmod y$ is a solution to $ax \equiv N \bmod y$

Linear Equation Thm says all other solutions to $ax + by = N$ are found by substituting in all $k \in \mathbb{Z}$ into

$(x_0 + k\frac{b}{g},\ y_0 - k\frac{a}{g})$

p.278 #7 $a = 85$, $b = 1 + 13i$ in $\mathbb{Z}[i]$

$\frac{85}{1+13i} \cdot \frac{(1-13i)}{(1-13i)} = \frac{1}{2} - \frac{13}{2}i$ choosing closest integers, $q = 0 - 6i$

$\therefore r = 85 + (1+13i)(6i) = 7 + 6i$

$\frac{1+13i}{7+6i} \cdot \frac{(7-6i)}{(7-6i)} = 1 + i \in \mathbb{Z}[i]$ $\therefore r = 0$ $\therefore (85, 1+13i) = \underline{\underline{(7+6i)}}$

For $a = 47 - 13i$, $b = 53 + 56i$:

repeat above procedure to get $q = 0 + i,\ 1 + i,\ i$

$\therefore$ finally $(a,b) = \underline{\underline{(-22 - 7i)}}$

p. 278 #9: Let $R = \mathbb{Z}[\sqrt{2}]$. Define $N: R^{\times} \to \mathbb{Z}$ by $x \mapsto a^2 - 2b^2$ if $x = a + b\sqrt{2}$

Show if $a | b$, $N(a) \le N(b)$. This can be done directly, as well as $N(xy) = N(x)N(y)$.

To show $\exists q, r$ s.t. $a = bq + r$ & either $N(r) = 0$ or $N(r) < N(b)$,

rewrite equation: $r = a - bq \Rightarrow \frac{r}{b} = (\frac{a}{b}) - q$

write $a/b := s + t\sqrt{2}$, $s, t \in \mathbb{Q}$

if $s, t \in \mathbb{Z}$, $a/b \in R$ so set $q = a/b$ and $r = 0$

else find $q \in R$, $q = x + y\sqrt{2}$ such that $N(q - a/b) < 1$

ie $N((x + y\sqrt{2}) - (s + t\sqrt{2})) < 1$ ie $|(x-s)^2 - 2(y-t)^2| < 1$

Take x, y integers closest to r & s respectfully $\therefore |s - x| \le 1/2$, $|t - y| \le \frac{1}{2}$

$\therefore |(x-s)^2 - 2(y-t)^2| \le \frac{1}{4} + \frac{2}{4} = \frac{3}{4} < 1$

$\therefore$ choose $q = x + y\sqrt{2} \in R$ and $N(a/b - q) < 1$ so $N(r) < N(b)$

Abstract Algebra Hw #10 Solns

Joe Cutrone

$\therefore N$ is Euclidean Norm in $\mathbb{Z}[\sqrt{2}]$ $\therefore R$ is ED

*Note: in general, $\mathbb{Z}[\sqrt{m}]$ is ED when $|m| \leq 2$

2. p 283 #5 Let $R = \mathbb{Z}[\sqrt{-5}]$. Define ideals $I_2 = (2, 1+\sqrt{-5})$, $I_3 = (3, 2+\sqrt{-5})$, $I_3' = (3, 2-\sqrt{-5})$

a) Following example 2 after proposition 1, I_2, I_3, I_3' non-principal

b) $2 \subset I_2^2$ clearly.

$$I_2^2 = \{\sum^N ab \mid a,b \in I_2\} = \{\sum^N \underbrace{(2\alpha + (1+\sqrt{-5})\beta)}_{a}\underbrace{(2\gamma + (1+\sqrt{-5})\delta)}_{b} \mid \alpha, \beta, \delta, \gamma \in \mathbb{Z}[\sqrt{-5}]\}$$

$$= \{\sum^N 4\alpha + (1+\sqrt{-5})[2\alpha\delta + 2\gamma\beta] + (1+2\sqrt{-5}-5)\beta\delta \mid \alpha, \beta, \gamma, \delta \in \mathbb{Z}[\sqrt{-5}]\}$$

$$= \{2\sum^N \alpha\alpha + (1+\sqrt{-5})(\alpha\delta + \gamma\beta) + (-2+\sqrt{-5})\beta\delta \mid \alpha, \beta, \gamma, \delta \in \mathbb{Z}[\sqrt{-5}]\}$$

$$\subseteq (2)$$

$$\therefore (2) = I_2^2$$

c) $I_2 I_3 = \{\sum^N (2\alpha + \beta(1+\sqrt{-5}))(3\gamma + \delta(2+\sqrt{-5}))\} = \{\sum^N 6\alpha\gamma + 4\alpha\delta + 2\alpha\delta\sqrt{-5} + 3\gamma\beta\sqrt{-5} + \delta\beta(-3+3\sqrt{-5})\}$

$$= \{\sum^N (6\alpha\gamma + 4\alpha\delta + 3\gamma\beta - 3\delta\beta) + (2\alpha\delta + 3\gamma\beta + 3\delta\beta)\sqrt{-5}\} \subseteq (1-\sqrt{-5})$$

Reverse inclusion clear $\therefore I_2 I_3 = (1+\sqrt{-5})$

Similar for $I_2 I_3' = (1+\sqrt{-5})$

$$\therefore I_2^2 I_3 I_3' \subseteq (2, 1 \pm \sqrt{-5}) \subseteq (6) \text{ and } (6) \subset (2) \subseteq I_2^2 I_3 I_3'$$

$$\therefore (6) = I_2^2 I_3 I_3'$$

p 283 #6

Let R be an ID s.t every prime ideal is principal

a) Let $\Sigma = \{I \subseteq R \mid I \text{ is an ideal}, I \text{ not principal}\} \neq \emptyset$

$\therefore$ under $\subseteq$, Σ has a maximal element by Zorn's Lemma (let upperbound in a chain be $\bigcup I_i$)

b) Let I be an ideal which is maximal w.r.t being non-principal. Let $a, b \in R$, $ab \in I$, $a, b \notin I$ (ie I not prime). Let $I_a := (I, a)$, $I_b := (I, b)$, $J := \{r \in R \mid rI_a \subseteq I\}$

$I \subseteq I_a$ and since I is maximal w.r.t being non-principal, $I_a = (\alpha)$ is principal

$J \subseteq I$ so similarly, it is principal. $I \subseteq I_b \subseteq J$ clear $\therefore I_a J = (\alpha\beta)$ clear

now $(ab) \subseteq I$ by property of J

c) if $x \in I$, by b), $I \subseteq J$. $\therefore x = s\alpha$ for $s \in J$. $\therefore I = I_\alpha J = (\alpha\beta)$ is principal

$\therefore$ no ideals not principal, ie every ideal principal $\therefore R$ is PID

3. p 293 #7

Let π be irreducible in $\mathbb{Z}[i]$

a) Let $n \geq 0$. $(\pi^{n+1}) = \pi^{n+1}\mathbb{Z}[i]$ is an ideal in $(\pi^n) = \pi^n \mathbb{Z}[i]$ since still group w.r.t + & still closed.

Abstract Algebra – Hw #10 Soln's

Joe Citrone

p3. w.r.t x of elements in π^n. $\mathbb{Z}[i] \xrightarrow{\pi^n} \mathbb{Z}(\pi^n)/(\pi^{n+1})$ is surjective with kernel π,

so $\mathbb{Z}[i]/(\pi) \cong \pi^n/\pi^{n+1}$

b) $\left|\mathbb{Z}[i]/(\pi)\right|^n \underset{\uparrow}{=} \left|\mathbb{Z}[i]/(\pi)\right| \cdot \left|(\pi)/(\pi^2)\right| \cdots \left|(\pi^{n-1})/(\pi^n)\right| = \left|\mathbb{Z}[i]/(\pi^n)\right|$

by part a)

c) By #6, p.293, the result holds for α irreducible, so let $\alpha = \pi_1^{a_1} \cdots \pi_n^{a_n}$

$\therefore N(\alpha) = N(\pi_1)^{a_1} \cdots N(\pi_n)^{a_n} = \left|\mathbb{Z}[i]/(\pi_1)\right|^{a_1} \cdots \left|\mathbb{Z}[i]/(\pi_n)\right|^{a_n} = \left|\mathbb{Z}[i]/(\pi_1^{a_1})\right| \cdots \left|\mathbb{Z}[i]/(\pi_n^{a_n})\right|$

$= \left|\mathbb{Z}[i]/(\pi_1^{a_1}) \times \cdots \times \mathbb{Z}[i]/(\pi_n^{a_n})\right| = \left|\mathbb{Z}[i]/(\pi_1^{a_1} \cdots \pi_n^{a_n})\right| = \left|\mathbb{Z}[i]/(\alpha)\right|$

~~p2~~ 306 #1

Let R be a UFD. $\therefore p = q_1 \cdots q_k$ for $q_i \in R[x]$ and each q_i monic and irreducible. By Gauss Lemma, also irreducible in $F[x]$

in $F[x]$, $p = ab$. Since $F[x]$ is UFD, $a = r \cdot q_{i_1} q_{i_2} \cdots q_{i_m}$ $r \in F^\times$

and $b = r^{-1} \cdot q_{j_1} \cdots q_{j_k}$.

But everything is monic $\therefore r = 1$ $\therefore a \in R[x]$ $\rightarrow\!\leftarrow$

Let $R = \mathbb{Z}[2\sqrt{2}]$. $x^2 - 2 = (x+\sqrt{2})(x-\sqrt{2})$ $\therefore R$ not UFD.

4. A quotient of a PID by a prime ideal is again a PID $\Rightarrow$ TRUE.

Let R be PID, I prime (hence maximal ideal by Prop 7 ... and yes, I said hence)

if $I = (0)$, $R/I \cong R$ $\therefore$ PID

else R/I field, which is PID

5. Let I be an ideal in $D^{-1}R$. Then $I \cap R$ is an ideal, say J, in R.

Since R is a PID, $J = aR$ for some $a \in R$

Claim: $I = aD^{-1}R$

$\alpha \in aD^{-1}R \in j \cdot (1/d)$ for $j \in J$, $d \in D$ $\therefore \alpha \in I$ since $J \subset I$

$x \in I \Rightarrow dx \in R \cap I = J$ for some $d \in D$ $\therefore dx = ay$ for some $y \in R$

$\therefore x = \frac{ay}{d} \in aD^{-1}R$

6. Let $R = \mathbb{Z}[\sqrt{-6}]$. For $\alpha \in \mathbb{Z}[\sqrt{-6}]$, if $\alpha = a + b\sqrt{-6}$, $N(\alpha) = a^2 + 6b^2$

a) $N(2) = 4$, $N(\sqrt{-6}) = 6$, which can not be written as the product of norms $\therefore$ irreducible

b) Assume R is UFD. $\therefore$ by Prop 12, prime $\leftrightarrow$ irreducible. By a), 2 is irreducible.

but 2 not prime since $\sqrt{-6} \cdot \sqrt{-6} = -6 \equiv 0 \mod 2$ in $\mathbb{Z}[\sqrt{-6}]/(2)$, and $\sqrt{-6} \notin (2)$ so $\mathbb{Z}[\sqrt{-6}]/(2)$ not ID.

$\therefore R$ not UFD.

Abstract Algebra Hw #10 Joe Cutrone

pg 4 c) By same method as a), easy to see $(1+\sqrt{-6})$ irred in R

From #5b, p293, either $\sqrt{-6}$ or $(1+\sqrt{-6})$ non-prime. Call non-prime a.

Let m be max ideal containing a. Then m is not principal, since if m principal, $m=(a) \rightarrow\leftarrow$ (since max $\Rightarrow$ prime)

else a is reducible, which contradicts pt a)

$\therefore m$ non-principal

7. Let $a = 11+7i$, $b = 18-i$ in $\mathbb{Z}[i]$

$\frac{11+7i}{18-i} = \frac{191}{325} + \frac{137}{325}i$ Choosing largest integer, let $q = 1+0i$

$\therefore r = (11+7i) - (18-i) = -7+8i$

$\frac{18-i}{-7+8i} = \frac{-134}{133} - \frac{137}{133}i$ $\therefore q = -1-i$

$\therefore r = (18-i) - (-7+8i)(-1-i) = 3$

$\frac{-7+8i}{3} = \frac{-7}{3} + \frac{8}{3}i$ $q = -2+3i$

$\therefore r = (-7+8i) - 3(-2+3i) = -1-i$

$\frac{3}{-1-i} = -\frac{3}{2} + \frac{3}{2}i$ $\therefore q = -2+2i$

$\therefore r = 3 - (-1-i)(-2+2i) = -1$

$\frac{-1-i}{-1} = 1+i \in \mathbb{Z}[i]$

$\therefore GCD(11+7i, 18-i) = 1+i$

8. Let $f(x) \in \mathbb{F}_p[x]$ of deg $n \geq 1$

From #14a), p.257, $\mathbb{F}_p[x]/(f(x)) = \{\bar{a}_0 + \bar{a}_1 x + \dots + \overline{a_{n-1}x^{n-1}} \mid a_i \in \mathbb{F}_p\}$

Since there are n coefficients $\bar{a}_1, \bar{a}_2, \dots, a_{n-1}$, and p choices for each,

total #elements is p^n

9. $\mathbb{Z}[x]/(2, x^3+1) \cong \mathbb{Z}/2\mathbb{Z}[x]/(x^3+1)$ where $x^3+1 = (x^2+x+1)(x+1)$ mod 2

$\cong \mathbb{Z}_2[x]/(x+1) \times \mathbb{Z}_2[x]/(x^2+x+1)$ by CRT

$\cong \mathbb{Z}_2 \times \mathbb{F}_4$ where $\mathbb{F}_4$ is a field with 4 elements by #8

$\therefore$ prime ideals are $(0, \mathbb{F}_4)$; $(\mathbb{Z}_2, 0)$

$\therefore$ in original ring, reversing the process in the isomorphisms, get corresponding ideals

$(2, x^2+x+1)$, $(2, x+1)$

10. $GCD(x^3-1, x+1) = x+1$, since $x+1 \mid x^3-1$ in $\mathbb{F}_2[x]$

indeed, $(x+1)(1+x+x^2) = x^3+1 \equiv x^3-1$ mod 2.