Pg 1

# Abstract Algebra Hw #9 Solutions

Joe Citrone

1. p. 258 #18

Let $R$ be an ID. Since $R[[x]]/(x) \cong R$, $(x)$ is prime

$R$ field $\leftrightarrow R[[x]]/(x) \cong R$ field $\leftrightarrow (x)$ maximal

p. 258 #19

Let $R$ be a finite commutative ring with identity. Let $P$ be a prime ideal.

$R/P$ is a finite integral domain $\therefore$ by Cor 3 p. 228, $R/P$ is a field $\therefore P$ is maximal

2. p. 259 #35

Let $A = (a_1, \ldots, a_n)$ be non-zero ideal (f.g) of $R$

$B \not\supseteq A$ iff $B \not\ni a_i$ for some $i$

Define $\Sigma = \{B \mid B \not\supseteq A\}$

$0 \in \Sigma$ so $\Sigma \neq \emptyset$

Let $B_1 \subseteq B_2 \subseteq \ldots$ be chain. Let $B = \bigcup B_i$, $A \not\subseteq B_i \; \forall i$

if $A \subseteq B$, then all $a_i \in B$ so $\forall i \in \{1, 2, \ldots, n\}$, $\exists m_i$ s.t $a_i \in B_{m_i} \Rightarrow$ all $a_i \in B_{\max\{m_i\}}$

$\therefore A \subseteq B_{\max\{m_i\}} \rightarrow\leftarrow$

$\therefore A \not\subseteq B \;\therefore B \subseteq \Sigma$

$\therefore$ by Zorn's Lemma, $\exists$ ideal $B$ maximal w.r.t chain.

p. 259 #36

Let $R$ commutative ring. Let $\Sigma = \{P \subseteq R \mid P$ prime ideal$\}$.

$R$ has a maximal ideal by Thm, so $\Sigma \neq \emptyset$

Make chain $P_1 \supseteq P_2 \supseteq \ldots$ in $\Sigma$.

Let $P = \bigcap P_i$.

Suppose $ab \in P$, $a \notin P$. Then $\exists n$ s.t $i \geq n$, $a \notin P_i$

since each $P_i$ is prime and $ab \in P \subsetneq P_i$, $b \in P_i$ for $i \geq n$

if $P_i \supseteq P_j$ since $P \subseteq P_i \; \forall i$ $\therefore$ By Zorn's lemma, $\Sigma$ has "maximal" element $\therefore R$ has min prime ideal.

Pg 2

# Abstract Algebra Hw #7 Solns

Joe Citrone

3. a) Let $f: \mathbb{Z} \hookrightarrow \mathbb{Q}$ be an injection. Then $(0) \subseteq \mathbb{Q}$ is a maximal ideal, but $(0) \subseteq \mathbb{Z}$ is prime & not maximal

b) Let $m \subseteq B$ be maximal ideal. Let $f: A \twoheadrightarrow B$ be surjective.

By 1st Iso Thm, $A/f^{-1}(m) \cong B/m$, which is a field since $m$ maximal

$\therefore A/f^{-1}(m)$ field $\therefore f^{-1}(m)$ max ideal in $A$

4. Let $A$ be comm. ring with a unit.

a) $Nil(A) = rad(0)$ (see prob #30 in 7.4) and is an ideal by prop 11 p.673

b) Let $a_0 \in A^\times$, $a_1, \ldots, a_n \in Nil(A)$. Let $p(x) = \sum_{i=0}^{n} a_i x^i$

Then each $a_i x^i$ are all nilpotent in $A[x]$ for $i = 1, n$

$\therefore$ since by a), $Nil(A[x])$ is an ideal, $a_1 x + a_2 x^2 + \cdots + a_n x^n$ nilpotent

$\therefore a_0 + \sum_{i=1}^{n} a_i x^i = p(x)$ is a unit by problem 3 on hw 7, (which says unit + nilpotent = unit)

c) Now let $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ for $n \geq 1$ be a unit in $A[x]$

$\therefore \exists\, g(x) \in A[x]^\times$ s.t. $f(x) g(x) = 1$

if $g(x) = \sum^{m} b_i x^i$, then $fg = \sum^{n+m} c_k x^k$, where $c_k = \sum_{i=0}^{k} a_i b_{k-i}$

$\therefore$ if $fg = 1$, by comparing coefficents, $a_0 b_0 = 1$ $\quad \therefore a_0$ is a unit

for $k > 0$, $c_k = \sum_{i=0}^{k} a_i b_{k-i} = 0$

$\therefore 0 = a_n^{r+1} c_{m+n-r-1} = \sum_j^n a_j a_n^{r+1} b_{m+n-r-1-j} = a_n^{r+2} b_{m-r-1}$

(since $m+n-r-1-j \geq m-r$ for $j \leq n-1$)

By induction, $a_n^{m+1} b_0 = 0$. Since $b_0$ is a unit, $a_n$ is nilpotent

$\therefore f - a_n x^n$ is a unit since $a_n x^n$ is nilpotent and $f$ is a unit

By induction, $a_1, \ldots, a_n$ are all nilpotent.

5. a) Let $\ell = lcm(3, 2+\sqrt{-5})$. $\qquad |a + b\sqrt{-5}| = \sqrt{a^2+5b^2}$

Then since both $3 \cdot (2+\sqrt{-5}) = 6 + 3\sqrt{-5}$ and 9 are divisible by 3 and $2+\sqrt{-5}$, $\ell \mid 6+3\sqrt{-5}$ & $\ell \mid 9$

Since $3 \mid \ell \mid 9$, $|3|^2 \mid |\ell|^2 \mid |9|^2 \Rightarrow |\ell|^2 = 9, 27$ or $81$

if $|\ell|^2 = 81$, then since $\ell \cdot r = 9$, $|\ell| \cdot |r| = |9| \Rightarrow |r| = 1 \Rightarrow r = \pm 1 \rightarrow \ell = \pm 9$ But then $\ell \nmid 6 + 3\sqrt{-5}$ $\rightarrow\leftarrow$

Abstract Algebra Hw #9 Solns

Joe Cutrone

if $|l|^2 = 9$; $l = \pm 3$ or $l = \pm 2 \pm \sqrt{-5} \Rightarrow l \nmid (2+\sqrt{-5})$ or $l \nmid 3$ $\rightarrow\leftarrow$

if $|l| = \sqrt{27}$, must have $a^2 + 5b^2 = 27$ for $a, b \in \mathbb{Z}$ $\rightarrow\leftarrow$

$\therefore$ $l$ does not exist.

b) To show $a = 3$, $b = 2 + \sqrt{-5}$ are coprime, show $\gcd(a,b) = 1$

Since $|3| = |2+\sqrt{-5}| = 3$, $g = \gcd(a,b)$ must have norm squared $|g|^2 \mid 9$

*note: care about $|\cdot|^2$ and not just norm since norm squared is an integer

since $|g|^2 \mid 9$, $|g| = 1, \sqrt{3}$ or $3$

$|g| \neq \sqrt{3}$ easy to see

$|g| \neq 3$ since else $|g|^2 = 9 \Rightarrow g = \pm 3$ or $\pm 2 \pm \sqrt{-5}$

but then if $g = \pm 3$, $g \nmid 2 \pm \sqrt{-5}$ ; if $g = \pm 2 \pm \sqrt{-5}$, $g \nmid 3$ $\rightarrow\leftarrow$

$\therefore |g| = 1$ $\therefore g = 1$

c) If $g = \gcd(3a, 3b)$ existed, $g \mid 9$ and $g \mid 6 + 3\sqrt{-5}$

$\therefore |g|^2 = 1, 3, 9, 27, 81$

$\therefore |g|$ is not 1: since $3 \mid g$, since 3 is a common divisor of $9, 6+3\sqrt{-5}$

not 9: since then $g = \pm 9$ ; $\pm 9 \nmid 6 + 3\sqrt{-5}$

~~[illegible]~~ not $\sqrt{3}$ or $\sqrt{27}$ by pt a) arguments

not 3 since $3 \mid g$ so $g = \pm 3$

but $2+\sqrt{-5} \mid g$ since $2+\sqrt{-5}$ is a common divisor of $9, 6+3\sqrt{-5}$

$\therefore$ g DNE

6. a) $y - x^2$ irred iff $x^2 - y$ irred

$x^2 - y$ irred by Eisenstein applied to $k[y]$ with prime ideal $(y)$

b) i) $x^2 + y^2 - 1 = x^2 + (y-1)(y+1)$ which is irreducible by Eisenstein applied to $k[y]$ with prime ideal $(y+1)$ (if $\operatorname{ch} k \neq 2$)

if $\operatorname{ch} k = 2$, $x^2 + y^2 - 1 = x^2 + y^2 + 1 = x^2 + (y+1)^2 = (x+y+1)^2$ $(*)$

ii) For $x^2 + y^2 + 1$,

if $y^2 + 1$ is irreducible in $k[y]$, apply Eisenstein with prime ideal $(y^2+1)$

if $y^2+1$ reducible, then $y^2 + 1 = (y + \sqrt{-1})(y - \sqrt{-1})$ with $\sqrt{-1} \in k$

if char $k \neq 2$, apply Eisenstein w/ prime ideal $(y + \sqrt{-1})$

if ch $k = 2$, see $(*)$

Abstract Algebra Hw #9 Soln's

TA- Joe Cutrone

7. a) Let $A = \mathbb{C}[x,y]/(-x^2-y^2+1)$. The automorphism $x \mapsto ix$, $y \mapsto iy$ induces an isomorphism $A \cong B$

The isomorphism $\mathbb{C}[u,v] \to \mathbb{C}[x,y]$ defined by $u \mapsto x+iy$, $v \mapsto x-iy$ induces an isomorphism $C \cong A$

b) The relation $uv-1$ makes $v$ the inverse of $u$ in $C \cong k[u, \frac{1}{u}]$

If $I \subseteq k[u, \frac{1}{u}]$ is an ideal, let $I \cap k[u] = (f)$ // $k[u]$ is a PID

Then $I = (f)$: if $g \in I$, then $gu^n \in k[u]$ for some $n$. Then $gu^n = hf$, so $g = \frac{h}{u^n} \cdot f$.

8. Use fact that if $N(\alpha)$ is $\pm$ prime in $\mathbb{Z}$, $\alpha$ irred in $\mathcal{O}$ ; prop 18, pt 2, p. 291

$N(1+3i) = (1+3i)(1-3i) = 10$ $\therefore$ reducible

$N(70+i) = (70+i)(70-i) = 4{,}901$ (not prime) $\therefore$ reducible

$N(201+43i) = (201+43i)(201-43i) = 42{,}250$ (not prime) $\therefore$ reducible

# Problem Set 9

From "Dummit & Foote"

1. nn. 18, 19 p. 258
2. n. 35, 36 p. 259

## Further exercises

3. Let $f : A \to B$ be a ring homomorphism and let $\mathfrak{m}$ be a maximal ideal of $B$. Let $\mathfrak{n} = f^{-1}(\mathfrak{m})$. Show that
   (1) $\mathfrak{n}$ is not in general a maximal ideal of $A$
   (2) if $f$ is surjective, then $\mathfrak{n}$ is a maximal ideal of $A$.

4. Let $A$ be a commutative ring with unit. Let denote by Nil(A) the set of nilpotent elements of $A$ (i.e. $a \in A$ such that $a^n = 0$ for some $n \in \mathbb{N}$). Show that Nil(A) is an ideal of $A$.
   Show that if $a_0 \in A^\times$ and $a_1, \ldots, a_n \in$ Nil(A), then the polynomial $p(x) = \sum_{i=0}^{n} a_i x^i \in A[x]^\times$.
   Finally, prove inductively that if $n \geq 1$ and $\sum_{i=0}^{n} a_i x^i \in A[x]^\times$, then $a_0 \in A^\times$ and $a_n \in$ Nil(A) and $a_{n-1}, \ldots, a_1 \in$ Nil(A).

5. Let $a = 3$ and $b = 2 + i\sqrt{5}$ be two elements in $\mathbb{Z}[i\sqrt{5}]$. Show that
   (1) $\mathrm{lcm}(a, b)$ does not exist
   (2) $a$ and $b$ are co-primes i.e. $\gcd(a, b) = 1$
   (3) $\gcd(3a, 3b)$ does not exist.

6. Let $k$ be a field. Study the irreducibility in $k[x, y]$ of the following polynomials:

$$y - x^2, \qquad x^2 + y^2 \pm 1.$$

7. Show that $A = \mathbb{C}[x, y]/(x^2 + y^2 - 1)$ and $B = \mathbb{C}[x, y]/(x^2 + y^2 + 1)$ are isomorphic to the ring $C = \mathbb{C}[u, v]/(uv - 1)$. Show that $C$ is a P.I.D.

8. Which among the following gaussian integers are reducible?

$$1 + 3i, \qquad 70 + i, \qquad 201 + 43i.$$