NAP 2019, HOMEWORK SET #2, MAY 20, 2019

ROGER & SYLVIA WIEGAND

• 3.4. This problem is an easy consequence of Theorem 3.14, but, pehaps as an illustration of the power of that theorem, we will just grind it out first. We may harmlessly assume that $n \geq m$. Then, since $a^n \in (a^m)$, it will suffice to show that $(a^n, b^n) = R$; for then we will have $R \subseteq (a^n, b^n) \subseteq (a^m, b^n) \subseteq R$ and hence $(a^m, b^n) = R$, as desired.

Let us assume, inductively, that $(a^n, b^n) = R$ for some positive integer n and prove that $(a^{n+1}, b^{n+1}) = R$. (The base case $n = 1$ is the orignial hypothesis.) We have, by assumption, $1 = ra^n + sb^n$ for suitable elements $r, s \in R$. Multiplying both sides by ab, we get $ab = rba^{n+1} + sab^{n+1}$, and hence

$$ab \in (a^{n+1}, b^{n+1})\,.$$

Also, from the base case we have $1 = ua+vb$ for suitable elements $u, v \in R$. Raising both sides to the $n + 1^{\text{st}}$ power, and using the binomial theorem, we get

$$1 = u^{n+1}a^{n+1} + M + v^{n+1}b^{n+1}\,,$$

where M is the sum of the other n terms in the binomial expansion. Each of the terms in M has ab as a factor, and we have already shown that $ab \in (a^{n+1}, b^{n+1})$, so we see that $1 \in (a^{n+1}, b^{n+1})$. It follows that $(a^{n+1}, b^{n+1}) = R$. □

Here's a quick proof using Theorem 3.14: If $(a^n, b^n) \neq R$, there is a maximal proper ideal $\mathfrak{m}$ containing (a^n, b^n). Then $R/\mathfrak{m}$ is a field, and the cosets $a^n + \mathfrak{m}$ and $b^n + \mathfrak{m}$ are zero. Therefore $a + \mathfrak{m} = 0 = b + \mathfrak{m}$, that is, $(a, b) \subset \mathfrak{m}$, contradiction. □

• 3.7. Let $I = (2, x)$. Then $\frac{\mathbb{Z}[x]}{I} \cong \mathbb{Z}/(2)$, which is a field. We claim that I^n needs exactly $n + 1$ generators, for $n \geq 0$. (Note $I^0 = \mathbb{Z}[x]$, which does indeed need exactly one generator.) It is easy to see that $n + 1$ generators suffice: $I^n = (2^n, 2^{n-1}x, \ldots, 2x^{n-1}, x^n)$. The easiest way to see that there is no generating set with fewer than $n + 1$ elements is to show, in fact, that the homomorphic image I^n/I^{n+1} actually needs $n + 1$ generators. This quotient is a vector space over the two-element field R/I, and it is not hard to see that the images of the generators above form a basis. Yeah, we're kind of using some more advanced stuff here, and not putting in details, so let's just say that this is one of the three problems that *we* are omitting. □

• 3.9. First we claim that if r is a non-zero element of R, then $r^2 \neq 0$. To see this, suppose $r^2 = 0$. Let $f : R \twoheadrightarrow (r)$ be the surjective homomorphism (of abelian groups) defined by $f(t) = tr$. then r is in the kernel of f, so there is an induced surjection $\overline{f} : R/(r) \twoheadrightarrow (r)$. Since $R/(r)$ is, by assumption, finite, so is (r). Now R (as an abelian group) is the union of the finitely many cosets of (r), each of which is finite, and thus R itself is finite, a contradiction to the hypotheses. This proves the claim.

Now let a and b be non-zero elements of R, and suppose that $ab = 0$. There is a ring homomorphism $g : R \to \frac{R}{(a)} \times \frac{R}{(b)}$ taking r to the ordered pair $\big(r + (a), r + (b)\big)$. If r is in the kernel of this map, then $r \in (a) \cap (b)$ and hence $r^2 = 0$. Therefore, by what we showed in the previous paragraph, $r = 0$. Thus g is injective, and this is absurd, since R is infinite but $\frac{R}{(a)} \times \frac{R}{(b)}$ is finite. □

• 3.10. When R is a domain, we have $\deg(fg) = \deg(f) + \deg(g)$ for non-zero elements $f, g \in R[x]$. Therefore, in order that $fg = 1$ both f and g have to be constants (degree 0). Moreover, they must be units of R. Thus the units of $R[x]$ are exactly the units of R.

Now let $R = \mathbb{Z}/(4)$, and let $f = a_0 + a_x + \cdots + a_m x^m$. We claim that f is a unit of $R[x]$ if and only if $a_0 = \pm 1$ and $a_i \in \{0, 2\}$ for $1 \leq i \leq m$. For the "if" direction, we can write such an f in the form $f = \pm 1 + 2g$; simply note that then $f^2 = 1$, so f is a unit. For the other direction, suppose f is a unit with inverse $g = b_0 + b_1 x + \ldots b_n x^n$. Then $a_0 b_0 = 1$, so $a_0 = b_0 = \pm 1$. Assume $a_i \notin \{0, 2\}$ (that is, $a_i = \pm 1$) for some $i \geq 1$, and let r be the *first* such integer i. The coefficient of x^r in the product fg is then $a_i b_0 + 2c$ for some $c \in R$. Therefore this coefficient is not zero, and we have a contradiction. □

• 3.11. Finally, an easy problem! However, we have to assume that the element a is non-zero, else the "if" direction fails, since prime elements are rrequired to be non-zero. Suppose a is prime, and let $r, s \in R/(a)$ with $rs = 0$. Write $r = x + (a)$ and $s = y + (a)$ with $x, y \in R$. Then $xy + (a) = rs = 0$, so $xy \in (a)$. This means $a \mid xy$. Since a is prime, either $a \mid x$ or $a \mid y$, that is, either $x \in (a)$ (in which case $r = 0$) or $y \in (a)$ (in which case $s = 0$.

Conversely, assume $a \neq 0$ and $R/(a)$ is a domain. If $a \mid xy$, with $x, y \in R$, then $xy \in (a)$. Therefore $(x + (a))(y + (a) = xy + (a) = 0$ in $R/(a)$. Since $R/(a)$ is domain, either $x + (a) = 0$ or $y + (a) = 0$. this means either $x \in (a)$ (in which case $a \mid x$) or $x \in (b)$ (in which case $a \mid y$. □

• 3.12. First we notice that if $\alpha \in \mathbb{Z} + i\sqrt{5}\mathbb{Z}$ then $\phi(\alpha) = \alpha\overline{\alpha}$, where $\overline{\alpha}$ is the complex conjugate. By multiplicativity of complex conjugation (or by a boring direct calculation) we have $\phi(\alpha\beta) = (\phi(\alpha))(\phi(\beta))$ for $\alpha, \beta \in \mathbb{Z} + i\sqrt{5}\mathbb{Z}$.

(a) If $\alpha = m + i\sqrt{5}n$ and $\alpha\beta = 1$, then $(\phi(\alpha))(\phi(\beta)) = \phi(\alpha\beta) = \phi(1) = 1$. Since $\phi(\alpha)$ and $\phi(\beta)$ are non-negative integers, it follows that $\phi(\alpha) = 1$, and hence $m = \pm 1$ and $n = 0$. □

(b) If $m + i\sqrt{5}n \notin \{0, 1, -1\}$, then either $|m| \geq 2$ (in which case $m^2 \geq 4$) or $|n| \geq 1$ (in which case $5n^2 \geq 5$). In both cases we have $\phi(m + i\sqrt{5}n) \geq 4 > 3$. Now let $\alpha = 2 \pm i\sqrt{5}$, and suppose $\alpha = \beta\gamma$, with $\beta, \gamma \in \mathbb{Z} + i\sqrt{5}\mathbb{Z}$, neither of them a unit and, of course, neither of them zero. Then $\beta, \gamma \notin \{0, \pm 1\}$, and we have $9 = \phi(\alpha) = \phi(\beta\gamma) = (\phi(\beta)) \cdot (\phi(\gamma)) > 3 \cdot 3 = 9$, contradiction. □

(c) $(2+i\sqrt{5})(2-i\sqrt{5}) = 6 = 2 \cdot 3$, so $2+\sqrt{5} \mid 2 \cdot 3$. If $2+i\sqrt{5} \mid 2$, write $(2+i\sqrt{5})\beta = 2$, getting $9\phi(\beta) = \phi(2) = 4$, which is absurd, since $\phi(\beta)$ is a non-negative integer. If $(2 + i\sqrt{5})\beta = 3$, we get $9\phi(\beta) = \phi(3) = 9$, forcing $\phi(\beta) = 1$, whence $\beta = \pm 1$, another absurdity. Thus $2 + i\sqrt{5}$ divides neither 2 nor 3 and therefore is not prime. The ring $\mathbb{Z} = i\sqrt{5}\mathbb{Z}$ is not a UFD because it has an irreducible element that is not prime. □

• 3.14. We choose to omit this one, because it is too easy.

• 3.16. A basic fact that we should formalize now is the "Correspondence Theorem", which says

Let I be an ideal in a ring R. The ideals of the ring R/I are exactly the sets J/I, where J is an ideal of R that contains I. Moreover, we have $\frac{R/I}{J/I} \cong R/J$ as rings. □

The Correspondence Theorem is sort of used in the proof of Theorem 3.16.

Back to the problem. The ideals of $\mathbb{Z}/(6)$ correspond to the ideals J of $\mathbb{Z}$ such that $(6) \subseteq J$, that is, the ideals (a) of $\mathbb{Z}$ such that $a \mid 6$. Therefore the ideals of $\mathbb{Z}/(6)$ are $(1)/(6), (2)/(6), (3)/(6), and (6)/(6)$, or (using overlines for cosets) $(\overline{1}), (\overline{2}), (\overline{3}), (\overline{0})$. The ring is a *principal ideal ring* but *not* a principal ideal *domain* since $\overline{2}\cdot\overline{3} = \overline{0}$. □

• 3.17. Closure under $\pm$: $\frac{r}{s} \pm \frac{u}{v} = \frac{rv \pm su}{sv}$. Closure under mulitplication: $\frac{r}{s} \cdot \frac{u}{v} = \frac{ru}{sv}$. (Note $p \nmid sv$ because p is prime. Identity: $1 = \frac{1}{1}$ and $p \nmid 1$. □An element $\frac{r}{s}$ (with $p \nmid s$ is a unit if and only if $p \nmid r$. To see this, suppose $p \mid r$ and $\frac{r}{s} \cdot \frac{u}{v} = 1$, then $ru = sv$, so $p \mid sv$, contradiction. Conversely, suppose $\frac{r}{s} \in R$ with $p \nmid s$ and $p \nmid r$. Then $\frac{s}{r} \in R$, and $\frac{r}{s} \cdot \frac{s}{r} = 1$, so $\frac{r}{s}$ is a unit. □

Let I be an ideal of R, and check easily that $K \cap \mathbb{Z}$ is an ideal of $\mathbb{Z}$. We can write $I \cap \mathbb{Z} = \mathbb{Z}x$ for some integer x (since $\mathbb{Z}$ is a PID). We will show that $I = Rx$. "$\supseteq$" is clear, since $x \in I$. For the reverse inclusion, let $y \in I$ and write $y = \frac{r}{s}$, where $r, s \in \mathbb{Z}$ and $p \nmid s$. Then $r = sy \in I \cap \mathbb{Z}$, so $r = cx$ for some integer c. Then $sy = cx$, so $y = \frac{c}{s}x \in Rx$. □

• 3.18. Since R is a domain but not a field, there is a non-zero non-unit $c \in R$. Let $I = (c, x)$ in $R[x]$, and suppose I is a principal ideal, say, $I = (a)$, where $a \in R[x]$. Then $c = ab$ for some $b \in R[x]$, and this means a must have degree 0, that is, $0 \neq a \in R[x]$. Also, we have $x \in aR[x]$, say $x = a(a_0 + a_1x + \ldots a_nx^n)$. From this we get $a_i = 0$ for $i \neq 1$ and $aa_1 = 1$. Therefore a is a unit of R. Since $(c, x) = aR[x]$, there are polynomials $f, g \in R[x]$ such that $a = cf + xg$. Setting $x = 0$, we get $a = cf(0)$, which, since a is a unit, impies that c is a unit, contradiction. □

• 3.19. Since "least common multiple" is not defined in the book, we shall do so here. Given non-zero elements $a_1, \ldots, a_k$ in a domain R, an element $m \in R$ is a *least common multiple* (LCM) of $a_1, \ldots, a_k$, provided (i) $a_i \mid m$ for each i, and (ii) if $n \in R$ and $a_i \mid n$ for each i, then $m \mid n$. Out of habits cultivated over many decades, we shall use the term *greatest common divisor* (GCD) for Garling's *highest common factor*. It is easy to check that if d is a GCD of a set $\{a_i\}$ and d' is any element of R, then d' is a GCD of $\{a_i\}$ if and only if d' is an associate of d. Note that for a *single* non-zero element $a \in R$, a is a GCD of $\{a\}$ and an LCM of $\{a\}$. Therefore we'll deal only with sets with more than one element. First we prove: If every two non-zero elements have a GCD, then every finite set $\{a_1, \ldots, a_n\}$, $n \geq 2$, of non-zero elements has a GCD. No problem if $n = 2$, so assume $n \geq 3$ and that $\{a_1, \ldots, a_{n-1}\}$ has a GCD d. Let e be a GCD of d and a_n. Then $e \mid d$, so $e \mid a_i$ for each $i \leq n - 1$, and of course $e \mid a_n$. Suppose f is a common divisor of $a_1, \ldots, a_n$; we want to show that $f \mid e$. Since $f \mid a_i$ for $1 \leq i \leq n - 1$, f must divide d. Also, $f \mid a_n$, so $f \mid e$.

Similarly, if every two elements of R have an LCM, then every finite set of two or more elements has an LCM. The problem now simplifies to: Every two elements have a GCD if and only if every two elements have an LCM. Alas, we don't know how to prove this. We *can* prove the "if" direction, and we can prove the "only if" direction if we assume that R satisfies ACCPI. It's conceivable that existence of LCMs implies ACCPI, in which case the problem would be solved, but this seems unlikely.

" if": Assume that m is an LCM of a and b. Since ab is a common multiple of a and b, m must divide ab, say, $md = ab$. We shall show that d is a GCD of a and b. Since $b \mid m$ we can write $br = m$. Then $dbr = dm = ab$, and hence $dr = a$. This shows that $d \mid a$, and a symmetric argument, starting with $a \mid m$, shows that $d \mid b$.

Next, let $e \in R$ be a common divisor of a and b, say, $eu = a$ and $v = b$. We want to show that $e \mid d$. **VOMITYPUS**

"only if", assuming ACCPI: Let a and b be non-zero elements of R. We want to find an LCM. Let $\mathcal{S} = \{(x) \mid a \mid x \quad \text{and} \quad b \mid x\}$. Note that $(ab) \in \mathcal{S}$, so $\mathcal{S}$ is a non-empty set of principal ideals. By ACCPI, $\mathcal{S}$ has a maximal element m. This means that m is a common multiple of a and b but no proper divisor of m is a common multiple of a and b. (To say that m' is a proper divisor of m means that $(m') \supsetneq (m)$.) We claim that m is an LCM of a and b. To see this, suppose n is a common multiple of a and b. We have to show that $m \mid n$. Let d be a GCD of m and n. (We are assuming that every pair of non-zero elements has a GCD.) Since $a \mid m$ and $a \mid n$, a is a common divisor of m and n, and hence $a \mid d$. By symmetry, $b \mid d$. Thus d is a common multiple of a and b, and so $(d) \in \mathcal{S}$. Since $d \mid m$, we have $(d) \supset (m)$ and therefore $(d) = (m)$, as (m) is maximal in $\mathcal{S}$. Thus $d = mw$, where w is a unit of R. Since $d \mid n$, we can write $n = yd$ for some $y \in R$. But then $n = ymw$, and hence $m \mid n$. □

• 3.24. Let J be a proper ideal of the countable ring R. Let $R \setminus J = \{x_1, x_2, x_3, \dots\}$. If $J + Rx_i = R$ for every $i \geq 1$, then J is a maximal proper ideal, and we are done. Otherwise, let i_1 be the least index for which $J + Rx_{i_1} \neq R$. Repeat: If $J + Rx_{i_1}$ is not a maximal ideal there must be some $j \neq i$ such that $J + Rx_{i_1} + Rx_j \neq R$. Let i_2 be the least such index, and note that $i_2 > i_1$. Continue. There are two possibilities. (1) At some finite stage $J + Rx_{i_1} + \cdots + Rx_{i_n}$ is a maximal ideal, and we are done. (2) The process goes on forever. In that case $\mathfrak{m} := J + Rx_{i_1} + Rx_{i_2} + Rx_{i_3} + \dots$ is a nested union of proper ideals of R. Then $\mathfrak{m}$ is a proper ideal since it does not contain 1. Also, it is not contained in any larger proper ideal, since there is no index greater than every i_j.

• 3.25. If u is invertible (that is, u is a unit), Then $Ru = R$, so R is not contained in any proper ideal. Conversely, if u is not invertible then Ru is a proper ideal and hence, by Theorem 3.14, is contained in a maximal proper ideal.

• 3.26. We won't prove that $J[x]$ is an ideal (too boring). An element $f(x) = a_0 + a_1x + \cdots + a_mx^m$ in $R[x]$ belongs to $J[x]$ if and only $a_i \in J$ for each i. Suppose now that $g(x) = b_0 + b_1x + \cdots + b_nx^n \in R[x]$, and that neither $f(x)$ nor $g(x)$ is in $J[x]$. Then each of these polynomials has a coefficient that's not in J. Let i be the least index for which $a_i \notin J$ and j the least index for which $b_j \notin J$. The coefficient of x^{i+j} in $f(x)g(x)$ is then

$$\sum_{\ell<i} a_\ell b_{i+j-\ell} \quad + a_ib_j + \quad \sum_{\ell>i} a_\ell b_{i+j-\ell}\,.$$

The middle term a_ib_j is not in J. In the first sum, each a_ℓ is in J, so the first sum is in J. In the last sum, each subscript $i + j - \ell$ is less than j, so $b_{i+j-\ell} \in J$. Therefore the last sum is in J. By the 3/4 Lemma (or something like that) the coefficient of x^{i+j} in $f(x)g(x)$ is outside J, and we have $f(x)g(x) \notin J$.

[The elegant way to do this is to observe that $R[x]/J[x] \cong (R/J)[x]$, which we know is an integral domain (since R/J is an integral domain). Therefore $J[x]$ is a prime ideal of $R[x]$. (We are using the easy observation that, in any ring A, an ideal I is prime if and only if A/I is an integral domain.)]

To show that $J[x]$ is not a maximal proper ideal, we'll use the elegant approach first. If $J[x]$ were a maximal proper ideal of $R[x]$, then $R[x]/J[x]$ would be a field, and hence the isomorphic ring $(R/J)[x]$ would be a field. But in the polynomial

ring $(R/J)[x]$ the only units are constants that are units of R/J. In particular, the non-zero polynonial x is not a unit, so $(R/J)[x]$ is not a field.

Taking a cue from the elegant approach, we can build a direct, computational argument by noting that $x \notin J[x]$, so that $J[x] + xR[x]$ is an ideal properly containing $J[x]$. Moreover, it's a proper ideal since it does not contain 1. Indeed, if $1 = f(x) + xg(x)$, where $f(x) \in J[x]$, we could set $x = 0$, getting $1 = a_0$, the constant term of $f(x)$. But $a_0 \in J$, and this means that $1 \in J$, contradicting the assumption that J is a prime ideal, and hence a proper ideal.