TheNumbersBook.com 2010

Stewart: # 4.4, 4.6, 4.8, 4.11, 4.13, 4.16

4.4 Show that a homomorphic image of a noetherian ring is noetherian.

Let $\phi : R \to S$ be a ring homomorphism, where R is noetherian. By First Isomorphism Theorem,

$$R/\ker(\phi) \cong \phi(R)$$

so it's sufficient to show $R/\ker(\phi)$ is noetherian.

Consider the natural projection, $\pi : R \to R/\ker(\phi)$ (which is surjective by 1st Isomorphism Theorem). We appeal to Problem 7.3.24 and use the following two facts:

(1) If J is an ideal of $R/\ker(\phi)$, then $\phi^{-1}(J)$ is an ideal of R.

(2) If I is an ideal of R then $\phi(I)$ is an ideal of $R/\ker(\phi)$.

Let $J \subseteq R/\ker(\phi)$ be an ideal. By Problem 7.3.24, $\pi^{-1}(J)$ is an ideal in R and since R is noetherian, it is finitely generated, say

$$\pi^{-1}(J) = \langle x_1, \cdots, x_n \rangle$$

for a finite number of elements $x_1, \cdots, x_n \in R$. The natural projection sends x_i to $x_i + \ker(\phi)$, so we get

$$\begin{aligned} J &= \pi(\pi^{-1}(J)) \\ &= \pi(\langle x_1, \cdots, x_n \rangle) \\ &= \langle \pi(x_1), \cdots, \pi(x_n) \rangle \\ &= \langle x_1 + \ker(\phi), \cdots, x_n + \ker(\phi) \rangle \\ &= \langle x_1 + \ker(\phi), \cdots, x_r + \ker(\phi) \rangle \text{ (1)} \end{aligned}$$

[note on (1): since x_i and x_j may both be in the same coset, the number of generators for J will be less than or equal to number of generators for $\pi^{-1}(J)$; hence, the notation $x_r + \ker(\phi)$ rather than $x_n + \ker(\phi)$]. So $x_1 + \ker(\phi), \cdots, x_r + \ker(\phi)$ are the generators of J, thus J is finitely generated. Since this is true for any ideal, $R/\ker(\phi)$ is noetherian. It follows that the image of R is noetherian. ∎

4.6 Find a ring that is not noetherian.

Let $R[x_1, x_2, x_3, \cdots]$ be a polynomial ring in infinitely many variables $x_1, x_2, x_3, \cdots$. Note that $\langle x_1 \rangle$ is a proper subring of $\langle x_1, x_2 \rangle$, both of which are ideals in $R[x_1, x_2, x_3, \cdots]$. In general,

$$\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \langle x_1, x_2, x_3 \rangle \subset \cdots$$

is an ascending chain of ideals that does not terminate because there are infinitely many variables. By Proposition 4.5, $R[x_1, x_2, x_3, \cdots]$ is not noetherian. ∎

4.8 Is $10 = (3+i)(3-i) = 2 \cdot 5$ an example of non-unique factorization in $\mathbb{Z}[i]$? Give reasons for your answer.

No. In order to have an example of non-unique factorization, we require that

$$10 = p_1 \cdots p_r = q_1 \cdots q_s$$

and there exists no permutation of $\{1, \cdots, r\}$ such that p_i and $q_{\pi(i)}$ are associates for some $i = 1, \cdots, r$. However, $3+i, 3-i, 2$ and 5 factorize as follows:

$$\begin{aligned} 3+i &= (1-i)(1+2i) \\ 3-i &= (1+i)(1-2i) \\ 2 &= (1+i)(1-i) \\ 5 &= (1+2i)(1-2i) \end{aligned}$$

Indeed, up to reordering, $(3+i)(3-i)$ and $2 \cdot 5$ is the factorization $(1+i)(1-i)(1+2i)(1-2i)$ and so we have

$$10 = (1+i)(1-i)(1+2i)(1-2i) = (1+i)(1-i)(1+2i)(1-2i)$$

Clearly, each of the factors is an associate with itself, so this is not an example of non-unique factorization. ∎

4.11 Show in $\mathbb{Z}[\sqrt{-5}]$ that $\sqrt{-5} | (a + b\sqrt{-5})$ iff $5|a$. Deduce that $\sqrt{-5}$ is prime in $\mathbb{Z}[\sqrt{-5}]$. Hence conclude that the element 5 factorizes uniquely into irreducibles in $\mathbb{Z}[\sqrt{-5}]$ although $\mathbb{Z}[\sqrt{-5}]$ does not have unique factorization.

($\Rightarrow$) Given that $\sqrt{-5} | (a + b\sqrt{-5})$, then $\sqrt{-5} | a$ because $b\sqrt{-5}$ is a multiple of $\sqrt{-5}$. So $\exists c \in \mathbb{Z}[\sqrt{-5}]$ such that

$$\sqrt{-5}c = a$$

Squaring both sides and simplifying, we get

$$\begin{aligned} -5c^2 &= a^2, \\ 5c' &= a^2 \text{ (for some } c' \in \mathbb{Z}[\sqrt{-5}]) \end{aligned}$$

So $5|a^2$. Since $5, a \in \mathbb{Z}$ and 5 is prime in $\mathbb{Z}$, then a must have a factor of 5. Thus, $5|a$.

$(\Leftarrow)$ Conversely, if $5|a$ then $\exists c \in \mathbb{Z}[\sqrt{-5}]$ such that $5c = a$. Furthermore,

$$\begin{aligned} 5c &= a \\ 5(5c^2) &= a^2, \\ (-5)(-5c^2) &= a^2, \\ \sqrt{-5}(\pm c\sqrt{-5}) &= a, \\ \sqrt{-5}c' &= a \text{ (for some } c' \in \mathbb{Z}[\sqrt{-5}]) \end{aligned}$$

so $\sqrt{-5}|a$. It is also true that $\sqrt{-5}$ must divide any multiple of itself, so $\sqrt{-5}|b\sqrt{-5}$. It follows that

$$\sqrt{-5}|(a + b\sqrt{-5})$$

This completes the first part of the problem.

We now show that $\sqrt{-5}$ is a prime in $\mathbb{Z}[\sqrt{-5}]$. Let $\alpha = a + b\sqrt{-5}, \beta = c + d\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$. Then $\alpha\beta = (ac - 5bd) + (ad + bc)\sqrt{-5}$. Now if $\sqrt{-5}|\alpha\beta$, then by the statement of the problem, $5|(ac - 5bd)$. Since $5bd$ is divisible by 5, so is ac, for $a, c \in \mathbb{Z}$. By definition of prime, $5|a$ or $5|c$. By the statement of the problem, we have that $\sqrt{-5}|(a + b\sqrt{-5})$ or $\sqrt{-5}|(c + d\sqrt{-5})$. We have thus shown that if $\sqrt{-5}|\alpha\beta$ then $\sqrt{-5}|\alpha$ or $\sqrt{-5}|\beta$, the precise definition of a prime.

Finally we show that 5 has unique factorization. By Proposition 4.12, $\sqrt{-5}$ is an irreducible. Note that $5 = -\sqrt{-5}\sqrt{-5}$. We show that this is a unique factorization. Let $5 = \alpha\beta$ for α and β as defined above. Since $\sqrt{-5}$ is prime, $\sqrt{-5}|\alpha$ or $\sqrt{-5}|\beta$. Without loss of generality, say $\sqrt{-5}|\alpha$. Then we have

$$-\sqrt{-5}\sqrt{-5} = 5 = \sqrt{-5}c'\beta \quad (1)$$

for some $c' \in \mathbb{Z}[\sqrt{-5}]$. We rewrite (1), and use the fact that $\mathbb{Z}[\sqrt{-5}]$ is an integral domain, to get that:

$$\begin{aligned} -\sqrt{-5}\sqrt{-5} &= \sqrt{-5}c'\beta \\ &\Downarrow \\ 0 &= \sqrt{-5}\sqrt{-5} + \sqrt{-5}c'\beta \\ &= \sqrt{-5}(\sqrt{-5} + c'\beta) \\ &\Downarrow \\ 0 &= \sqrt{-5} + c'\beta \text{ (since } \mathbb{Z}[\sqrt{-5}] \text{ is an ID)} \\ -\sqrt{-5} &= c'\beta \end{aligned}$$

If we now write out β, we see that $c'(c + d\sqrt{-5}) = c'c + c'd\sqrt{-5}$ is divisible by $\sqrt{-5}$. Specifically, this means that $\sqrt{-5}|c'c$. In other words, $\exists k \in \mathbb{Z}[\sqrt{-5}]$ such that $k\sqrt{-5} = c'c$.

Plugging this into (1), we have

$$\begin{aligned}
-\sqrt{-5}\sqrt{-5} &= \alpha\beta \\
&= \sqrt{-5}c'\beta \\
&= \sqrt{-5}c'(c+d\sqrt{-5}) \\
&= \sqrt{-5}(c'c+c'd\sqrt{-5}) \\
&= \sqrt{-5}(\sqrt{-5}k+c'y\sqrt{-5}) \text{ (we just derived this)} \\
&= \sqrt{-5}(\sqrt{-5})(k+c'y) \quad (2)
\end{aligned}$$

Adding $\sqrt{-5}\sqrt{-5}$ to both sides yields

$$\begin{aligned}
-\sqrt{-5}\sqrt{-5} &= \sqrt{-5}(\sqrt{-5})(k+c'y) \\
&\Downarrow \\
0 &= \sqrt{-5}\sqrt{-5}(1+k+c'y)
\end{aligned}$$

Since $\sqrt{-5}\sqrt{-5}$ is nonzero, it must be that $1+k+c'y=0$, or equivalently, that $k+c'y$ is a unit. How does this help us? Observing (2), we see that

$$\begin{aligned}
\alpha\beta &= \sqrt{-5}(\sqrt{-5})(k+c'y) \\
&= u\sqrt{-5}\sqrt{-5}
\end{aligned}$$

for some unit $u \in \mathbb{Z}[\sqrt{-5}]$. In other words, 5 factorizes uniquely in $\mathbb{Z}[\sqrt{-5}]$. It is easy to see that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, however, as 2 is an irreducible in $\mathbb{Z}[\sqrt{-5}]$ but not prime (Theorem 4.13). ■

4.13 Let p be an odd rational prime and $\zeta = e^{\frac{2\pi i}{p}}$. If α is a prime element in $\mathbb{Z}[\zeta]$, prove that the rational integers which are divisible by α are precisely the rational integer multiples of some prime rational integer q. (Hint: $\alpha | N(\alpha)$, so α divides some rational prime factor q of $N(\alpha)$. Now show α is not a factor of any $m \in \mathbb{Z}$ prime to q).

We begin by making some important observations:

(1) $\mathbb{Z}$ is a ED and the only units are ± 1.

(2) Bezout's identity: If $m, q \in \mathbb{Z}$ and $\gcd(m,q)=1$, then there exist $x, y \in \mathbb{Z}$ such that $mx+qy=\gcd(m,q)=1$.

Now $\alpha | N(\alpha)$ and since $\alpha \in \mathbb{Z}[\zeta]$, $N(\alpha) \in \mathbb{Z}$. This allows us to factorize $N(\alpha)$ into prime factors as follows:

$$N(\alpha) = qp_1 \cdots p_n$$

for rational prime integers $q, p_1, \cdots, p_n \in \mathbb{Z}$. Since α is prime in $\mathbb{Z}[\zeta]$, α must divide some prime factor of $\mathbb{Z}$, say q. In other words, $\exists c \in \mathbb{Z}$ such that

$$\alpha c = q \qquad (*)$$

We now show that $\alpha \not| m$ for any $\gcd(m, q) = 1$. Suppose not. That is, let $m \in \mathbb{Z}$ be prime to q and suppose that $\alpha | m$. Then there exists an integer c' such that

$$\alpha c' = m \qquad (**)$$

Now, using (2), we have that

$$\begin{aligned} 1 &= mx + qy, \\ &= (\alpha c')x + (\alpha c)y, \\ &= \alpha(c'x + cy), \end{aligned}$$

which immediately implies that α and $c'x + cy$ are units in $\mathbb{Z}[\zeta]$. By definition of prime (page 87), this contradicts our assumption that α is prime. We conclude that $\alpha \nmid m$ for any m prime to q.

We now prove the statement of the problem. If $\alpha | n$, a rational integer, then α divides some prime factor of n. Since we've shown that α is not a factor of any $m \in \mathbb{Z}$ prime to q, it follows that that factor must be precisely q. Thus, n is a multiple of q, as desired.

■

4.16 Let $\mathbb{Q}_2$ be the set of all rational numbers $\frac{a}{b}$, where $a, b \in \mathbb{Z}$ and b is odd. Prove that $\mathbb{Q}_2$ is a domain, and that the only irreducibles in $\mathbb{Q}_2$ are 2 and its associates.

We begin by showing that $\mathbb{Q}_2$ is a domain. Let $\frac{a}{b}, \frac{x}{y}$ be two non-zero elements in $\mathbb{Q}_2$ and suppose, by way of contradiction, that

$$\left(\frac{a}{b}\right)\left(\frac{x}{y}\right) = 0$$

Multiplying both sides by xy, we have

$$\begin{aligned} 0 &= \frac{a}{b}\frac{x}{y} \\ &= \frac{ax}{by} \\ 0(by) &= ax \\ 0 &= ax \end{aligned}$$

Since $a, x \in \mathbb{Z}$, which *is* an integral domain, we have that either $a = 0$ or $x = 0$. This, however, implies that either $\frac{a}{b} = 0$ or $\frac{x}{y} = 0$, contradicting our initial assumption. It follows that $\mathbb{Q}_2$ is a domain.

We begin by identifying all units of $\mathbb{Q}_2$. Since $\frac{1}{b} \in \mathbb{Z}$ for b odd, **all odd integers are units**. We also know that if $b \in \mathbb{Q}_2$ for b odd, then $\frac{1}{b} \in \mathbb{Q}_2$. We therefore have the stronger statement: **if a and b are odd, then $\frac{a}{b}$ is a unit**. We also prove the converse, **if $\frac{a}{b}$ is a unit, then a and b are odd**: Suppose $\frac{a}{b} \in \mathbb{Q}_2$ is a unit. Then $\exists \frac{x}{y} \in \mathbb{Q}_2$ such that

$$\frac{a}{b}\frac{x}{y} = 1$$
$$ax = by \text{ (multiply by } by\text{)}$$

Since both b and y are odd (because $\frac{1}{b}, \frac{1}{y} \in \mathbb{Q}_2$), we have that both a and x are odd. Specifically, a and b are odd, as required. We now have a complete characterization of units: $\frac{a}{b}$ **is a unit iff both a and b are odd.**

Now suppose that $\alpha \in \mathbb{Q}_2$ is irreducible and a non-unit. Then $\alpha = \frac{a}{b}\frac{c}{d}$ and either $\frac{a}{b}$ or $\frac{c}{d}$ is a unit (but not both). Suppose, without loss of generality, that $\frac{a}{b}$ is a unit. Then, by above property, both a and b are odd. Rewriting the expression yields $bd\alpha = ac$. Now if c is odd, then the righthand side is odd so the expression $bd\alpha$ must also be odd. This forces α to be a unit, contradicting the non-unit property of α. Thus, $c = 2k$ for some $k \in \mathbb{Z}$. We now have the following equality

$$\alpha = \frac{2ak}{bd}$$

If $2|k$ then $\alpha = \frac{2}{1}\frac{ak}{bd}$ and both $\frac{2}{1}$ and $\frac{ak}{bd}$ have a factor of 2, and therefore not units. This contradicts the irreducibility of α because we've written α in terms of two non-units. Thus k is odd. We now have the following form: $\alpha = 2\frac{ak}{bd}$ where a, k, b, d are odd. Thus, the only irreducible elements are 2 and anything of the form $2u$ where u is a unit (associates of 2).

■