Homework 8

Kevin Guillen

MATH 200 — Algebra I — Fall 2021

May I have my proof for 11.3 graded please, thank you.

Problem 11.1 Prove the statements in Remark 11.2.

Proof. (a) $a \mid a$ and $a \mid 0$.

Proof. Given $a \in R$. We can consider the multiplicative identity $1 \in R$, we know that it satisfies $a1 = a$. Which by definition means $a \mid a$

Now consider $0 \in R$, by definition it satisfies for $a \in R$, that $a0 = 0$. Meaning $a \mid 0$. □

(b) $0 \mid a$ if and only if $a = 0$.

Proof. If $0 \mid a$ that means there exists $c \in R$ such that $0c = a$, but by definition a must be 0.

If $a = 0$ then from (a) we know $0 \mid 0$. □

(c) $u \mid a$.

Proof. Because u is a unit of R that means there exists $u^{-1} \in R$. We also know R is closed under multiplication therefore $u^{-1}a \in R$. Now consider the following,

$$u(u^{-1}a) = (uu^{-1})a = 1a = a$$

therefore $u \mid a$. □

(d) $a \mid u$ if and only if $a \in R^{\times}$.

Proof. Given $a \mid u$, it means there exists $b \in R$ such that $ab = u$. Since u is a unit there exists $u^{-1} \in R$ such that $uu^{-1} = 1$. Now consider the following,

$$\begin{aligned} uu^{-1} &= 1 \\ (ab)(ab)^{-1} &= 1 \\ (ab)(b^{-1}a^{-1}f &= 1 \\ aa^{-1} &= 1 \\ 1 &= 1. \end{aligned}$$

Therefore if $a \mid u$ then $a \in R^{\times}$.

Given $a \in R^{\times}$, then it follows from (c) that $a \mid u$. □

(e) If $a \mid b$ and $b \mid c$ then $a \mid c$.

Proof. Given that $a \mid b$ that means there exists $a' \in R$ such that $aa' = b$. Now given $b \mid c$ that means there exists $b' \in R$ such that $bb' = c$. Now consider the following,

$$\begin{aligned} bb' &= c \\ aa'b' &= c \\ a(a'b') &= c \qquad\qquad\qquad a'b' \in R \end{aligned}$$

therefore $a \mid c$. $\square$

(f) If $a \mid b_1, \dots, a \mid b_n$ then $a \mid r_1 b_1 + \cdots + r_n b_n$.

Proof. Given that $a \mid b_1, \dots, a \mid b_n$, then we know there exists $c_i \in R$ for $i \in \{1, \dots, n\}$ such that $ac_i = b_i$. Therfore,

$$r_1 b_1 + \cdots + r_n b_n = r_1(ac_1) + \cdots + r_n(ac_n)$$

and by definition of being in a ring we have distribution so therefore,

$$r_1 b_1 + \cdots + r_n b_n = a(r_1 c_1 + \cdots + r_n c_n).$$

Because $(r_1 c_1 + \cdots + r_n c_n) \in R$, that means $a \mid r_1 b_1 + \cdots + r_n b_n$ $\square$

(g) $a \mid b$ if and only if $bR \subseteq aR$.

Proof. Given that $a \mid b$, that means there exists $c \in R$ such that $ac = b$. Therefore for all $r \in R$ we have,

$$\begin{aligned} br = (ac)r &= a(cr) \qquad\qquad\qquad cr = r' \in R \\ &= ar' \in aR \end{aligned}$$

Therefore $bR \subseteq aR$.

Given that $bR \subseteq aR$, it means that for any $r \in R$ then there exists some $r' \in R$ such that $br = ar'$. Now consider the case where $r = 1$, then $b = ar'$ which means $a \mid b$. $\square$

(h) $\sim$ is an equivalance relation on R.

Proof. First we see if $a \sim a$ that means $a \mid a$ and $a \mid a$ which follows from (a).

Next we see if $a \sim b$ and $b \sim c$ that means $a \mid b$ and $b \mid c$. From (e) we know then that $a \mid c$. Next we know it means that $b \mid a$ and $c \mid b$, but it also follows from (e) that $c \mid a$. Meaning $a \sim c$.

Finally the symmetric follows trivially since $a \sim b$ implies $a \mid b$ AND $b \mid a$ which means $b \sim a$. $\square$

$\square$

Problem 11.3 Show that the ideal (X) of $\mathbb{Z}[X]$ is a prime ideal but not a maximal ideal.

Proof. Every $f(x) \in \mathbb{Z}[X]$ is of the form $\sum_{k=0}^{n} a_k x^k$ where a_0 is the constant term which is an integer. Now consider the following map,

$$\begin{aligned} \pi : \mathbb{Z}[X] &\to \mathbb{Z} \\ f(X) &\mapsto f(0) = a_0 \end{aligned}$$

This simply takes a polynomial and evaluates it at 0 which we know then is a ring homomorphism. This just leaves the constant term, a_0. Now we want to show that this map is surjective so let $b \in \mathbb{Z}$ be an arbitrary integer. We want to show that there exists a polynomial $f \in \mathbb{Z}[X]$ such that $\pi(f) = f(0) = b$. We know this f exists simply consider $f(X) = X + b$,

$$f(0) = 0 + b = b.$$

This shows that π is surective meaning $\mathrm{im}(\pi) = \mathbb{Z}$. Now if we consider the kernel of π it is simply

$$\ker(\pi) = \{f \mid f \in \mathbb{Z}[X], f(0) = 0\}$$

If $f \in \ker(\pi)$ that means then $f \in (X)$. As a matter of fact $\ker(\pi) = (X)$. This is because (X) is all polynomials with integer coefficients where every polynomial's constant term is 0. Therefore by the fundamental theorem of ring homomorphisms $\mathbb{Z}[X]/\ker(\pi) = \mathbb{Z}[X]/(X) \cong \mathrm{im}(\pi) = \mathbb{Z}$. Note though that $\mathbb{Z}$ is an integeral domain, and therefore so is $\mathbb{Z}[X]/(X)$ meaning (X) is a prime ideal. The reason it is not maximal is because $\mathbb{Z}$ is not a field, meaning $\mathbb{Z}[X]/(X)$ is not a field, so (X) cannot be maximal as we've proved in class. $\square$

Problem 12.6 Let $R = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. Computer the greatest common divisor of $\alpha = 10$ and $\beta = 1 - 5i$.

Solution. Let's consider the following,

$$\begin{aligned} 10 &= (2i)(1-5i) - 2i & \qquad N(-2i) &= 4 < N(1-5i) = 26 \\ 1 - 5i &= 2(-2i) + 1 - i & N(1-i) &= 2 < N(-2i) = 4 \\ -2i &= (1-i)(1-i) + 0 & & \end{aligned}$$

Thus $1 - i$ and its associates are the GCD of α and β $\square$

Problem 12.9 Show that the ring $R = \mathbb{Z}[\sqrt{2}] = \left\{a + b\sqrt{2} \mid a, b\mathbb{Z}\right\}$ is a Euclidean domain.

Proof. We already know that this ring forms an integral domain. Now let us consider the map given to us by,

$$\begin{aligned} N : R &\to \mathbb{N}_0 \\ a + b\sqrt{2} &\mapsto \left|a^2 - 2b^2\right| \end{aligned}$$

First we see that for $0 \in R$, $N(0) = 0^2 - 2 \cdot 0^2 = 0$. Now we want to show that this norm has a divison algorithm. Let α, $\beta \in \mathbb{Z}[\sqrt{2}]$, where $\beta \neq 0$. Then they are of the form $\alpha = x + y\sqrt{2}$, $\beta = w + z\sqrt{2}$. Consider the following,

$$\frac{\alpha}{\beta} = \frac{x + y\sqrt{2}}{w + z\sqrt{2}} = \frac{xw - 2yz + (yw - xz)\sqrt{2}}{w^2 - 2z^2}.$$

Now let $j, k \in \mathbb{Q}$, where $j = \frac{xw-2yz}{w^2-2z^2}$ and $k = \frac{(yw-xz)}{w^2-2z^2}$. Now let $n, m \in \mathbb{Z}$ be the smallest integers such that,

$$|j - n| \leqslant \frac{1}{2}$$
$$|k - m| \leqslant \frac{1}{2}$$

Now let γ be defined as the following,

$$\gamma = (j - n) + (k - m)\sqrt{2} = j + k\sqrt{2} - n - m\sqrt{2} = \frac{\alpha}{\beta} - (n + m\sqrt{2})$$

.

We then get the following,

$$\gamma = \frac{\alpha}{\beta} - (n + m\sqrt{2})$$
$$\beta\gamma = \alpha - \beta(n + m\sqrt{2})$$
$$\beta\gamma + \beta(n + m\sqrt{2}) = \alpha$$

where $(n + m\sqrt{2})$ and $\beta\gamma \in \mathbb{Z}[\sqrt{2}]$.

Now consider the norm of γ, which will be $\left|(j-n)^2 - 2(k-m)^2\right|$, using the triangle inequality and how we chose n and m we get the following,

$$\left|(j-n)^2 - 2(k-m)^2\right| \leqslant |j-n|^2 + 2\,|k-m|^2 \leqslant \frac{1}{4} + 2\frac{1}{4} = \frac{3}{4}$$

This is useuful to us because by definition we need $N(\beta\gamma) < N(\beta)$, where $\beta\gamma$ is the remainder when dividing α by β. We see this is true because consider the following,

$$N(\beta\gamma) = N(\beta)N(\gamma) \leqslant N(\beta)\frac{3}{4}$$

which is obviously less than $N(\beta)$. This means then that $\mathbb{Z}\sqrt{2}$ is indeed a Euclidean Domain since all together we have $\alpha = \beta(n + m\sqrt{2}) + \beta\gamma$ where $N(\beta\gamma) < N(\beta)$, and $(n + m\sqrt{2}), \beta\gamma \in \mathbb{Z}[\sqrt{2}]$ $\square$