Solutions to Exercise Sheet 8

Solution 8.1. *Examples of norms of ideals.*

(1) Using the formula in Example 6.18, we have $N(\alpha) = a^2 - b^2 d$. By Proposition 8.9, $N(I) = |N(\alpha)| = |a^2 - b^2 d|$.

(2) By Lemma 6.16, we have $N(a) = a^n N(1) = a^n$. (We can also do it by writing down a matrix for L_a, which is a diagonal matrix with a's along the diagonal.) By Proposition 8.9, $N(I) = |N(a)| = |a^n|$.

Solution 8.2. *Examples of sums and products of ideals.*

(1) We show $IJ \subseteq I$. Every element in IJ has the form $a_1b_1 + a_2b_2 + \cdots + a_kb_k$ for some positive integer k, where $a_i \in I$, $b_i \in J$ for each $i = 1, 2, \cdots, k$. Since $a_i \in I$ and $b_i \in J \subseteq R$, we have $a_ib_i \in I$ for each i. Hence their sum $a_1b_1 + a_2b_2 + \cdots + a_kb_k \in I$. We then show $I \subseteq I + J$. For every element $a \in I$, we have $a = a + 0 \in I + J$ since $0 \in J$. Both claims are proved.

(2) We need to show mutual inclusions. First we show $(\alpha)I \supseteq \{\alpha a \mid a \in I\}$. This is clear because $\alpha \in (\alpha)$ and $a \in I$ imply $\alpha a \in (\alpha)I$. Then we show the other inclusion $(\alpha)I \subseteq \{\alpha a \mid a \in I\}$. Every element in (α) has the form $r\alpha$ for some $r \in R$. By the definition of the product of two ideals, every element in $(\alpha)I$ can be written as a finite sum $r_1\alpha a_1 + r_2\alpha a_2 + \cdots + r_k\alpha a_k$ for some positive integer k, where $r_1, \cdots, r_k \in R$ and $a_1, \cdots, a_k \in I$. Since I is an ideal, we know that $r_ia_i \in I$ for each $i = 1, \cdots, k$, hence $\gamma = r_1a_1 + \cdots + r_ka_k \in I$. Therefore $r_1\alpha a_1 + r_2\alpha a_2 + \cdots + r_k\alpha a_k = \alpha(r_1a_1 + \cdots + r_ka_k) = \alpha\gamma$ has the required form.

(3) We need to show mutual inclusions. First we show $(\alpha)(\beta) \supseteq (\alpha\beta)$. Every element in $(\alpha\beta)$ has the form $r\alpha\beta$ for some $r \in R$. since $r\alpha \in (\alpha)$ and $\beta \in (\beta)$, we know that $r\alpha\beta \in (\alpha)(\beta)$. We then show the other inclusion $(\alpha)(\beta) \subseteq (\alpha\beta)$. By part (2) we know $(\alpha)(\beta) = \{\alpha\gamma \mid \gamma \in (\beta)\}$, hence every element in $(\alpha)(\beta)$ has the form $\alpha\gamma$ for some $\gamma \in (\beta)$. We write $\gamma = \beta\delta$ for some $\delta \in R$, then $\alpha\gamma = \alpha\beta\delta \in (\alpha\beta)$.

(4) We need to show two directions. First we show every element in (x, y) is a polynomial with zero constant term. Since (x, y) is defined to be the sum of ideals $(x) + (y)$, every element in it has the form $xf + yg$ for some $f, g \in \Bbbk[x, y]$. Every term in the expansion of $xf + yg$ has either a factor of x (if it comes from xf) or a factor of y (if it comes from yg). Hence the expansion of $xf + yg$ is a polynomial with zero constant term. Now we show that every polynomial $h \in \Bbbk[x, y]$ with zero constant term is an element in (x, y). Since h has zero constant term, every non-zero term in h has a factor x or y (possibly both). Now we write h as the sum of two polynomials $h = h_1 + h_2$ as follows: if a term in h is divisible by x but not divisible by y, then it becomes a term in h_1; if it is divisible by y but not by x,

then it becomes a term in h_2; if it is divisible by both x and y, then it becomes a term in either h_1 or h_2 (the one of your choice). Now we realise that every term in h_1 is divisible by x, hence we can write $h_1 = xf$ for some $f \in \Bbbk[x, y]$. Similarly every term in h_2 is divisible by y, hence we can write $h_2 = yg$ for some $g \in \Bbbk[x, y]$. Therefore $h = xf + yg \in (x) + (y) = (x, y)$.

Solution 8.3. *Examples of prime and maximal ideals.*

(1) It is clear that (p) is a proper ideal since $1 \notin (p)$. We first show (p) is a prime ideal. If $ab \in (p)$ for some $a, b \in \mathbb{Z}$, then $p \mid ab$. Since p is a prime, $p \mid a$ or $p \mid b$, which means either $a \in (p)$ or $b \in (p)$. Hence (p) is a prime ideal. We then show (p) is a maximal ideal. Assume there is an ideal I such that $(p) \subseteq I \subseteq \mathbb{Z}$. Since $\mathbb{Z}$ is a PID, $I = (a)$ is a principal ideal generated by some $a \in \mathbb{Z}$. Then we have $(p) \subseteq (a) \subseteq \mathbb{Z}$, which implies that $p \in (a)$, hence $a \mid p$. It follows that $a = \pm 1$ or $\pm p$. In other words, $I = (a) = (1) = \mathbb{Z}$ or $I = (a) = (p)$. Hence (p) is a maximal ideal.

(2) It is clear that (x) is a proper ideal since the constant polynomial $1 \notin (x)$. We first show (x) is a prime ideal. If $fg \in (p)$ for some $f, g \in \Bbbk[x]$, then $x \mid fg$. Hence either f or g has a factor x, which means either $f \in (x)$ or $g \in (x)$. Hence (x) is a prime ideal. We then show (x) is a maximal ideal. Assume there is an ideal I such that $(x) \subseteq I \subseteq \Bbbk[x]$. Since $\Bbbk[x]$ is a PID, $I = (h)$ is a principal ideal generated by some $h \in \Bbbk[x]$. Then we have $(x) \subseteq (h) \subseteq \Bbbk[x]$, which implies that $x \in (h)$, hence h is a factor of x. It follows that h is a non-zero constant polynomial or a non-zero constant multiple of x. Since every non-zero constant polynomial is a unit in $\Bbbk[x]$, if h is a non-zero constant, then $I = (h) = \Bbbk[x]$; if h is a non-zero constant multiple of x, then $I = (h) = (x)$. Hence (x) is a maximal ideal.

(3) By Exercise 8.2 (4), every element in (x, y) is a polynomial with zero constant term. Hence the constant polynomial $1 \notin (x, y)$, and (x, y) is a proper ideal. We first show that (x, y) is a prime ideal. Assume $fg \in (x, y)$ for some $f, g \in \Bbbk[x, y]$. Then fg has a zero constant term. It follows that either f or g has a zero constant term (otherwise the constant term of fg, as a product of two non-zero constant terms, is non-zero). This shows that either f or g is an element in (x, y), hence (x, y) is a prime ideal. We then show that (x, y) is a maximal ideal. Assume $(x, y) \subseteq I \subseteq \Bbbk[x, y]$. Then either $I = (x, y)$ or I contains some polynomial h with a non-zero constant term. In the second possibility, we write $h = h_0 + c$ where c is the constant term of h while h_0 is the sum of all other terms in h. Since $h \in I$ and $h_0 \in (x, y) \subseteq I$, we know that $c = h - h_0 \in I$. However c is a unit in $\Bbbk[x, y]$, hence $I = \Bbbk[x, y]$. We have proved that an intermediate ideal I is either (x, y) or $\Bbbk[x, y]$. Therefore (x, y) is a maximal ideal.

We now look at the ideal (x). Clearly $1 \notin (x)$, hence (x) is a proper ideal. We first show (x) is a prime ideal. If $fg \in (p)$ for some $f, g \in \Bbbk[x, y]$, then $x \mid fg$. Hence either f or g has a factor x, which means either $f \in (x)$ or $g \in (x)$. Hence (x) is a prime ideal. Then we show that (x) is not a maximal ideal. Indeed, it is clear that every polynomial in (x) is a multiple of x, hence has zero constant term. It follows that $(x) \subseteq (x, y)$. Since y is a polynomial in (x, y) but not in (x), we get the strict inclusions $(x) \subsetneq (x, y) \subsetneq \Bbbk[x, y]$, which shows that (x) is not maximal.

Solution 8.4. *Cancellation law and "to contain is to divide".*

(1) By Proposition 8.13, there is an ideal J such that $IJ = (\gamma)$ is a non-zero principal ideal. Multiply $IJ_1 = IJ_2$ on both sides by J. We find $(\gamma)J_1 = (\gamma)J_2$.

We show that $J_1 \subseteq J_2$. For any element $\alpha \in J_1$, we know that $\gamma\alpha \in (\gamma)J_1$ hence $\gamma\alpha \in (\gamma)J_2$. By Exercise 8.2 (2), we know that every element in $(\gamma)J_2$ can be written as $\gamma\beta$ for some $\beta \in J_2$. It follows that $\gamma\alpha = \gamma\beta$. Since $\gamma \neq 0$, we have $\alpha = \beta \in J_2$. This shows $J_1 \subseteq J_2$. By switching subscripts we can show that $J_2 \subseteq J_1$ using the same argument. Hence $J_1 = J_2$.

(2) If $I_2 = 0$, then $I_1 = 0$, hence we can choose J to be any ideal in $\mathcal{O}_K$. If $I_2 \neq 0$, then by Proposition 8.13, there is an ideal I_3 and $\gamma \neq 0$ such that $I_2 I_3 = (\gamma)$. Hence we have $I_1 I_3 \subseteq I_2 I_3 = (\gamma)$. We define $J = \{\alpha \in \mathcal{O}_K \mid \gamma\alpha \in I_1 I_3\}$.

We show that J is an ideal in $\mathcal{O}_K$. For any $\alpha_1, \alpha_2 \in J$, we have $\gamma\alpha_1, \gamma\alpha_2 \in I_1 I_3$. Since $I_1 I_3$ is an ideal, we get $\gamma(\alpha_1 + \alpha_2) = \gamma\alpha_1 + \gamma\alpha_2 \in I_1 I_3$. By the definition of J, $\alpha_1 + \alpha_2 \in J$. On the other hand, for any $\alpha \in J$ and any $\beta \in \mathcal{O}_K$, since $\alpha\gamma \in I_1 I_3$ and $I_1 I_3$ is an ideal, we know that $\beta\alpha\gamma \in I_1 I_3$. It follows that $\beta\alpha \in J$ by the definition of J. These two conditions prove J is an ideal in $\mathcal{O}_K$.

We claim that $(\gamma)J = I_1 I_3$. First we show that $(\gamma)J \subseteq I_1 I_3$. By Exercise 8.2 (2), every element in $(\gamma)J$ can be written as $\gamma\alpha$ for some $\alpha \in J$. By the definition of J, we have $\gamma\alpha \in I_1 I_3$. Hence $(\gamma)J \subseteq I_1 I_3$. To show the other inclusion, assume we have $\beta \in I_1 I_3$. Since $I_1 I_3 \subseteq (\gamma)$, we know $\beta \in (\gamma)$ hence $\beta = \gamma\alpha$ for some $\alpha \in \mathcal{O}_K$. In fact, by the definition of J we actually have $\alpha \in J$. Hence $\beta = \gamma\alpha \in (\gamma)J$, which shows that $I_1 I_3 \subseteq (\gamma)J$. The mutual inclusions show that $(\gamma)J = I_1 I_3$. It follows that $I_1 I_3 = (\gamma)J = I_2 I_3 J$. By Corollary 8.14 which we have proved in part (1), we can cancel I_3 on both sides and conclude $I_1 = I_2 J$.