Mathematics GU4042 Modern Algebra II
Assignment # 3

Benjamin Church

December 21, 2017

Page 138.

2. It suffices to show that $\mathbb{Z}[i]$ is a Euclidean Domain and then apply problem 3 to conclude that $\mathbb{Z}[i]$ is a PID. Define $N : \mathbb{Z}[i] \to \mathbb{N}$ by $N(a + ib) = |a + ib|^2 = a^2 + b^2$. By Lemma 0.1, N extends to a function $\mathbb{Q}[i] \to \mathbb{Q}^+ \cup \{0\}$ which is totally multiplicative.

   Take $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$. Then since $\mathbb{Q}[i] \cong Q_{Z[i]}$ we have $\frac{\alpha}{\beta} \in \mathbb{Q}[i]$ so $\frac{\alpha}{\beta} = p + iq$ with $p, q \in \mathbb{Q}$. Now, consider the best integer approximations of p and q, namely, n and k s.t. $|p - n| \leq \frac{1}{2}$ and $|q - n| \leq \frac{1}{2}$. These approximations exist by Lemma 0.2. Let $\gamma = n + ik \in \mathbb{Z}[i]$ and $\delta = \alpha - \beta\gamma \in \mathbb{Z}[i]$. Consider,

$$N(\delta) = N(\alpha - \beta\gamma) = N(\beta) N\left(\frac{\alpha}{\beta} - \gamma\right) = N(\beta)\left[(p-n)^2 + (q-k)^2\right] \leq N(\beta)\left(\frac{1}{4} + \frac{1}{4}\right) < N(\beta)$$

   Thus, $\alpha = \beta\gamma + \delta$ with $N(\delta) < N(\beta)$ and $\gamma, \delta \in \mathbb{Z}[i]$ so $\mathbb{Z}[i]$ is a Euclidean Domain.

3. Let R be a Euclidean Domain with a function $\varphi : R \backslash \{0_R\} \to \mathbb{N}$. Explicitly, for every $a, b \in R$ with $b \neq 0$ there exists $q, r \in R$ s.t. $a = bq + r$ and either $r = 0$ or $\varphi(r) < \varphi(q)$.

   Consider an ideal $I \subset R$. If $I = (0)$ then it is principal. Otherwise, $\varphi(I \backslash \{0_R\}) \subset \mathbb{N}$ is not empty so by well-ordering, it has a least element k. Since $g \in \varphi(I \backslash \{0_R\})$, $\exists g \in I$ s.t. $\varphi(g) = k$ and $g \neq 0_R$. Thus, for any $a \in I$, by the Euclidean property, $\exists q, r \in R$ s.t. $a = gq + r$. Now $r = a - gq \in I$ because $a, g \in I$ and I is an ideal. However, unless $r = 0$, $\varphi(r) < \varphi(g)$ which is a contradiction because $r \in I$ and $\varphi(g) = k$ the least element of $\varphi(I \backslash \{0_R\})$. Therefore, $r = 0$ so $g \mid a$. Thus, $\forall a \in I : a \in (g)$ so $I \subset (g)$ and because $g \in I$ by closure and absorption we also have that $(g) \subset I$. Therefore, $I = (g)$ so every ideal is principal.

9. Suppose K is a field and a polynomial $f \in K[X]$ has degree 2 or 3. If f has a root α in K then $X - \alpha \mid f$. Thus, $f = (X - \alpha)g$. Also, $\deg f = \deg(X - a) + \deg g = 2$ or 3 so $\deg g = 1$ or 2. Therefore, g is not a unit because K is a domain and thus the only units of $K[X]$ are the units of K which have degree 0. Thus, f is reducible in $K[X]$.

   Consider $\deg f = 2$ or 3 and f is reducible. Then $f = gh$ for $g, h \in K[X]$ and $g, h \notin K[X]^\times$. However, K is a field so $K[X]^\times = K^\times = K \setminus \{0\}$. Therefore, $\deg g, \deg h \geq 1$ but $\deg g + \deg h = \deg f = 2$ or 3. The only solutions are $\deg g = 1$, $\deg h = 2$ or $\deg g = 2$, $\deg h = 1$. WLOG take $\deg g = 1$ and $\deg h = 2$. Thus $g = aX + b$ for $a, b \in K$ and $a \neq 0$. Now since K is a field and $a \neq 0$ then $-\frac{b}{a} \in K$ so consider

$$f\left(-\frac{b}{a}\right) = \left(-\frac{b}{a}a + b\right) h\left(-\frac{b}{a}\right) = 0 \cdot h\left(-\frac{b}{a}\right) = 0$$

Thus, f has a root in K. Therefore, f has a root in K iff f is reducible in $K[X]$. Equivalently, f is irreducible in $K[X]$ iff f has no roots in K.

10. $X^5+X^3-X^2-1 = X^3(X^2+1)-(X^2+1) = (X^3-1)(X^2+1) = (X-1)(X^2+X+1)(X^2+1)$ The first factor is irreducible over $\mathbb{R}$ because it has degree 1. The other two factors are irreducible over $\mathbb{R}$ by problem 9 because they have degree 2 and no roots in $\mathbb{R}$. This can be shown by considering the discriminant $\Delta = b^2-4ac$ which cannot be negative if the quadratic equation has roots in $\mathbb{R}$. However, $\Delta_{X^2+X+1} = 1-4 = -3 < 0$ and $\Delta_{X^2+1} = 0-4 = -4 < 0$.

Lemmas

Lemma 0.1. *$N : \mathbb{Q}[i] \to \mathbb{Q}^+ \cup \{0\}$ given by $N(p+iq) = p^2+q^2$ is multiplicative and* $\operatorname{Im} N|_{Z[i]} \subset \mathbb{N}$.

Proof. Take $\alpha = 1+iq_1, \beta = p_2+iq_2 \in \mathbb{Q}[i]$ then $N(p_1+iq_1) = p_1^2+q_1^2 \in \mathbb{Q}^+ \cup \{0\}$. Thus,

$$\begin{aligned} N(\alpha\beta) &= N(p_1p_2 - q_1q_2 + i(p_1q_2+p_2q_1)) = (p_1p_2-q_1q_2)^2 + (p_1q_2+p_2q_1)^2 \\ &= p_1^2p_2^2 - 2p_1p_2q_1q_2 + q_1^2q_2^2 + p_1^2q_2^2 + 2p_1q_2p_2q_1 + p_2^2q_1^2 \\ &= p_1^2p_2^2 + q_1^2q_2^2 + p_1^2q_2^2 + p_2^2q_1^2 = (p_1^2+q_1^2)(p_2^2+q_2^2) = N(\alpha)N(\beta) \end{aligned}$$

Finally, if $\alpha \in \mathbb{Z}[i]$ then $\alpha = a+ib$ with $a, b \in \mathbb{Z}$ so $N(\alpha) = a^2+b^2 \in \mathbb{N}$. $\square$

Lemma 0.2. *$\forall r \in \mathbb{R} : \exists z \in \mathbb{Z}$ s.t. $|z-r| \leq \frac{1}{2}$. In particular, this holds for $r \in \mathbb{Q}$.*

Proof. Consider $S = \{n \in \mathbb{Z} \mid r < n+1\}$. S is non-empty because $\mathbb{Z}$ is unbounded but S is bounded below by r so by well ordering, S has a least element z. Since $z \in S$, $r < z+1$. Suppose that $r < z$ then $z-1 \in S$ contradicting the fact that z is the least element. Thus, $z \leq r < z+1$.

Now if $|r-z| < \frac{1}{2}$ then we are done. Else, $|r-z| = r-z \geq \frac{1}{2}$ so $1-\frac{1}{2} \geq z+1-r$ so $(z+1)-r \leq \frac{1}{2}$. However, $z+1 > r$ so $|(z+1)-r| \leq \frac{1}{2}$ and $z+1 \in \mathbb{Z}$. $\square$