Sixth Homework Assignment

Please pledge this whole homework: no help from anyone (or any resources other than your book) for any of the problems.

Turn-in problems due 10/24: Chapter 18 8,18,20,26,32; Chapter 19 4,10,16,24,30

8: Suppose that $u$ is a unit in the Euclidean Domain $D$ with measure $d$. According to the measure equation, $d(u) \leq d(ub)$ for any $b \in D$. If we choose $b = u^{-1}$, then we get $d(u) \leq d(uu^{-1}) = d(1)$. Similarly, we get $d(1) \leq d(1 \cdot b)$ for any $b \in D$, so choose $b = u$ to get $d(1) \leq d(u)$. The combination of the two inequalities yields $d(u) = d(1)$. Now suppose that $d(u) = d(1)$: we want to show that $u$ is a unit. By the division algorithm part of the definition of a measure, we have that $1 = uq + r$ where $d(r) < d(u)$ or $r = 0$. If $r \neq 0$, since $d(u) = d(1)$, this is the same as saying that $d(r) < d(1)$, but the other part of the definition of measure implies that $d(1) \leq d(1 \cdot r)$. The contradiction implies that $r = 0$. Thus, $1 = uq$ and $u$ is a unit.

18: Suppose that $7 = ab$ for $a, b \in \mathbb{Z}[^{\sqrt{6}}]$ (we want to show that either $a$ is a unit or $b$ is). We use the norm that is defined on $\mathbb{Z}[^{\sqrt{6}}]$, namely $N(x + y\sqrt{6}) = |x^2 - 6y^2|$. If $a = x + y\sqrt{6}$ and $b = z + w\sqrt{6}$, then $49 = N(7) = N(ab) = |x^2 - 6y^2||z^2 - 6w^2|$. If neither of these is a unit, then $|x^2 - 6y^2| = 7$. If we read the equation mod 7, we get $x^2 + y^2 = 0$ mod 7 (remember that $6 = -1$ mod 7). Since $x^2 = 1, 2, \text{ or } 4$ mod 7 and the same for $y^2$ (unless they are 0 mod 7 which implies they are divisible by 7), and there are no solutions to the equation $x^2 + y^2 = 0$ mod 7 other than $x = y = 0$ mod 7. If both $x$ and $y$ are divisible by 7, then the norm is divisible by 49 and hence must be 49, which implies that $N(b) = 1$ and $b$ is a unit. This implies that 7 is irreducible but $N(7)$ is not prime.

20: To show that $\mathbb{Z}[^{\sqrt{-3}}]$ is not a PID, we show that it is not a UFD. Example 1 on page 321 shows that $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ where $2, (1 + \sqrt{-3}), \text{ and } (1 - \sqrt{-3}$ are all irreducible. The units in $\mathbb{Z}[^{\sqrt{-3}}]$ are those elements with norm 1, and that is only $\pm 1$. Thus, 4 is a product of irreducibles in two different ways that are not just unit multiples different from each other, implying that $\mathbb{Z}[^{\sqrt{-3}}]$ is not a UFD. Theorem 18.2 implies that it cannot be a PID.
26: If \(ab\) is a unit in \(\mathbb{Z}[^d]\) under the conditions of the problem, then the norm identifies units by \(N(u) = 1\) if and only if \(u\) is a unit. Since the norm is multiplicative, we get \(1 = N(ab) = N(a)N(b)\), but the only way to get two positive integers to multiply to get 1 is if \(N(a) = N(b) = 1\). This implies that \(a\) and \(b\) are both units.

32: Let \(D\) be an integral domain with the descending chain condition, and let \(a\) be a nonzero element of \(D\). Consider the chain of ideals \(\langle a \rangle \subseteq \langle a^2 \rangle \subseteq \langle a^3 \rangle \subseteq \cdots\). Since this chain must be finite, we must have \(\langle a^k \rangle = \langle a^{k+1} \rangle\) for some \(k\). This implies that \(a^k \in \langle a^{k+1} \rangle\), so \(1 \cdot a^k = ca^{k+1}\). Since we are in a domain, we can cancel \(a^k\) from both sides leaving \(1 = ca\). This implies that \(a\) is a unit, so all nonzero elements of the domain are units. Thus, \(D\) is a field.

4: The “one-step subspace test” requires \(cv + dw\) to be in the subspace whenever \(v, w\) are in the subspace (\(c\) and \(d\) are scalars). If we have \(\Sigma a_i v_i \) and \(\Sigma b_i v_i\) are arbitrary elements of \(\langle v_1, v_2, \ldots, v_n \rangle\), then \(c\Sigma a_i v_i + d\Sigma b_i v_i = \Sigma (ca_i + db_i) v_i \in \langle v_1, v_2, \ldots, v_n \rangle\). Thus, \(\langle v_1, v_2, \ldots, v_n \rangle\) is a subspace.

10: Let \(V\) be a finite dimensional vector space and let \(S = \{v_1, v_2, \ldots, v_n\}\) be a linearly independent subset of \(V\). If the vectors in \(S\) span \(V\), then \(S\) is a basis for \(V\) and we are done. If the vectors in \(S\) don’t span \(V\), then choose \(w_1 \in V - \text{Span}(S)\), and consider the collection of vectors \(S_1 = \{v_1, v_2, \ldots, v_n, w_1\}\). I claim the vectors in \(S_1\) are linearly independent. To see this, suppose \(a_1 v_1 + \cdots + a_n v_n + b_1 w_1 = 0\). If \(b_1 \neq 0\), then we have \(w_1 = (a_1 b_1^{-1}) v_1 + \cdots + (a_n b_n^{-1}) v_n\), which would imply that \(w_1\) was in the span of \(S\). Since it is not, we must have \(b_1 = 0\). That reduces our equation to \(a_1 v_1 + \cdots + a_n v_n = 0\), and the fact that the \(v_i\) are linearly independent implies that all of the \(a_i\) must be 0. Thus, \(S'\) is a collection of linearly independent vectors. If they span \(V\), then we are done. If they don’t, continue adding \(w_i\) one at a time until you get a spanning set. You know you will eventually get a spanning set since the vector space is finite dimensional (we can’t have a linearly independent set with more vectors than the dimension of the space).

16: All we need to do is to show that this is a subspace of all matrices of this form, so we use the one-step subspace test. If we have \(\begin{pmatrix}a_1 & b_1 \\ b_1 & c_1\end{pmatrix}\) and \(\begin{pmatrix}a_2 & b_2 \\ b_2 & c_2\end{pmatrix}\) as arbitrary elements of \(V\), then
$d_1 \left( \begin{array}{cc} a_1 & b_1 \\ b_1 & c_1 \end{array} \right) + d_2 \left( \begin{array}{cc} a_1 & b_1 \\ b_1 & c_1 \end{array} \right) = \left( \begin{array}{cc} d_1 a_1 + d_2 a_2 & d_1 b_1 + d_2 b_2 \\ d_1 b_1 + d_2 b_2 & d_1 c_1 + d_2 c_2 \end{array} \right)$. Since this matrix has the appropriate form (the top left and bottom right entries are equal), we have that $V$ is a subspace. A basis for this subspace is $\left( \begin{array}{cc} 1 & 0 \\ 0 & 0 \end{array} \right)$, $\left( \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right)$, and $\left( \begin{array}{cc} 0 & 0 \\ 0 & 1 \end{array} \right)$ (there are plenty of other correct answers for this).

24: Let $v_1$ and $v_2$ be arbitrary elements of $U \cap W$. Since $v_1$ and $v_2$ are both in $U$, it must be the case that $cv_1 + dv_2 \in U$ for any scalars $c, d$. Similarly, $cv_1 + dv_2 \in W$, so $cv_1 + dv_2 \in U \cap W$ as required and $U \cap W$ is a subspace. If $u_1 + w_1$ and $u_2 + w_2$ are arbitrary elements of $U + W$, then $c(u_1 + w_1) + d(u_2 + w_2) = (cu_1 + du_2) + (cw_1 + dw_2) \in U + W$. This implies that $U + W$ is a subspace.

30: Let $T$ be an onto linear transformation from $V$ onto $W$, and let $w$ be an arbitrary element of $W$. Since $T$ is onto, there is a $v \in V$ so that $T(v) = w$. Since $\{v_1, v_2, \ldots, v_n\}$ spans $V$, there are scalars $a_i$ so that $v = a_1 v_1 + \cdots + a_n v_n$. By properties of linear transformations, we have that $w = T(v) = T(a_1 v_1 + \cdots + a_n v_n) = a_1 T(v_1) + \cdots + a_n T(v_n)$. Therefore, $\{T(v_1), \ldots, T(v_n)\}$ spans $W$.

**Problem, 20 points:** (Euclid’s algorithm for finding the greatest common divisor in a Euclidean domain). Let $a_1, a_2$ be non-zero elements of a Euclidean Domain $D$, where $\delta$ is the measure function for $D$. Define $a_i$ and $q_i$ recursively by $a_1 = q_1 a_2 + a_3, a_i = q_i a_{i+1} + a_{i+2}$ where $\delta(a_{i+2}) = 0$ or $\delta(a_{i+2}) < \delta(a_{i+1})$. Show that there exists an $n$ such that $a_n \neq 0$ but $a_{n+1} = 0$, and that $d = a_n$ is the greatest common divisor of $a_1$ and $a_2$. Also use the equations to obtain an expression for $d$ in the form $xa_1 + ya_2$ for $x, y \in D$.

Define everything as above. Since the sequence of domain elements $a_1, a_2, \ldots, a_n$ satisfies $\delta(a_{i+2}) < \delta(a_{i+1})$ or $a_{i+2} = 0$, we must have that there is an $a_n = 0$ for some $n$ (otherwise, there would be in infinitely strictly decreasing sequence of positive integers, but that sequence would have to go negative at some point if it didn’t terminate). To show that $a_n$ is the greatest common divisor of $a_1$ and $a_2$, we must first show that it divides them and then show that any other divisor must divide $a_n$. To show the first, we observe that $a_{n-1} = q_{n-1} a_n + a_{n+1} = q_{n-1} a_n$, so $a_n | a_{n-1}$. Going back another step, we see that $a_{n-2} = q_{n-2} a_{n-1} + a_n = q_{n-2} (q_{n-1} a_n) + a_n$, implying that $a_n | a_{n-2}$. We continue in this manner: if we already have that $a_i = q a_n$ for some $q$ and $a_{i+1} = q' a_n$ for some
\[ q', \] then \( a_{i-1} = q_i a_i + a_{i+1} = q_i - 1 q a_n + q' a_n, \] which implies that \( a_n | a_i \) (this is a reverse induction). Therefore, \( a_n | a_1 \) and \( a_n | a_2 \). Now suppose that \( e | a_1 \) and \( e | a_2 \). By the equation \( a_1 = q_1 a_2 + a_3 \) we get that \( e | a_3 \). Similarly, by the equation \( a_2 = q_2 a_3 + a_4 \) we get \( e | a_4 \). Continuing in this manner we get \( e | a_n \). Thus, \( a_n \) is the greatest common divisor of \( a_1 \) and \( a_2 \). Finally, we feed all of the equations back into each other to get:

\[
\begin{align*}
a_3 &= a_1 - q_1 a_2 \\
a_4 &= (-q_2) a_1 + (1 + q_1 q_2) a_2 \\
a_5 &= (1 + q_2 q_3) a_1 + (-q_1 - q_3 + q_2 q_3 - q_1 q_2 q_3) a_2 \\
&\vdots \: \vdots \: \vdots \n\end{align*}
\]

\[ a_n = (Q_{n-2,1} - q_{n-2} Q_{n-1,1}) a_1 + (Q_{n-2,2} - q_{n-2} Q_{n-1,2}) a_2 \]

The last equality uses the inductive assumption that \( a_{n-2} = Q_{n-2,1} a_1 + Q_{n-2,2} a_2 \) for some \( Q_{n-2,1} \) and \( Q_{n-2,2} \); \( a_{n-1} = Q_{n-1,1} a_1 + Q_{n-1,2} a_2 \) for some \( Q_{n-1,1} \) and \( Q_{n-1,2} \); and \( a_n = -q_{n-2} a_{n-1} + a_{n-2} \). This proves the claim.