MATH 431 Written Homework 4 Solution Radford 02/07/09

Let R be a commutative ring with unity. Recall that $R^{\times}$ denotes the multiplicative group of units of R. Let $a \in R$. Throughout $R = D$ is an integral domain.

---

1. Page 334, number 22: (**20 points**) We base our solution on the discussion of Example 1 on page 321 of the text.

$D = \mathbf{Z}[\sqrt{5}]$. By the Eisenstein Criterion $x^2 - 5 \in \mathbf{Q}[x]$ is irreducible. Therefore all elements of $x \in D$ have a unique expression $x = m + n\sqrt{5}$, where $m, n \in \mathbf{Z}$. In particular $N : D \longrightarrow \{0, 1, 2, 3, \ldots\}$ defined by

$$N(m + n\sqrt{5}) = |(m + n\sqrt{5})\overline{(m + n\sqrt{5})}| = |(m + n\sqrt{5})(m - n\sqrt{5})||m^2 - 5n^2|$$

is multiplicative and $x \in D^{\times}$ if and only if $N(x) = 1$.

Note that

$$2{\cdot}2 = 4 = (1 + \sqrt{5})(-1 + \sqrt{5}) \qquad (1)$$

and $2, 1 + \sqrt{5}, -1 + \sqrt{5}$ are distinct. We first show that these elements are irreducible.

Observe that $4 = N(2) = N(1+\sqrt{5}) = N(-1+\sqrt{5}) = 4$. Since $N(\ )$ is multiplicative, to show that $2, 1 + \sqrt{5}, -1 + \sqrt{5}$ are irreducible we need only show that $N(x) = 2$ is not possible for $x = m + n\sqrt{2} \in D$ (**5**).

Suppose that $N(x) = 2$; that is $m^2 - 5n^2 = \pm 2$. Then m, n are even or m, n are odd. In the first case $m = 2\ell$ and $n = 2k$, for some $k, \ell \in \mathbf{Z}$. Therefore $m^2 - 5n^2 = 4k^2 - 5(4\ell^2) = 4(k^2 - 5\ell^2)$ which does not divide ± 2. In the second case $m = 2k + 1$ and $n = 2\ell + 1$ for some $k, \ell \in \mathbf{Z}$. But then

$$m^2 - 5n^2 = (4k^2 + 4k + 1) - 5(4\ell^2 + 4\ell + 1) = 4(k^2 + k - \ell^2 - \ell - 1)$$

does not divide ± 2. Therefore $N(x) = 2$ is not possible (**5**). We have shown that $2, 1 + \sqrt{5}, -1 + \sqrt{5}$ are irreducible.

Now we show that these elements are not prime. Suppose that 2 is prime. Then from (1) we conclude that 2 divides $1 + \sqrt{5}$ or $-1 + \sqrt{5}$; that is $2(m + n\sqrt{5})$ is $1 + \sqrt{5}$ or $-1 + \sqrt{5}$ for some $m, n \in \mathbf{Z}$. But $2m = \pm 1$ is not possible. Therefore 2 is not prime (**5**).

Suppose that $1 + \sqrt{5}$ is prime. Then from (1) we see that $2 = (1 + \sqrt{5})(m + n\sqrt{5}) = (m + 5n) + (m + n)\sqrt{5}$, for some $m, n \in \mathbf{Z}$. But then $m + 5n = 2$ and $m + n = 0$ from which we conclude that $m = -n$ and $4n = 2$, a contradiction. Therefore $1 + \sqrt{5}$ is not prime (**5**).

2. Page 334, number 32: (**20 points**) The hypothesis is equivalent to every descending chain of ideals of D must terminate (stabilize).

Let $a \in D$ be a non-zero element. Then the descending chain of ideals

$$Ra \supseteq Ra^2 \supseteq Ra^3 \supseteq Ra^4 \supseteq$$

must stabilize (**5**). Therefore $Ra^n = Ra^{n+1}$ for some $n \geq 1$ (**5**). Since $a^n = 1a^n \in Ra^n = Ra^{n+1}$ there is an $r \in D$ such that $1a^n = a^n = ra^{n+1} = raa^n$ (**5**). Now $a^n \neq 0$ since $a \neq 0$. By cancellation $1 = ra$. We have shown that $a \in D^\times$ (**5**). Therefore D is a field.

3. Page 335, number 36: (**20 points**) Set $D = \mathbf{Z}[\sqrt{2}]$. Since $x^2 - 2 \in \mathbf{Q}[x]$ is irreducible by the Eisenstein Criterion, all $a \in D$ have a unique representation $a = m + n\sqrt{2}$, where $m, n \in \mathbf{Z}$. Since $(1+\sqrt{2})(-1+\sqrt{2}) = -1^2 + 2 = 1$ it follows that $1+\sqrt{2}$ has a multiplicative inverse in D which is $-1+\sqrt{2}$ (**7**).

We show that $1+\sqrt{2}$ has infinite order. Suppose that $(1+\sqrt{2})^n = k + \ell\sqrt{2}$, where $k, \ell > 0$. This is the case when $n = 1$. Then

$$(1+\sqrt{2})^{n+1} = (1+\sqrt{2})(1+\sqrt{2})^n = (1+\sqrt{2})(k+\ell\sqrt{2}) = (k+2\ell) + (k+\ell)\sqrt{2}$$

which shows that $(1+\sqrt{2})^{n+1} = k' + \ell'\sqrt{2}$, where $k', \ell' > 0$ (**5**). Thus $(1+\sqrt{2})^n \neq 1 = 1 + 0\sqrt{2}$ for $n > 0$ by uniqueness of expression (**5**) since the coefficient of $\sqrt{2}$ on the left is never 0. Thus $1+\sqrt{2}$ has infinite order (**5**).

4. Page 349, number 22: (**20 points**) Let $\{v_1, \ldots, v_n\}$ be a basis for V. By Exercise 4 every $v \in V$ has a unique expansion $v = a_1v_1 + \cdots + a_nv_n$, where $a_1, \ldots, a_n \in \mathbf{Z}_p$ (**5**). Therefore there is a bijection from V to the set $\{(a_1, \ldots, a_n) \,|\, a_1, \ldots, a_n \in \mathbf{Z}_p\}$ given by

$$a_1v_1 + \cdots a_nv_n \mapsto (a_1, \ldots, a_n). \;\; (\mathbf{5})$$

The latter has

$$\underbrace{p\cdot \;\cdots\; \cdot p}_{n-factors} = p^n \;\; (\mathbf{5})$$

elements. We have shown $|V| = p^n$ (**5**).

5. Page 349, number 24: (**20 points**) We first show that $U \cap W$ is a subspace of V. Since U, W are additive subgroups of V it follows that $U \cap W$ is an additive subgroup of V from group theory (**5**). Let $a \in F$ and $v \in U \cap W$. Then $v \in U, W$. As these are subspaces of V we conclude $rv \in U, W$ (**5**). Therefore $rv \in U \cap W$. We have shown that $U \cap W$ is a subspace of V.

Next we show that $U + W$ is a subspace of V. Since V ia an additive abelian group, all subgroups of V are normal. It follows that $U + W$ is an additive subgroup of V from group theory (**5**). Let $v \in U + W$ and $r \in F$. Then $v = u + w$ for some $u \in U$ and $w \in W$. Since U, W are subspaces of V it follows that $ru \in U$ and $rw \in W$ (**5**). Therefore $r(u+w) = ru + rw \in U + W$. We have shown that $U + W$ is a subspace of V.