# Algebra I, Fall 2016

Solutions to Problem Set 6

1. We know from Problem Set 5, Questions 5(a) that every ideal $J$ of $S^{-1}A$ is of the form $S^{-1}I$ for an ideal $I$ of $A$. Since $A$ is a PID, $I$ is generated by an element $a$, so $J$ is generated by $\frac{a}{1}$.

2. First note that if $a$ is a nonzero element in $A$, then $\frac{a}{1}$ is a unit in $S^{-1}A$ if and only if $(a) \cap S \neq \emptyset$: if $s \in (a)$, then $s = ax$, then $\frac{a}{1}\frac{x}{s} = 1$; and conversely if $\frac{a}{1}\frac{x}{s} = 1$, then $xa \in (a) \cap S$.

We now prove the second statement. If $p$ is a prime in $A$ such that $(p) \cap S = \emptyset$, then $\frac{p}{1}$ is non-unit, and if $\frac{a}{s_1}\frac{b}{s_2} \in (\frac{p}{1})$, then

$$\frac{a}{s_1}\frac{b}{s_2} = \frac{x}{s}\frac{p}{1},$$

so $abs = s_1 s_2 xp$, so $p|abs$, so $p|a$ or $p|b$ or $p|s$. But $p$ cannot divide $s$ since then $(p) \cap S \neq \emptyset$. If $p|a$, then $a = a'p$, so $\frac{p}{1}\frac{a'}{s_1} = \frac{a}{s_1}$, so $\frac{p}{1}$ divides $\frac{a}{s_1}$. Similarly if $p|b$ then $\frac{p}{1}$ divides $\frac{b}{s_2}$. So $\frac{p}{1}$ is a prime element, and the same is true for any associate of $p$ in $S^{-1}A$.

Conversely if $\frac{a}{s}$ is prime, and $a = p_1 \dots p_k$ is the prime factorization of $a$ in $A$, then exactly for one $i$, $(p_i) \cap S \neq \emptyset$ since $\frac{a}{s}$ is prime and therefore irreducible, and

$$\frac{a}{s} = \frac{1}{s}\frac{p_1}{1} \dots \frac{p_r}{1}.$$

($(p_i) \cap S$ cannot be non-empty for all $i$ since in this case $\frac{a}{s}$ would be unit.) Note that what we actually proved here is that if $\frac{a}{s}$ is irreducible in $S^{-1}A$, then $\frac{a}{s} = u\frac{p}{1}$ where $u$ is a unit in $S^{-1}A$ and $p$ is a prime in $A$.

Note that if $\frac{a}{s}$ is irreducible in $S^{-1}A$, then it follows from the above argument that $\frac{a}{s} = u\frac{p}{1}$ where $u$ is a unit in $S^{-1}A$ and $p$ is prime in $A$, so again by the above argument $\frac{p}{1}$ is prime in $S^{-1}A$. so $\frac{a}{s}$ is a prime element.

To show $S^{-1}A$ is a UFD, the uniqueness of factorization follows by the argument in class since we know every irreducible element in $S^{-1}A$ is a prime element. So it is enough to show a factorization to product of irreducible elements exists. If $\frac{a}{s}$ is a non-unit element, and if $a = p_1 \dots p_r$ is a factorization of $a$ as a product of irreducible (and hence prime) elements in $A$, then

$$\frac{a}{s} = \frac{p_1}{s}\frac{p_2}{1}\cdots\frac{p_r}{1}$$

and it follows from the first part of the proof that each $\frac{p_i}{1}$ and $\frac{p_1}{s}$ are prime and therefore irreducible in $S^{-1}A$.

4. Let $N(a+2bi) = a^2 + 4b^2$. We show that every element $z \in \mathbf{Z}[2i]$ with $N(z) = 4$ is irreducible, and therefore 2, $2i$ and $-2i$ are irreducible. Since $N$ is multiplicative (it is just the complex modules), if $N(z) = 4$ and $z = z_1 z_2$, then $N(z_1)N(z_2) = 4$. since $a^2 + 2b^2$ cannot be equal to 2 for integers $a$ and $b$, $N(z_1) = 1$ or $N(z_2) = 1$, so $z_1 = \pm 1$, or $z_2 = \pm 1$, so $z_1$ is a unit, or $z_2$ is a unit.

Next notice that the only units of $\mathbf{Z}[2i]$ are $\pm 1$, and so 2 and $2i$ are not associates, and 2 and $-2i$ are not associates, so $4 = 2 \cdot 2 = (2i) \cdot (-2i)$ gives two different factorization of 4 into product of irreducible elements.

5. We saw in class that to divide $y = a + bi$ by a positive number $n$ we first divide $a$ by $n$, and write $a = nq_1 + r_1$ such that $|r_1| \leq n/2$, and then divide $b$ by $n$ and write $b = nq_2 + r_2$ such that $|r_2| \leq n/2$. Then $a + bi = n(q_1 + iq_2) + (r_1 + ir_2)$ and $N(r_1 + ir_2) < N(n) = n^2$.

We also saw that to divide $y = a + ib$ by $x = c + id$, we set $n = N(c + di) = x\bar{x}$, and divide $y\bar{x}$ by $n$: $y\bar{x} = qn + r$, and then

$$y = qx + (y - qx)$$

so the remainder $r$ is $y - qx$.

So to divide $\alpha = 11 + 3i$ by $\beta = 1 + 8i$, we divide $\alpha\bar{\beta} = (11 + 3i)(1 - 8i) = 35 - 85i$ by $n = (1 + 8i)(1 - 8i) = 65$. Since $35 = 65 \cdot 0 + 35$ and $-85 = 65 \cdot (-1) - 20$, we get $q = 0 - i$, so

$$11 + 3i = (-i)(1 + 8i) + (3 + 4i)$$

Since $\gcd(11 + 3i, 1 + 8i) = \gcd(1 + 8i, 3 + 4i)$, we divide $1 + 8i$ by $3 + 4i$ using the same method: $(1 + 8i)(3 - 4i) = 35 + 20i$, and if we divide $35 + 20i$ by $N(3 + 4i) = 25$, we get

$$35 + 20i = (1 + i)25 + (10 - 5i)$$

so $q = 1 + i$ and so if we divide $1 + 8i$ by $3 + 4i$, we get

$$1 + 8i = (1 + i)(3 + 4i) + (2 + i)$$

And similarly

$$3 + 4i = (2 + i)(2 + i) + 0$$

So

$$\gcd(11 + 3i, 1 + 8i) = \gcd(1 + 8i, 3 + 4i) = \gcd(3 + 4i, 2 + i) = 2 + i.$$

Note that the units of the ring are $1, -1, i, -i$, so $-1 + 2i$, $1 - 2i$, and $-2 - i$ are also possible answers.