Sheet 7 Solutions

Robert Kropholler

December 14, 2017

1. Let R be a principal ideal domain. Let D be a multiplicatively closed subset of a ring R. Show that $D^{-1}R$ is a principal ideal domain.

   Proof. Let I be an ideal of $D^{-1}R$. Consider the ideal $J = I \cap D^{-1}R$, this is a principal ideal and is generated by an element x. Thus every element of J has the form rx for some $r \in R$. Let $\frac{s}{d}$ be an element of the ideal I. Therefore $s = d(\frac{s}{d}) \in J$ and so $s = rx$ for some r and we can see that $\frac{s}{d} = \frac{1}{d} \cdot rx$ hence I is principal and generated by x. □

2. Let R be an integral domain and suppose that every prime ideal is principal.

   (a) Assume the set of ideals of R that are not principal is nonempty and use Zorn's Lemma to show that there is a maximal element.

   Proof. Let N be the set of non-principal ideals. Consider an ascending chain $I_1 \subset I_2 \subset \dots$. We will show that this chain has an upper bound and so N has a maximal element. Let $J = \cup_{i=1}^{\infty} I_i$. We must show that J is not a principal ideal. Assume J is principal and generated by a single element x. There is a k such that $x \in I_k$ and hence $(x) \subset I_k \subset J \subset (x)$ and so we get equalitites. However I_k was assumed to be non principal leading to a contradiction. Thus there is a maximal element of N. □

   (b) Let I be the maximal element from above, note this is not a prime ideal since it is not principal. Let $a, b \in R$ be elements of the ring R such that $ab \in I$ but $a \notin I$ and $b \notin I$. Let $I_a = (I, a)$ be the ideal generated by I and a, let I_b be defined similarly, and define $J = \{r \in R \mid rI_a \subset I\}$. Prove that $I_a = (\alpha)$ and $J = (\beta)$ are principal ideals in R with $I \subsetneq I_b \subset J$ and $I_a J \subset I$.

   Proof. Since I is not principal it cannot be a prime ideal so we have a, b as above. It is clear to see that $I \subset (I, a)$ and this is strict so by maximality of I we must have that (I, a) is principal generated by some element α. Similarly I_b is principal since $I \subsetneq I_b$.

It remains to show that J contains I_b. Let x be an element of I_b. Then x has the form $i + rb$ for some $i \in I$ and $r \in R$. similarly any element of I_a has the form $i' + sa$ for some $i' \in I$ and $s \in R$. Multiplying these together we get $(i + rb)(i' + sa) = ii' + isa + i'rb + rsab$, it is clear that each term of this sum is in I and so the whole sum is. This shows that an element of I_b multiplied by an element of I_a is in I and hence $I_b \subset J$ and J is principal generated by some element β. □

(c) If $x \in I$ show that $x = s\alpha$ for some $s \in J$. Deduce that $I = I_a J$ and that I is principal. Use this contradiction to prove that R is a PID.

Proof. Let x be an element of I then since $I \subset I_a$ we know that $x = s\alpha$ for some $s \in R$. We will show that this element is in J. To show that s is in J we must show that $sy \in I$ for all $y \in I_a$. Since $y \in I_a$ we know that $y = r\alpha$ for some $r \in R$. Thus $sy = rs\alpha = rx \in I$ so the element s is in J. □

3. Read the section in Dummit and Foote on the "Factorisation in the Guassian integers" p.289 – 291

4. Let $R = \mathbb{Z}[i]$ be the Guassian integers.

(a) Show that $R/(1 + i)$ is a field with 2 elements.

Proof. By the section above we know that $1 + i$ is a prime and $\mathbb{Z}[i]$ is a PID so $(1 + i)$ is a maximal ideal so the quotient is a field. Consider the map $\phi\colon \mathbb{Z}[i] \to \mathbb{Z}/2\mathbb{Z}$ given by $\phi(a + bi) = a + b$. This is a surjective homomorphism with kernel $(1 + i)$ thus the quotient above is a field with 2 elements. □

(b) Let q be a prime equivalent to 3 mod 4. Show that $R/(q)$ is a field with q^2 elements.

Proof. Once again we know that this ideal is maximal by the above section. We are left to show that it has q^2 elements. Every element has a representative of the form $a + bi$ where $0 \leqslant a, b < q$. One can also see that two of these representatives give the same coset iff they are equal. Thus the quotient has q^2 elements. □

5. Let R be a unique factorisation domain. The *least common multiple* of a and b, denoted $\operatorname{lcm}(a, b)$ is an element r such that $a|r$ and $b|r$ and if $a|s$ and $b|s$, then $r|s$.

(a) Prove that $\operatorname{lcm}(a, b) = \gcd\{x \mid x = ra, x = sb\}$.

Proof. We will show that l divides d and vice versa, thus they are the same up to a unit. Let $m = \text{lcm}(a, b)$ and $d = \gcd\{x \mid x = ra, x = sb\}$. By definition l is divisible by a and b so is also divisible by d.

Let $x = ra = sb$, then x is divisible by a, b and d by definition. So l divides x however x was arbitrary so l must divide d. □

(b) Show that the ideal $(a) \cap (b)$ is principal and generated by the least common multiple of a and b.

Proof. The ideal $(a) \cap (b)$ is equal to the set $\{x \mid x = ra, x = sb\}$ and so is contained in the $(d) = (l)$. However l is divisible by a and b and hence $l \in (a) \cap (b)$. So we get the other containment. □

(c) Given factorisations of a and b describe the least common multiple of a and b in terms of these factorisations.

Proof. Let $a = p_1^{i_1} \dots p_n^{i_n}$ and $b = p_1^{j_1} \dots p_n^{j_n}$. We can assume the same primes appear in both decompositions by not requiring i_k or j_k to be positive.

We can then easily see that $p_1^{\max(i_1, j_1)} \dots p_n^{\max(i_n, j_n)}$ has the desired properties. □