Math 581 Problem Set 4 Solutions

1. Find the greatest common divisor of $2+3i$ and $6-7i$ in $\mathbb{Z}[i]$. Write the greatest common divisor as a linear combination of $2+3i$ and $6-7i$.

Solution omitted.

An integral domain R is a *Euclidean domain* if there is a function δ from the nonzero elements of R to the nonnegative integers with these properties:
(i) If a and b are nonzero elements of R, then $\delta(a) \leq \delta(ab)$.
(ii) If $a, b \in R$ and $b \neq 0_R$, then there exist $q, r \in R$ such that $a = bq + r$ and either $r = 0_R$ or $\delta(r) < \delta(b)$.

2. Let p be an irreducible element in a Euclidean domain R. Prove that if $p|bc$, then $p|b$ or $p|c$.

Proof: See the proof of Proposition 2.5 in Chapter 1. The exact same argument carries through here. See also Proposition 1.7 in Chapter 3 for the corresponding statement in terms of polynomials.

3. Prove that every Euclidean domain is a PID.

Proof: Let R be an Euclidean domain and I be a non-zero ideal in R. Using the map δ we can find an element a in I with $\delta(a)$ minimal. (The $\delta(a)$ are in $\mathbb{N}$!) Now let b be any element in I. Using the Euclidean algorithm we have that there exists q and r with $b = qa + r$ and $r = 0$ or $\delta(r) < \delta(a)$. If $r = 0$, then $a|b$ and we are done. If $r \neq 0$, then $\delta(r) < \delta(a)$ with $r = b - qa \in I$. However, a was chosen so that $\delta(a)$ is minimal among elements of I. Thus it must be that $r = 0$. Hence, $I = \langle a \rangle$. ■

An ideal $\wp$ in a commutative ring R is said to be *prime* if $\wp \neq R$ and whenever $bc \in \wp$, then $b \in \wp$ or $c \in \wp$. An ideal $\mathfrak{m}$ in a ring R is said to be *maximal* if $\mathfrak{m} \neq R$ and whenever I is an ideal such that $\mathfrak{m} \subset I \subset R$, then $\mathfrak{m} = I$ or $I = R$.

4. Prove that $\mathfrak{m}$ is a maximal ideal if and only if $R/\mathfrak{m}$ is a field.

Proof: We begin by proving the more general result, which you were told you were allowed to quote without proof.

Theorem: The ideals in R that contain I correspond bijectively to the ideals in R/I.

Pf: Let J be an ideal that contains I and consider the onto homomorphism $\phi : R \to R/I$. We saw in a previous homework set that $\phi(J)$ is an ideal in R/I. Alternatively, let M be an ideal in R/I. Note that M contains $0_{R/I}$ necessarily. Consider $\phi^{-1}(M)$. This is an ideal by a previous homework problem. We claim this contains I. Note that $I = \ker \phi$ and so $I = \phi^{-1}(0_{R/I}) \subset \phi^{-1}(M)$. ■

Let $\mathfrak{m}$ be a maximal ideal of R. To see that $R/\mathfrak{m}$ is a field we show that the only ideals in $R/\mathfrak{m}$ are $\langle 0_{R/\mathfrak{m}} \rangle$ and $R/\mathfrak{m}$. Suppose J is an ideal in $R/\mathfrak{m}$ that is not the zero ideal or the entire ring. Then by the result above we see that J gives an ideal in R that contains $\mathfrak{m}$. It is not equal to $\mathfrak{m}$ or J would be the zero ideal and it is not R or J would be $R/\mathfrak{m}$. This contradicts $\mathfrak{m}$ being a maximal ideal.
Let $R/\mathfrak{m}$ be a field. Suppose that $\mathfrak{m} \subsetneq I \subsetneq R$. Then we have that $\phi(I)$ is a non-zero ideal in $R/\mathfrak{m}$ that is not equal to the entire ring, contradicting the fact that $R/\mathfrak{m}$ is a field. ■

5. Prove that every maximal ideal is a prime ideal.

Proof: Let $\mathfrak{m}$ be a maximal ideal in a ring R. Problem 4 shows that $R/\mathfrak{m}$ is a field. Since every field is an integral domain, we see from problem 10 on the midterm that $\mathfrak{m}$ is necessarily a prime ideal. ■

6. List all the maximal ideals in $\mathbb{Z}/10\mathbb{Z}$.

Solution: Note that all the ideals in this ring are principal by previous homework set. We also know that $\langle n \rangle = \mathbb{Z}/10\mathbb{Z}$ for all n so that $\gcd(n, 10) = 1$. This eliminates $n = 1, 5, 7, 9$ from consideration as a maximal ideal. It is only a matter of checking the remaining ideals to see which are distinct. This leaves us with the ideals $\langle 0 \rangle$, $\langle 2 \rangle$, and $\langle 5 \rangle$. The zero ideal is contained in every ideal, so is not a maximal ideal. The other two are properly contained by no other ideal, so they are both maximal.

7. Show that the principal ideal $\langle x - 1 \rangle$ in $\mathbb{Z}[x]$ is a prime ideal but not a maximal ideal.

Proof: Define a map $\phi : \mathbb{Z}[x] \to \mathbb{Z}$ by $\phi(f(x)) = f(1)$. This is a surjective map and is a homomorphism (it is an evaluation map). The kernel of this map is $\langle x-1\rangle$, so $\mathbb{Z}[x]/\langle x-1\rangle \cong \mathbb{Z}$. Since $\mathbb{Z}$ is an integral domain, $\langle x-1\rangle$ is a prime ideal by problem 10 on the midterm. It is not a maximal ideal because $\mathbb{Z}$ is not a field, so $\langle x-1\rangle$ cannot be a maximal ideal (see problem 4). ■

8. Let $\phi : R \to S$ be a surjective homomorphism of commutative rings. If $\wp$ is a prime ideal in S, prove that $\phi^{-1}(\wp)$ is a prime ideal in R. (Note this property is NOT true for maximal ideals!)

Proof: Note that $\phi^{-1}(\wp)$ is an ideal by previous homework. To see it is prime, we must show if $ab \in \phi^{-1}(\wp)$, then a or b is in $\phi^{-1}(\wp)$. Let $ab \in \phi^{-1}(\wp)$, i.e., $\phi(ab) \in \wp$. Using that ϕ is a homomorphism we have that $\phi(a)\phi(b) \in \wp$. Now we use that $\wp$ is a prime ideal to conclude that $\phi(a)$ or $\phi(b)$ is in $\wp$. Thus, a or b is in $\phi^{-1}(\wp)$.
A more sophisticated proof is as follows. Since $0_S \in \wp$ necessarily, it follows from the definition that $\ker\phi \subset \phi^{-1}(I)$. Thus, one has that by considering the map induced from ϕ given by $R \to S \to S/\wp$ that $R/\phi^{-1}(\wp)$ is isomorphic to its image inside $S/\wp$. Thus, $R/\phi^{-1}(\wp)$ is isomorphic to a subring of an integral domain, thus must be an integral domain itself. Thus, $\phi^{-1}(\wp)$ is a prime ideal. ■

9. Suppose that $I \subsetneq R$ is an ideal with the property that every element $a \notin I$ is a unit. Prove that I is a maximal ideal.

Proof: Suppose J is an ideal such that $I \subsetneq J \subseteq R$. To see that I is a maximal ideal, we need to show that $J = R$. Since $I \subsetneq J$ there is at least one element a in J that is not in I. However, by assumption we know that since $a \notin I$, a must be a unit. Since J contains a unit, we know $J = R$ by previous homework. Thus I is a maximal ideal. ■

10. Prove that the maximal ideals of $\mathbb{C}[x]$ are in a one-to-one correspondence with points of $\mathbb{C}$, i.e., there is a bijection between the set of maximal ideals in $\mathbb{C}[x]$ and $\mathbb{C}$.

Proof: Let $a \in \mathbb{C}$ and consider the ideal $\langle x-a\rangle \subset \mathbb{C}[x]$. One has that $\mathbb{C}[x]/\langle x-a\rangle \cong \mathbb{C}$, thus $\langle x-a\rangle$ is a maximal ideal by problem 4. Thus, we get a map from $\mathbb{C}$ to the set of maximal ideals of $\mathbb{C}[x]$ by sending a to $\langle x-a\rangle$. It is clear that this map is an injective map, i.e., if $\langle x-a\rangle = \langle x-b\rangle$ then $a = b$. (Otherwise we would have $x-a$ and $x-b$ both in an ideal, but for $a \neq b$ these are relatively prime, and hence the ideal would contain

1 and be the entire ring.) To see this map is surjective, let $\mathfrak{m}$ be a maximal ideal in $\mathbb{C}[x]$. We know that $\mathbb{C}[x]$ is a PID (we saw this with $F[x]$, so just apply that result with $F = \mathbb{C}$.) Let $\mathfrak{m} = \langle f(x) \rangle$. Consider the quotient ring $\mathbb{C}[x]/\langle f(x) \rangle$. If $\deg f(x) \geq 2$, then $f(x)$ factors into linear polynomials over $\mathbb{C}$ and hence is reducible in $\mathbb{C}[x]$. Thus, $\mathbb{C}[x]/\langle f(x) \rangle$ is a field if and only if $\deg f(x) = 1$. Thus maximal ideals are generated by linear polynomials, i.e., they are determined by a complex number, the root of the linear polynomial. ■