Solution Set 11

Daniel Gardiner

January 3, 2006

Math 122

1 (a) **Claim:** $\mathbb{R}[X,Y]$ is not a Euclidean domain.
Proof: If $\mathbb{R}[X,Y]$ was a Euclidean domain, then it would be a principal ideal domain. But consider $I = (x,y) = (x) + (y)$. I is certainly not a principal ideal, as if it were, there would be some polynomial, g that divides everything in I, so g would divide x, implying that g does not contain any monomials with positive degree in y, and likewise g would divide y, implying that g does not contain any monomials with positive degree in x, so g is a constant polynomial, contradicting the fact that I is clearly not the unit ideal.

Claim: $\mathbb{Z}[X]$ is not a Principal Ideal Domain.
Proof; Consider $I = (2,x) = (2) + (x)$. A similar argument as above shows that I is not principal, as if I were generated by some polynomial, g, then g would have to divide 2, so g would have to either be a unit, which is impossible since I is not the unit ideal, or g would have to be a unit times 2, which again generates a different ideal since x is not in (2). Hence, $\mathbb{Z}[X]$ is not a Principal Ideal Domain.

2 **Claim:** 30 factors as $3(1+i)(1-i)(2+i)(2-i)$ in $\mathbb{Z}[i]$.
Proof: Certainly, $30 = 3(1+i)(1-i)(2+i)(2-i)$. We need to verify that each of these factors are actually prime. Since $\mathbb{Z}[i]$ is a principal ideal domain, an element is prime if and only if it is irreducible, so it suffices to check that each factor is irreducible. For this, we define the norm function $||*|| : \mathbb{Z}[i] \longrightarrow \mathbb{N}$ given by $||a+bi|| = a^2 + b^2$. It is easily verified that $||*||$ is a multiplicative function, namely that $||m*n|| = ||m||||n||$. Moreover, if for some $r \in \mathbb{Z}[i]$, $||r|| = 1$, then, if $r = a + bi$, $a^2 + b^2 = 1$ implies that either $a = 1$ and $b = 0$ or $a = 0$ and $b = 1$, implying that r is either $1, -1, i$, or $-i$, and thus is a unit.

Hence, since if r reduces in $\mathbb{Z}[i]$, $r = mn$ with m and n non-unit elements of $\mathbb{Z}[i]$, $||m||||n|| = ||r||$, with $||m||$ and $||n||$ strictly less than $||r||$, As a first consequence, note that this shows that if $||r||$ is irreducible, r must be irreducible as well. Thus, we

immediately have that $(1+i), (1-i), (2+i)$, and $(2-i)$ are irreducible in $\mathbb{Z}[i]$ since their norms are prime. To see that 3 is irreducible, note that $||3|| = 9$, so if $3 = a * b$ for non-unit $a, b \in \mathbb{Z}[i]$, we would have $||a|| = ||b|| = 3$, but there are no elements in $\mathbb{Z}[i]$ with norm 3.

3 Let $R = \mathbb{Z}[\sqrt{-5}]$

(a) **Claim:** $R^x = \{\pm 1\}$ (recall that R^x is the unit group of R.)

Proof: Exactly as above, we define a norm function $|| * || : R \longrightarrow \mathbb{N}$, where $||a + b\sqrt{-5}|| = a^2 + 5b^2$. A simple calculation verifies that $|| * ||$ is a multiplicative function, namely that $||m * n|| = ||m||||n||$; alternatively, note that our function just takes any r to ths square of its complex norm, and since squaring is certainly a multiplicative function, the composition of these two operations is multiplicative as well. With this in mind, assume that $r \in R^x$. Then $\exists\ a \in R^x$ s.t. $ra = 1$. Applying the norm, we have that $||r||||a|| = 1$, implying that $||r|| = 1$, so if $r = x + y\sqrt{-5}$, we must have $x = \pm 1, y = 0 \Rightarrow r \in \{\pm 1\}$.

(b) **Claim:** Every element of R can be written as a product of irreducble elements of R.

Proof: We again apply the norm function from above. We know that if $||r|| = 1$, $r \in \{\pm 1\}$ from above, so in particular r is a unit. Hence, take some element $y \in R$. Then if y is irreducible, we are done; if not, we can write $y = a * b$, with a, b non-unit elements of $R \Rightarrow ||a|| > 1$ and $||b|| > 1$. Hence $||a|| < ||y||$ and $||b|| < ||y||$. If a and b are irreducible, then we are done. If not, we can repeat this process. We know that since the norm of our factors are getting progressively smaller, and anything with norm 1 is a unit, this process must terminate in a finite number of steps. Hence, we can write y as a product of irreducible elements of R.

(c) **Claim:** $2, 3, 1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are irreducible elements of R.

Proof: We again apply our norm. Note that $||2|| = 4$, so if 2 factored into a product of non-unit elements of R, each factor would have norm 2, but since there are no elements of norm 2 in R, 2 must be irreducible. Similarly, there are no elements of norm 3 in R, so 3 must be irreducible as well. Now $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ both have norm 6, so again since there are no elements of norm 3 or 2 in R, we have that $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are irreducible as well.

(d) **Claim:** R is not a unique factorization domain (i.e. R does not have unique factorization into irreducibles.)

Proof; Note that $6 = 2 * 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}$, and we just showed that each of these factors are irreducible. Since $R^x = \{\pm 1\}$, it is clear that none of these factors are associates (i.e., differ by only a unit). Hence, since 6 has two distinct factorizations, R is not a unique factorization domain.

4 **Claim:** (p) is a nonzero prime ideal in a ring R if and only if p is a prime element.

Proof: Assume that p is a prime element. Then $p \neq 0$, so clearly (p) is not the zero ideal. Moreover, if $ab \in (p)$, then p divides ab, so, since p is prime, p divides a or p

divides b. Hence, a or b is in (p), so (p) is prime.
Conversely, assume that (p) is a non-zero prime ideal. Then certinaly $p \neq 0$. Moreover, if p divides ab, $ab \in (p)$, so, since (p) is prime, $(a) \in (p)$ or $(b) \in (p) \Rightarrow p$ divides a or p divides b.

5 **Claim:** Two polynomials in $\mathbb{Z}[X]$ are relatively prime in $\mathbb{Q}[X]$ if and only if the ideal they generate in $\mathbb{Z}[X]$ contains a nonzero integer.
Proof: Let $f, g \in \mathbb{Z}[X]$, and assume that (f, g) in $\mathbb{Z}[X]$ contains a nonzero integer, c. Then $rf + sg = c$ for polynomials $r, s \in \mathbb{Z}[X]$, so, defining $r' = r/c, s' = s/c$, we have $r'f + s'g = 1$ for $r', s' \in \mathbb{Q}[X]$, so $1 \in (f, g)$ in $\mathbb{Q}[X]$, implying that $(f, g) = (f) + (g) = (1)$, implying that f, g are relatively prime (the proof of this last statement is in Artin and is a good condition for proving that polynomials are relatively prime, which is why I used it here - of course there are plenty of other ways to do this that don't use that last fact, but it's good to know in my opinion.)
Conversely, if f, g are relatively prime in $\mathbb{Q}[X]$, then by the above fact, $(f, g) = (f) + (g) = (1)$, so there exist polynomials $r, s \in \mathbb{Q}[X]$ s.t. $rf + sg = 1$. Multiplying through by the greatest common denominator of all the coefficients of r and s, which will be denoted d, we have $(dr)f + (ds)g = d$, where $dr, ds \in \mathbb{Z}[X]$, so $(f, g) \in \mathbb{Z}[X]$ contains the nonzero integer d.

6 (a) **Claim:** $f(x) = x^2 + 27x + 213$ is irreducible in $\mathbb{Q}[X]$.
Proof: We apply Eisenstein's Criterion for $p = 3$. Then p does not divide the first coefficient, p divides all of the other coefficients, and p^2 does not divide the last coefficient, so we have that $f(x)$ is irreducible in $\mathbb{Z}[X]$ and hence in $\mathbb{Q}[X]$ as well (by an application of Gauss' Lemma proven in class and in Artin.)
(b) **Claim:** $f(x) = x^3 + 6x + 12$ is irreducible in $\mathbb{Q}[X]$.
Proof: We again apply Eisenstein's Creiterion for $p = 3$. p does not divide the first coefficient, p divides all the other ones (note that p tautologically divides 0, the coefficient of the x^2 term), and p^2 does not divide the last coefficient, so $f(x)$ is irreducible in $\mathbb{Z}[X]$ and hence in $\mathbb{Q}[X]$ as well by the above fact.
(c) **Claim:** $f(x) = 8x^3 - 6x + 1$ is irreducible in $\mathbb{Q}[X]$.
Proof: We reduce modulo 5 to get $g(x) = 3x^3 - x + 1 \in \mathbb{Z}/5\mathbb{Z}[X]$. Now since g is a cubic polynomial, it reduces in $\mathbb{Z}/5\mathbb{Z}[X]$ if and only if it has a root. But $\mathbb{Z}/5\mathbb{Z}$ is a finite field, so we just check the 5 possibilities for roots: $g(0) = 1, g(1) = 3, g(2) = 3, g(3) = 4$, and $g(4) = 4$, so $3x^3 - x + 1$ is irreducible. Since f is irreducible in $\mathbb{Z}/p\mathbb{Z}[X]$ for $p = 5$, and a polynomial is irreducible in $\mathbb{Z}[X]$ if it is irreducible in $\mathbb{Z}/p\mathbb{Z}[X]$ for some prime p, we get that f is irreducible in $\mathbb{Z}[X]$ and hence in $\mathbb{Q}[X]$ as well.
Note: Many people tried to apply Eisenstein's Criterion here for $p = 2$, but since 2 divides 8, the first coefficient, this does not work.

7 **Claim:** Let $f(x) = x^n + c_{n-1}x^{n-1} + ... + c_1x + c_0$, and let r be a root of f. Then r is an integer.
Proof: Let $r = a/b \in \mathbb{Q}$, where a and b are relatively prime. Then f factors as $(x-r)q(x)$ in $\mathbb{Q}[X]$, where $q(x)$ is a monic polynomial. Now $(x-r) = (1/b)(bx-a)$, and $bx-a$ is a primitive polynomial with integer coefficients since by assumption, $gcd(a,b) = 1$. Hence, the unique content of $(x-r)$ must be $1/b$. Now, $q(x)$ must have some content c as well, so we can write $q(x) = c * q_0(x)$ for some primitive $q_0 \in \mathbb{Z}[X]$. Hence, we have $f = (c/b)(bx-a)q_0$; but f was a monic integer polynomial, so its unique content must be 1. Hence, c/b=1 since again content is unique, so we have $f = (bx-a)q_0$ where $q_0 \in \mathbb{Z}[X]$. But f is monic by assumption, and q_0 is an integer polynomial, so b is a unit in the integers, implying that b is 1 or -1, so r is an integer as desired.

8 (a) **Claims:** Let $\varphi : V \longrightarrow W$ be a homomorphism of modules over a ring R, and let V', W' be submodules of V, W respectively. Then:
1: $\varphi(V')$ is a submodule.
Proof: We need to verify the module axioms; note that it suffices to check closure under addition, additive inversion, and multiplication by an arbitrary element of R, since clearly $0 \in \varphi(V')$ and $\varphi(V')$ inherits associativity of multiplication and all of the other properties from W. Now, if $\varphi(a), \varphi(b) \in \varphi(V')$, then $\varphi(a) + \varphi(b) = \varphi(a+b)$, and $a + b \in V'$, so $\varphi(a) + \varphi(b) \in \varphi(V')$. Likewise, if $\varphi(a) \in \varphi(V')$, then, since φ is also a homomorphism of additive groups, $\varphi(-a) = -\varphi(a)$, so $\varphi(V')$ is closed under inversion. Now take $r \in R, \varphi(a) \in \varphi(V')$. Then similarly, $r\varphi(a) = \varphi(ra)$, and $ra \in V$, so $r\varphi(a) \in V'$. Note that we have repeatedly used the fact that V' is a submodule.

2: $\varphi^{-1}(W')$ is a submodule.
Proof: Again we need to verify the module axioms, and again it suffices to consider the axioms targeted above. If $a, b \in \varphi^{-1}(W')$ then $\varphi(a+b) = \varphi(a) + \varphi(b)$, and $\varphi(a), \varphi(b) \in W' \Rightarrow \varphi(a) + \varphi(b) \in W'$. Hence, $\varphi^{-1}(W')$ is closed under addition. Likewise, if $a \in \varphi^{-1}(W')$, then $\varphi(-a) = -\varphi(a) \in W'$, so $\varphi^{-1}(W')$ is closed under inversion. Note also that clearly $\varphi^{-1}(W')$ contains 0. Finally, for $r \in R, a \in \varphi^{-1}(W')$, $\varphi(ra) = r\varphi(a) \in W'$ since W' is a submodule $\Rightarrow \varphi^{-1}(W')$ is closed under multiplication by arbitrary elements of R. Note that we have repeatedly used the fact that W' is a submodule.

Corollary: $Ker(\varphi)$ and $Im(\varphi)$ are submodules of V and W respectively.
Proof: This is just the fact that $Im(\varphi) = \varphi(V)$ and $Ker(\varphi) = \varphi^{-1}(0)$, and clearly V and 0 are submodules of V and W respectively.

(b) **Claim:** Let $\varphi : V \longrightarrow W$ be a homomorphism of simple modules. Then either φ is the zero map, or it is an isomorphism.

Proof: We apply the above corollary. Since $Im(\varphi)$ is a submodule of W and W is simple, either $Im(\varphi) = \{0\}$, in which case φ is just the zero homomorphism, or $Im(\varphi) = W$. But $Ker(\varphi)$ is a submodule of V, and V is simple as well, and in this second case, clearly $Ker(\varphi) \neq V$ since $W \neq \{0\}$, so $Ker(\varphi) = \{0\} \Rightarrow \varphi$ is a bijection and hence an isomorphism.

(c) **Claim:** Let V be a simple module over a ring R. Then V is isomorphic to R/M where M is a maximal ideal.
Proof:. Since V is simple, it is not the zero module, so take some non-zero $v \in V$. Then we have a module homomorphism $\varphi : R \longrightarrow V$, where $\varphi(r) = rv$. That φ is a homomorphism follows by definition from the module axioms. Now $Im(\varphi)$ is a submodule of V from our corollary, and $Im(\varphi)$ is non-zero since v is non-zero and $1 \in R$. Hence, $Im(\varphi) = V$, so our map is onto. Now φ has some kernel, which is a submodule of R and therefore an ideal, so applying the 1st Isomorphism Theorem for Modules (which I'm not sure if we've proved yet, but should be in Artin, and the proof is identical to the one for vector spaces), we get an isomorphism $\beta : R/M \longrightarrow V$. Now, viewing R/M as a ring, which we can do since M, as a submodule of R is just an ideal, we get that M must be maximal, as if M were not maximal, R/M would not be a field, so R/M would have some proper, non-trivial ideal I, which is a submodule over R as certainly I is closed under addition, inversion, etc., and, for general $r \in R, r' + M \in I$, $r(r' + M) = rr' + M = (r + M)(r' + M) \in I$ since I is an ideal (note that we have used the definition of multiplication over R in a quotient module, which again should be in Artin, and again is exactly the same as for vector spaces). Then $\varphi(I)$ is a submodule of V, and φ is a bijection, so $\varphi(I)$ is not the zero submodule and $\varphi(I)$ is also not all of V, contradicting the fact that V is a simple module. This establishes the result.

9 (a) **Claim:** Not every set of generators contains a basis.
Proof: By counter-example. Let $V = R = \mathbb{Z}$ and consider $\{2, 3\}$. Then $3 - 2 = 1$, so certainly $\{2, 3\}$ generates V, but clearly neither 2 nor 3 generate V over R, so $\{2, 3\}$ does not contain a basis.
(b) **Claim:** Not every linearly independent set can be extend to a basis,
Proof: Again, let $V = R = \mathbb{Z}$, and consider $\{2\}$. Certainly, $\{2\}$ is linearly independent, but if we add any other integer, b to $\{2\}$, we would pick up the non-trivial linear relation $(2)b + (-b)2 = 0$, contradicting linear independence.
Note: If, like me, you were a bit confused about whether that linear relation actually "counts" since it seems rather trivial, perhaps a good way to convince yourself is to consider the induced map from $\mathbb{Z}^2 \longrightarrow \mathbb{Z}$ taking (x, y) to $bx + 2y$. Then $(2, -b)$ is a non-trivial element in the kernel of this map, and if our set $\{2, b\}$ was really linearly independent, that induced map should be an injection.