Chapter 6

Dave

February 21, 2015

1 A Recollection of Rings

1. If e and e' are both identity elements in a ring R then $e = e'e = e'$. And if $rr' = e = r''r$ for some $r \in R$, then multiplying the equality $rr' = e$ on the left by r'' gives $r''rr' = r' \to r'' = r'$.

2. The additive inverse of $\sum_I a_I x^I$ is $\sum_I -a_I x^I \in R[x_1, \dots x_n]$ since R is a ring. Similarly, the sum and product of elements of $R[x_1, \dots x_n]$ are in $R[x_1, \dots x_n]$. For distributivity of multiplication over addition, $\sum_I a_I x^I (\sum_I b_I x^I + \sum_I c_I x^I) = \sum_I a_I x^I (\sum_J (b_J + c_J) x^J) = \sum_I \sum_J a_I (b_J + c_J) x^{I+J} = \sum_I \sum_J a_I b_J x^{I+J} + \sum_I \sum_J a_I c_J x^{I+J} = \sum_I a_I x^I \sum_I b_I x^I + \sum_I a_I x^I \sum_I c_I x^I$. Finally, for associativity of multiplication, $\sum_I a_I x^I (\sum_I b_I x^I \sum_I c_I x^I) = \sum_I a_I x^I (\sum_I \sum_J b_I c_J x^{I+J}) = \sum_I \sum_J \sum_K a_I b_J c_K x^{I+J+K} = (\sum_I \sum_J a_I b_J x^{I+J}) \sum_I c_I x^I = (\sum_I a_I x^I \sum_I b_I x^I) \sum_I c_I x^I$. Finally, the multiplicative identity in $R[x_1, \dots x_n]$ is the same as that in R.

3. Let R be the group of infinite matrices with finitely many nonzero elements. If $A, B \in R$, then $A + B$ has at most as many nonzero elements as the total such elements in A and B, which is finite. The additive inverse of A is $-A$, which has as many nonzero entries as A since $-x = 0 \leftrightarrow x = 0$ for $x \in \mathbb{R}$. $(AB)_{ij} = \sum_k A_{ik} B_{kj}$, which if only finitely many A_{ik} and B_{kj} are nonzero then only finitely many sums of their products are nonzero. Since R is a subset of the ring of real-valued infinite matrices, this suffices to prove it a subring.

4. If A and B are upper triangular, then $(A + B)_{ij} = A_{ij} + B_{ij} = 0 + 0 = 0$ if $i > j$, so the sum of upper triangular matrices is upper triangular. And $(AB)_{ij} = \sum_k A_{ik} B_{kj}$, so if $i < j$ then $A_{ik} = 0$ for $k = 1 \dots j - 1$ and $B_{kj} = 0$ for $k = j + 1 \dots n$ and each product $A_{ik} B_{kj}$ has at least one of these zeros so the product of upper triangular matrices is upper triangular. The additive inverse of an upper triangular matrix is upper triangular since -0 = 0, so the upper triangular matrices are a subring of the real matrices. The identity matrix is upper triangular.

For the upper triangular matrices with zeros on the diagonal, the arguments of the above paragraph go through unchanged except with $i < j$ changed to $i \leq j$, and of course the identity does not have zeros on its main diagonal.

5. A linear combination of integers is an integer, so the set of integer-valued matrices is closed under sum and product. The same statement applies to natural numbers. The integer matrices are a subring while the natural matrices are not, because $-z \in \mathbb{Z}$ for all $z \in \mathbb{Z}$, whereas $-n \notin \mathbb{N}$ for any $n \in \mathbb{N}$, so the integer matrices are closed under additive inverse while the naturals are not.

6. Let R be the set of symmetric polynomials, and let $a, b \in R$. Then $a(x,y,z) = a(\pi(x,y,z)), b(x,y,z) = b(\pi(x,y,z))$ for all $\pi \in S_3 \leftrightarrow (a+b)(x,y,z) = a(x,y,z) + b(x,y,z) = a(\pi(x,y,z)) + b(\pi(x,y,z)) = (a+b)(\pi(x,y,z))$, so R is closed under sums. A similar proof holds for products, and having established products we get additive inverses for free, since the additive inverse of a is $-1 * a$, and -1 is a symmetric polynomial. This suffices to demonstrate that R is a subring of the three-variabled polynomials.

7. I like chikin.

8. Compositions, sums, and inverses of linear maps are linear, so the linear maps on V are a subring of the functions on V.

9. Let $e \in R$ be an identity, and let $r \in R$ with $f(r) = s$ where f is our isomorphism and $s \in S$. Then $s = f(r) = f(er) = f(e)f(r) \to f(e)$ is the identity in S. Since f^{-1} is also a ring isomorphism, this proof is bidirectional. Similarly, $rr' = r'r \leftrightarrow f(rr') = f(r'r) \leftrightarrow f(r)f(r') = f(r')f(r)$, and since f is a bijection, it is surjective so we can find $r, r' \in R$ such that $f(r) = s, f(r') = s'$ for any $s, s' \in S$.

10. Let $\{A_\alpha\}$ be a collection of subrings of R. Then $x, y \in \cap_\alpha A_\alpha \to x, y \in A_\alpha \forall \alpha \to x + y, xy, -x \in A_\alpha \forall \alpha$ since each A_α is a subring, so $xy, x+y, -x \in \cap_\alpha A_\alpha \to \cap_\alpha A_\alpha$ is a subring.

    Let Q be the smallest subring that contains S, then $R' \cap Q = Q$ for each R' since otherwise the intersection would be a smaller subring containing S since both Q and R' contain S, so since Q is one of the R', the intersection of all of them is equal to Q.

11. $p/q + p'/q' = (pq' + p'q)/qq' \in R(x), (p/q)(p'/q') = pp'/qq' \in R(x), -(p/q) = -p/q \in R(x)$, so $R(x)$ is a ring. The multiplicative inverse of p/q is $q/p \in R(x)$, so $\mathbb{R}(x)$ is a field.

12. Defining addition and multiplication pointwise, the closure of the set of functions from X to R under sum, product and additive inverse follows from those properties

of R. $rr' = r'r$ for all $r, r' \in R \to f(x)g(x) = g(x)f(x) \forall x \in X \forall f, g : X \to R$ since $f(x), g(x) \in R$. The reverse implication follows from the fact that R is isomorphic to the constant-valued functions on X, which is trivial since we defined our operations on functions pointwise and the constant functions take only a single value. If R has an identity, then the constant function on X whose value is that identity is the identity in the function ring, and the units in the function ring are the functions whose range is comprised of units.

13. Let $T, T' \in S'$, then $STT' = TT'S, S(T+T') = ST + ST' = TS + T'S = (T+T')S$, and $S(-T) = -ST = -TS = (-T)S$, so S' is closed under sums, products and additive inverses, so it is a subring of $\mathrm{End}_K(V)$.

14. Let X be our set of linear combinations. Then $\sum n_{1g}g + \sum n_{2g}g = \sum (n_{1g} + n_{2g})g \in X, -\sum n_g g = \sum n_{-g} g \in X$, and $(\sum n_{1g}g)(\sum n_{2g}g) = \sum_g \sum_h n_{1g}n_{2h}gh \in X$, so X is a subring of $GL(V)$.

15. $\mathbb{Z}G$ is an abelian additive group as long as G is, since the inverse of $\sum_{g\in G} a_g g$ is $\sum_{g\in G} -a_g g \in \mathbb{Z}G$ and the other group properties are even more self-evident. Additionally, multiplication is associative, since $\sum a_g g(\sum b_h h * \sum c_i i) = \sum_g a_g g(\sum_h \sum_i b_h c_i hi) = \sum_g \sum_h \sum_i a_g b_h c_i ghi = (\sum_g \sum_h a_g b_h gh) \sum_i c_i i = (\sum a_g g * \sum b_h h) \sum c_i i$, and multiplication is distributive over addition, since $\sum a_g g(\sum b_h h + \sum c_i i) = \sum_g a_g g(\sum_h (b_h + c_h)h) = \sum_g \sum_h a_g(b_h + c_h)gh = \sum_g \sum_h a_g b_h gh + a_g c_h gh = \sum a_g g \sum b_h h + \sum a_g g \sum c_i i$.

16. Let f be our isomorphism, then $f(a+bi+c+di) = (a+b+c+d, a+c-b-d) = (a+b, a-b) + (c+d, c-d) = f(a+bi) + f(c+di)$, and $f((a+bi)(c+di)) = f(ac+bd+adi+bci) = (ac+bd+ad+bc, ac+bd-ad-bc) = (a+b, a-b)(c+d, c-d) = f(a+bi)f(c+di)$ where $i = \xi$. So f respects ring operations, and it's a bijection since its inverse is $f^{-1}(x, y) = ((x+y)/2, (x-y)/2)$, so it's a ring isomorphism.

17. The proofs are the same as those for $R[x]$, just with infinities as the upper limit of the sums.

18. $0(00) = 0 = (00)0$, $0 + 0 = 0$, $0(0 + 0) = 0 = 00 + 00$, etc. so the zero ring is a ring. If 1=0, then for all $x \in S, x = x1 = x0 = 0$, so $S = \{0\}$.

2 Homomorphisms and Ideals

1. Let $f(A) = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$, then $f(AB) = \begin{pmatrix} AB & 0 \\ 0 & AB \end{pmatrix} = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}\begin{pmatrix} B & 0 \\ 0 & B \end{pmatrix} = f(A)f(B)$, and $f(A+B) = \begin{pmatrix} A+B & 0 \\ 0 & A+B \end{pmatrix} = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix} + \begin{pmatrix} B & 0 \\ 0 & B \end{pmatrix} = f(A) +$

$f(B)$. So f is a homomorphism, and $f(I_2) = I_4$, so it's unital. Let $g(A) = \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}$, then similar computations give that g is a homomorphism.

2. $\phi(a+bx+cx^2)(d+ex+fx^2) = \phi(ad+aex+afx^2+bdx+bex^2+cdx^2) = \begin{pmatrix} ad & ae+bd & af+be+cd \\ 0 & ad & ae+bd \\ 0 & 0 & ad \end{pmatrix} = \begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix} \begin{pmatrix} d & e & f \\ 0 & d & e \\ 0 & 0 & d \end{pmatrix} = \phi(a+bx+cx^2)\phi(d+ex+fx^2)$, and $\phi(a+bx+cx^2+d+ex+fx^2) = \begin{pmatrix} a+d & b+e & c+f \\ 0 & a+d & b+e \\ 0 & 0 & a+d \end{pmatrix} = \begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix} + \begin{pmatrix} d & e & f \\ 0 & d & e \\ 0 & 0 & d \end{pmatrix} = \phi(a+bx+cx^2) + \phi(d+ex+fx^2)$, so ϕ respects ring operations, so it is a homomorphism, and $\phi(1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, so ϕ is unital. Its colonel is the polynomials of degree > 3, since those have zeros for the coefficients a_0, a_1 and a_2.

3. $f(1)^2 = f(1^2) = f(1)$, and $f(x) = f(1x) = f(x1) = f(1x1) \to ef(x) = f(x)e = ef(x)e$.

4. If $x = f(a), y = f(b) \in S$, then $x + y = f(a) + f(b) = f(a+b) \in f(R), xy = f(a)f(b) = f(ab) \in f(R)$, and $-x = -f(a) = f(-a) \in f(R)$, so $f(R)$ is a subring of S.

5. $f(g(xy)) = f(g(x)g(y)) = f(g(x))f(g(y))$ and $f(g(x+y)) = f(g(x) + g(y)) = f(g(x)) + f(g(y))$, so $f \circ g$ is a ring homomorphism.

6. For $f \in I$, $f(x) = 0$ for $x \in S$, so for $g \in R$, $f(x)g(x) = 0g(x) = 0$, so I is an ideal.

7. $\begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} d & e & f \\ 0 & g & h \\ 0 & 0 & i \end{pmatrix} = \begin{pmatrix} 0 & ag & ah+bi \\ 0 & 0 & ci \\ 0 & 0 & 0 \end{pmatrix} \in I$, so I is an ideal.

8. This follows from Proposition 6.2.25, setting $\mathcal{S} = \{x\}$.

9. This follows from Proposition 6.2.27, setting $\mathcal{S} = \{x\}$.

10. Let I be a nonzero ideal in a field F, and $x \neq 0 \in I$, then for all $y \in F$, $xx^{-1}y = y \in I$ by the definition of an ideal, so $I = F$, so F is a simple ring.

11. The given "hint" is the entire proof.

12. The functions whose range is contained in $\{0,1\}$ are the idempotents in a ring of functions. The only continuous such functions are the constant 0 and 1 functions.

13. $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$.

14. $re + r'(1-e) = 0$ for some $r, r' \in R \to re + r' - r'e = 0 \to e(re + r' - r'e) = 0 \to re^2 + r'e - r'e^2 = 0 \to re + r'e - r'e = 0 \to re = 0 \to r = 0 \to r' = 0$, so by 6.2.30d, $R \cong Re \oplus R(1-e)$.

15. 15 is a nontrivial idempotent, and $\mathbb{Z}_{35} \cong 15\mathbb{Z}_{35} \oplus 21\mathbb{Z}_{35} \cong \mathbb{Z}_7 \oplus \mathbb{Z}_5$.

16. The colonel of a homomorphism f is an ideal so in a simple ring R it must be either all of R in which case $f = 0$, or $\{0\}$ in which case f is injective.

17. Let A_α be a family of ideals in R. Then $x \in \cap A_\alpha \to x \in A_\alpha$ for each $A_\alpha \to rxr' \in A_\alpha \forall r, r' \in R \forall \alpha$ since each A_α is an ideal, so $rxr' \in \cap A_\alpha \to \cap A_\alpha$ is an ideal. The other statement is trivial.

18. For $r, r' \in R, a+b \in I+J, r(a+b)r' = rar' + rbr'$. Since I is an ideal, $rar' \in I$, and similarly $rbr' \in J$, so $rar' + rbr' \in I+J$, so $I+J$ is an ideal.

19. For $r, r' \in R, a_i \in I, b_i \in J, r(\sum_i a_i b_i)r' = \sum_i ra_i b_i r' = \sum_i (ra_i)(b_i r') \in IJ$ since $ra_i \in I$ and $b_i r' \in J$ since I and J are ideals, so IJ is an ideal. Also, since $a_i \in I, b_i \in R$, $a_i b_i \in I$, and since $b_i \in J, a_i \in R, a_i b_i \in J$, so each $a_i b_i \in I \cap J$, so $IJ \subset I \cap J$.

20. Any ideal that contains a must at least contain all powers of a and all products ra, ar, rar' for $r, r' \in R$, by the definition of ideal, so if this set is an ideal then it is the smallest ideal containing a. In fact, $r(a^n + r'a + ar'' + r'''ar'''')r''''' = ra^n r''''' + rr'ar''''' + rar''r''''' + rr'''ar''''r''''' \in \mathbb{Z}a + Ra + aR + RaR$, so $\mathbb{Z}a + Ra + aR + RaR$ is the ideal generated by a. If R is commutative, then the last three items in this sum are the same, so $\mathbb{Z}a + Ra + aR + RaR = \mathbb{Z}a + Ra$.

21. For $r, r', r'', r''' \in R, m \in M, r(m + r'ar'')r''' = rmr''' + rr'ar''r''' \in M + RaR$ since M is an ideal, so $M + RaR$ is an ideal. Since any ideal containing A must contain RaR, $M + RaR$ is the smallest ideal that contains M and a. If R does not have an identity, then the ideal generated by M and a is $M + \mathbb{Z}aRa + aR + RaR$, since if $1 \notin R$ then any of RaR, Ra, aR and $\mathbb{Z}a$ might contain elements not present in any other of them, whereas if R has an identity then all of them are contained in RaR. All four of RaR, Ra, aR and $\mathbb{Z}a$ must be present in order for a set containing a to be an ideal.

22. (a) $(n,r)((m,s)(l,p)) = (n,r)(ml, mp + sl + sp) = (nml, nmp + nsl + nsp + rml + rmp + rsl + rsp) = (nm, ns + rm + rs)(l,p) = ((n,r)(m,s))(l,p)$, so multiplication

is associative, and $(n,r)((m,s)+(l,p)) = (n,r)(m+l,s+p) = (n(m+l), n(s+p)+r(s+p)+r(m+l)) = (nm+nl, ns+np+rs+rp+rm+rl) = (nm, ns+mr+rs)+(nl, np+rl+rp) = (n,r)(m,s)+(n,r)(l,p)$, so multiplication is distributive. The direct product of abelian groups is an abelian group, so $\tilde{R}$ is a ring. $(n,r)(1,0) = (n, 0+r+0)$, so (1, 0) is the identity in $\tilde{R}$.

(b) $f : r \to (0,r)$ is injective, since its colonel is 0, and its image is clearly $0 \times R$. $f(rl) = (0,rl) = (0,r)(0,l) = f(r)f(l)$, so f is a homomorphism. $0 \times R$ is the colonel of the homomorphism $(n,l) \to n$, so it is an ideal.

(c) Let $\tilde{f}(n,r) = n1 + f(r)$, then $\tilde{f}(0,r) = f(r)$ and $\tilde{f}(1,0) = 1$. $\tilde{f}$ is a homomorphism since $\tilde{f}((n,r)(m,s)) = \tilde{f}(nm, ns+mr+rs) = 1nm + f(ns+mr+rs) = 1nm+nf(s)+mf(r)+f(r)f(s) = (n1+f(r))(m1+f(s)) = \tilde{f}(n,r)\tilde{f}(m,s)$, and $\tilde{f}((n,r)+(m,s)) = \tilde{f}(m+n, r+s) = (m+n)1+f(r+s) = m1+n1+f(r)+f(s) = \tilde{f}(n,r)+\tilde{f}(m,s)$. Uniqueness follows since our $\tilde{f}$ can be derived by starting with $\tilde{f}(0,r) = f(r)$ and $\tilde{f}(1,0) = 1$ and applying the homomorphism properties.

3 Quotient Rings

1. $x^2 = x^2 - 1 + 1$, so $(a+bx)(c+dx) = ac + (ad+bc)x + bdx^2 = ac + (ad+bc)x + bd$.

2. $x^3 = x^3 - 1 + 1$, and $x^4 = x(x^3-1)+x$, so $(a+bx+cx^2)(a'+b'x+c'x^2) = aa' + ab'x + ac'x^2 + ba'x + bb'x^2 + bc'x^3 + ca'x^2 + cb'x^3 + cc'x^4 = (aa'+bc'+cb') + (ab'+ba'+cc')x + (ac'+bb'+ca')x^2$.

3. Let $B \subset \bar{R}$ be a subring, then $\psi^{-1}(B)$ is a subgroup of R and if $x, y \in \psi^{-1}(B)$ then $x = \psi^{-1}(a), y = \psi^{-1}(b)$ for some $a, b \in \bar{R}$ so $xy = \psi^{-1}(a)\psi^{-1}(b) = \psi^{-1}(ab) \in \psi^{-1}(B)$ since B is a ring, so $\psi^{-1}(B)$ is a ring.

   And if I is an ideal in $\bar{R}$ and $x \in \psi^{-1}(I)$ then for any $r \in R$, $r = \psi^{-1}(p)$ for some $p \in \bar{R}$ since ψ is surjective so $rx = \psi^{-1}(p)\psi^{-1}(x) = \psi^{-1}(px) \in \psi^{-1}(I)$, so $\psi^{-1}(I)$ is an ideal.

4. Let $f(x) = x + \bar{I}$, then, $f \circ \rho$ is a surjective ring homomorphism with colonel I since $\rho(I) = \bar{I}$, so by the homomorphism theorem $R/I \cong \bar{R}/\bar{I}$ using $f \circ \rho$ as the subjective map that the theorem refers to, and furthermore $\bar{R} \cong R/J$ and $\bar{I} \cong I/J$ by the homomorphism theorem using ρ as the map.

5. Let $x \in R$. Then $x \in \rho^{-1}(\rho(A)) \leftrightarrow \exists a \in A : \rho(x) = \rho(a) \leftrightarrow x \in a+I \leftrightarrow x \in A+I$, so $\rho^{-1}(\rho(A)) = A+I$. $A+I$ is a group since it's a sum of groups, and $(a+i)(a'+i') = aa' + (ai' + a'i + ii') \in A+I$ since I is an ideal, so $A+I$ is a subring. $A+I$ contains I since $0 \in A$ since A is a ring, and so the homomorphism theorem applied to the restriction of ρ to $A+I$ gives $(A+I)/I \cong \rho(A)$, and the homomorphism theorem with the restriction of ρ to A gives $A/(A \cap I) \cong \rho(A)$, since the colonel of ρ is I.

6. Let N be an ideal in R/M, then $\rho^{-1}(N)$ where ρ is the quotient projection is an ideal in R containing M by Proposition 6.3.7. If N is a nonzero proper ideal then $\rho^{-1}(N)$ is a proper ideal in R, since $x \notin N \leftrightarrow \rho^{-1}(x) \notin \rho^{-1}(N)$, so M is not maximal since this proper ideal contains it. Since ρ^{-1} is a bijection between ideals of R/M and ideals of R containing M, if there is no such proper ideal $N \subset R/M$ then there is no proper ideal of R containing M, so M is maximal.

7. (a) Let $n = mk$ be a factorization of n, then for all $nz \in n\mathbb{Z}$, $nz = mkz$, so $n\mathbb{Z} \subset m\mathbb{Z}$ and $n\mathbb{Z} \subset k\mathbb{Z}$. Iff n is prime, the only such m and k are 1 and n, so $n\mathbb{Z}$ is a maximal ideal.

   (b) Let $f = gh$ be a factorization of f, then for all $fq \in fK[x]$, $fq = ghq$, so $fK[x] \subset gK[x]$ and $fK[x] \subset hK[x]$. Iff f is irreducible, the only such g and h are units and polynomials of the same degree as f, so $fK[x]$ is a maximal ideal.

   (c) This follows from Proposition 6.3.13, which states that a ring modulo a maximal ideal is a field, and $n\mathbb{Z}$ and $fK[x]$ are maximal ideals iff n is prime and f is irreducible.

8. Consider a product $(\sum_j a_j x^j)(\sum_k i_k x^k)$, where $a_j \in R$ and $i_j \in J$. The lth coefficient of this product is $\sum_{j+k=l} a_k i_j$; each element in this sum is a product of an element of I with an element of R, so each element in this sum is in I, so the sum is in I, so the product in question is in $J[x]$, so $J[x]$ is an ideal.

   The map $f : \sum_i r_i x^i \to \sum_i (r_i + J)x^i$ is a homomorphism from $R[x]$ to $(R/J)[x]$ by corollary 6.2.9 since the quotient map is a homomorphism. The colonel of this map is $J[x]$, so by the homomorphism theorem for rings, $R[x]/J[x] \cong (R/J)[x]$.

9. Let $P \in \mathrm{Mat}_n(R), I \in \mathrm{Mat}_n(J)$. Then $(PI)_{ij} = \sum_k P_{ik} I_{kj}$, and each element in that sum is in J since J is an ideal, so the whole sum is in J, so the product $PI \in \mathrm{Mat}_n(J)$, so $\mathrm{Mat}_n(J)$ is an ideal in $\mathrm{Mat}_n(R)$.

   Define $f : \mathrm{Mat}_n(R) \to \mathrm{Mat}_n(R/J)$ by $f(A)_{ij} = A_{ij} + J$, then f is a surjective homomorphism since the quotient map respects addition and multiplication, and its colonel is $\mathrm{Mat}_n(J)$, so $\mathrm{Mat}_n(R)/\mathrm{Mat}_n(J) \cong \mathrm{Mat}_n(R/J)$ by the homomorphism theorem for rings.

10. Let $f(\sum_i r_i x^i) = r_0$, then f is a surjective homomorphism from $R[x]$ to R with colonel $xR[x]$, so by the homomorphism theorem for rings we have $R \cong R[x]/xR[x]$.

11. (a) This map f is injective since if $f(x) = (0 + P, 0 + Q)$, then $x \in P \cap Q = \{0\}$. And it's homomorphic because the quotient map is. For surjectivity, since $P + Q = R$, we have for any $x \in R$ a $p \in P, q \in Q : p + q = x$. So for any $(a + P, b + Q) \in R/P \oplus R/Q$, there is a $p \in P, q \in Q : p + q = a$ and there is $p', \in P, q' \in Q : p' + q' = b$. So let $y = q + p'$. Then $y + P = a + P$, and $y + Q = b + Q$, so $f(y) = (a + P, b + Q)$, so f is surjective.

(b) Let $f(r) = (r + P, r + Q)$ then the same proof as in part a gives that f is an isomorphism from R to $R/P \oplus R/Q$ with colonel $P \cap Q$, and the result follows from the ring homomorphism theorem.

12. Let $a_1, a_2, \ldots a_n$ be a sequence of relatively prime polynomials, and let $a = \prod_i a_i$, then $aK[x] \cong a_1K[x] \oplus a_2K[x] \oplus \ldots \oplus a_nK[x]$ under the isomorphism $g : f \to (f + a_1K[x], f + a_2K[x], \ldots f + a_nK[x])$.

Proof. If $g(q) = 0$, then each a_i divides q, so q is a multiple of a, so it is zero modulo a, so g is injective. g is a homomorphism because the quotient map is. Let $(x_1 + a_1K[x], x_2 + a_2K[x], \ldots x_n + a_nK[x]) \in a_1K[x] \oplus a_2K[x] \oplus \ldots \oplus a_nK[x]$, then we want to find polynomials q_i such that $q_i + a_iK[x] = 1 + a_iK[x]$ and $q_i + a_jK[x] = 0 + a_jK[x] \forall j \neq i$, since if we had such q_i then $\sum_i x_iq_i$ would be the preimage of $(x_1 + a_1K[x], x_2 + a_2K[x], \ldots x_n + a_nK[x])$. So let $n_i = a/a_i$, then $n_i + a_jK[x] = 0 \forall j \neq i$ and n_i is relatively prime to a_i, so there exist polynomials f and g such that $fa_i + gn_i = 1$, so let $q_i = gn_i$, then $q_i + a_iK[x] = 1 + a_iK[x]$ as we desire, so we have found the q_i polynomials we seek and the result follows. □

4 Integral Domains

1. (a) If $r, x \in R, x^k = 0$, then $(rx)^k = r^kx^k = r^k0 = 0$, so the set of nilpotents is an ideal.

   (b) $(r + N)^k = 0 \to r^k + N = 0 + N \to r^k \in N \to r^k$ is nilpotent $\to r$ is nilpotent $\to r \in N \to r + N = 0 + N$.

   (c) If $x^k = 0$, then $0 = \phi(x^k) = \phi(x)^k$, so $\phi(x)$ must be zero or else $\phi(x)^k$ would be a product of nonzero elements whose product is zero, which cannot exist in S since it is an integral domain.

2. Suppose $x^k = 0$. Then computations like $(1 - x)(1 + x) = 1 - x^2$; $(1 - x^2)(1 + x^2) = 1 - x^4$, and so forth give a sequence of ring elements $1 - x^{2^n}$ divisible by 1-x, and you need only repeat until $2^n > k$ to find $1 - x^{2^n} = 1 - 0 = 1$.

3. $e^2 = e \to e(e - 1) = 0$, so in an integral domain e must be 1 or 0, otherwise this product would be a product of nonzero elements that is equal to 0.

4. Let $f, g \in R[x] \setminus \{0\}$, and let m, n be the degrees of f and g. Then the coefficient of x^{m+n} in fg is the product of the coefficients of x^m in f and x^n in g; since R is an integral domain, this product is nonzero since neither m nor n is zero by the definition of degree, so $R[x]$ is an integral domain.

5. Exercise 4 showed that $R[x]$ is an integral domain; another previous exercise showed that $R[x, y] \cong R[x][y]$. So suppose $R[x_1, x_2 \ldots x_n]$ is an integral domain, then

$R[x_1, x_2, \ldots x_{n+1}] \cong R[x_1, x_2 \ldots x_n][x_{n+1}]$, so it is a polynomial ring with coefficients in an integral domain, so it is an integral domain.

6. $R[[x]]$ is an integral domain by the same logic we used in exercise 4, except instead of letting m and n be the degrees of f and g we let them be the smallest powers of x in f and g. The units in $R[[x]]$ are just the units in R, added to an infinite sequence of zeros.

7. (a) R' is a commutative ring with identity by hypothesis, and if $x, y \in R'$ have the property that $xy = 0$, then they have that property as elements of R, so $x = 0$ or $y = 0$.

   (b) The Gaussian integers are a subring of the integral domain of complex numbers that contains 1, so by part a they are an integral domain.

   (c) The symmetric polynomials are a subring of all the polynomials that contains 1, so by part a they are an integral domain.

8. $\mathbb{Z}$ is an integral domain, but $\mathbb{Z}_6$ is not.

9. $a/b \sim a/b$ since $ab = ab$, $a/b \sim c/d \rightarrow ad = bc \rightarrow bc = ad \rightarrow c/d \sim a/b$, and $a/b \sim a'/b', a'/b' \sim a''/b'' \rightarrow ab' = a'b, a'b'' = a''b' \rightarrow ab'a'b'' = a''b'a'b \rightarrow ab'' = a''b \rightarrow a/b \sim a''/b''$.

10. $a/b \sim a'/b', c/d \sim c'/d' \rightarrow a'b = ab', c'd = cd' \rightarrow (dd')ab' = (dd')a'b, (bb')cd' = (bb')c'd \rightarrow (dd')ab' + (bb')cd' = (dd')a'b + (bb')c'd \rightarrow b'd'(ad + bc) = bd(a'd' + c'b') \rightarrow (ad+bc)/bd \sim (a'd' + c'b')/b'd'$, and $ac/bd \cong a'c'b'd' \leftrightarrow acb'd' = a'c'bd \leftrightarrow (ab')(cd') = (a'b)(c'd)$, which follows from our hypotheses, so addition and multiplication on $Q(R)$ are well-defined.

11. (a) $a/b(c/d{*}e/f) = a/b(ce/df) = ace/bdf = (ac/bd){*}e/f = (a/b{*}c/d){*}e/f$, so multiplication is associative. $a/b(c/d+e/f) = a/b((cf+de)/df) = a(cf+de)/bdf = acf/bdf + ade/bdf = ac/bd + ae/bf = a/b(c/d) + a/b(e/f)$, so multiplication is distributive over addition. $(1/1)(a/b) = a/b$, and $(0/1)(a/b) = 0/b = 0/1$, so $1/1$ is the identity and $0/1$ is 0, so $Q(R)$ is a ring with multiplicative identity.

    (b) $a/b + c/d = (ad + bc)/bd = c/d \leftrightarrow a = 0$.

    (c) $(a/b)(b/a) = ab/ba = 1/1$.

12. (a) Let $f(a) = a/1$, then $f(ab) = ab/1 = a/1 * b/1 = f(a)f(b)$ and $f(a + b) = (a + b)/1 = a/1 + b/1 = f(a) + f(b)$ and $f(1) = 1/1$, so f is a unital ring homomorphism.

    (b) Let $g(a/b) = b^{-1}a$, then the colonel of g is $[0/1]$ so g is injective and $g(a/b + c/d) = g((ad + bc)/bd) = d^{-1}b^{-1}(ad + bc) = b^{-1}a + d^{-1}c = g(a/b) + g(c/d)$ and $g(a/b * c/d) = g(ac/bd) = d^{-1}b^{-1}ac = g(a/b)g(c/d)$ and $g(a/1) = a$ and

$g(1/1) = 1$ so g is the injective unital homomorphism we seek. ($b^{-1} \in F$ since F is a field.)

13. Let $f((a+bi)/(c+di)) = (ac+bd+(bc-ad)i)/(c^2+d^2)$, then since the homomorphism is accomplished only by multiplying $(a/bi)/(c+di)$ by $1 = (c-di)/(c-di)$, it is readily apparent that this is an isomorphism.

14. $\exists a, b \in R : (a + J)(b + J) = 0 + J, a + J \neq 0 + J, b + J \neq 0 + J \leftrightarrow a \notin J, b \notin J$, but $ab \in J$, so J is prime if and only if there exist no such a and b.

15. $d\mathbb{Z}$ is the set of multiples of d, so d divides every element of $d\mathbb{Z}$, and so if d is prime then for any product $ab \in d\mathbb{Z}, d$ divides a or d divides b, so $a \in d\mathbb{Z}$ or $b \in d\mathbb{Z}$. On the other hand, if d is not prime, then $d = ab$ for some a, b that d does not divide, and since $ab = d1 \in d\mathbb{Z}, d\mathbb{Z}$ is not prime.

16. Let J be a maximal ideal in a ring R, then by coronary 6.3.14 R/J is a field, so it is an integral domain, so J is prime by Exercise 6.4.14.

5 Euclidean Domains, Principal Ideal Domains, and Unique Factorization

1. (a) Do repeated division with remainder, each time obtaining a remainder of smaller degree. $g = q_1 f + f_1, f = q_2 f1 + f_2, \ldots f_{r-1} = q_{r+1} f_r$. Then $f_r \in gR + fR$, and f_r divides g and f.

   (b) Any common divisor of f and g divides all elements of $fR+gR$, so if $1 \in fR+gR$ then any common divisor of f and g must divide 1 which means it cannot have degree greater than 0 so 1 is a GCD. If $1 \notin fR + gR$, then it can't be the GCD since part a already showed that the GCD is in $fR + gR$.

2. (a) Let I be an ideal in R, and let d be an element of least nonnegative degree in I. Then $dR \subset I$ since I is an ideal and for any $p \in I$ we have $p = qd + r$ where the degree of r is less than the degree of d by the Euclidean properties and $r \in I$ since $p \in I$ and $qd \in I$ so since d has the least nonnegative degree that means that r must be zero so d divides p so $I \subset dR \rightarrow I = dR$.

   (b) Suppose $p = ab$ and p does not divide a, then p and a are relatively prime so $1 \in pR + aR \rightarrow 1 = pr + as$ for some $r, s \in R \rightarrow b = bpd + abs$ and since p divides p and p divides ab, p divides the right hand side of this equation so it divides b.

3. We already showed that R is a principal ideal domain, and that implies that it's a unique factorization domain by 6.5.19.

4. Let $N(z) = |z|^2$ for $z \in \mathbb{Z}[\sqrt{-2}]$, then N respects multiplication since the complex norm has that property and given $z, w \in \mathbb{Z}[\sqrt{2}]$, let q be the element of $\mathbb{Z}[\sqrt{2}]$ closest to z/w then $|R(q - z/w)| \leq 1/2$ and $I(q - z/w)| \leq \sqrt{2}/2$, so $z = qw + r$ where $r \in \mathbb{Z}[\sqrt{2}]$ and $N(r) = |z/w - q|^2 N(w) \leq ((1/2)^2 + (\sqrt{2}/2)^2)N(w) = 3/4N(w)$ so $\mathbb{Z}[\sqrt{2}]$ is Euclidean.

5. This set is isomorphic to the Gaussian integers under the rotation of the complex plane by $2\pi/3$ radians, so it is also a Euclidean domain.

6. $|ab| = |a||b|$, so the norm of a divisor of $x \in \mathbb{Z}[i]$ divides the norm of x, so the norm of a common divisor of $14 + 2i$ and $21 + 26i$ must divide 200 and 1117, which is prime so a GCD is 1.

7. Using the same process, the norm of a common divisor of $33 + 19i$ and $18 - 16i$ must divide 1450 and 580, so it can have norm up to 290, and $17 + i$ has just this norm so it is a common divisor.

8. $a|b \to b = ac; b|a \to a = bd \to b = bdc \to dc = 1 \to c$ and d are units. For the reverse implication, $a = ub \leftrightarrow u^{-1}a = b$.

9. $a = a1$ so it's reflexive. $a = ub \to b = u^{-1}a$ so it's symmetric. $a = ub, b = u'd \to a = uu'd$, and the product of units is a unit so it's transitive.

10. There are no nonzero nonunits of degree 1, 2 or 3, so the base case is the nonzero, nonunit elements of degree 4, ± 2, which are irreducible so they have a factorization by irreducibles. So suppose all nonzero nonunits of degree $\leq n$ have a factorization by irreducibles, then for an element of degree $n + 1$, $n = ab$ is a proper factorization $\leftrightarrow |a| < |n|$ and $|b| < |n|$, since $|n| = |a||b|$ and $|x| = 1 \leftrightarrow x$ is a unit. So for any proper factorization of n, the proper factors have a factorization by irreducibles, so either n is irreducible or it has a factorization by irreducibles; in either case, it has a factorization by irreducibles.

11. Consider $I = \{2x + iy\sqrt{5}\}$, the set of elements of $\mathbb{Z}[\sqrt{-5}]$ whose real part is divisible by 2. Since 2 is irreducible, the only possible x such that $I = x\mathbb{Z}[\sqrt{-5}]$ are $1, -1, 2$, and -2, none of which work.

12. $x\mathbb{Q}[x]$ is an ideal in $\mathbb{Z}+x\mathbb{Q}[x]$, since given $xp(x) \in x\mathbb{Q}[x], n+q(x) \in \mathbb{Z}+x\mathbb{Q}[x], (xp(x))(n+q(x)) = nxp(x)+xp(x)q(x) \in x\mathbb{Q}[x]$, but it is not principal since if $p \in \mathbb{Z}+x\mathbb{Q}[x], p(\mathbb{Z}+x\mathbb{Q}[x])$ is the set of polynomials of degree $d(p)$ or greater whose term of degree p has a coefficient which is an integer times the coefficient of that integer in p, and the integer part of p must be 0 or else products of p and elements of $\mathbb{Z} + x\mathbb{Q}[x]$ will have nonzero integer part so p must be a monomial degree 1 to be even remotely viable, but there is no rational q such that $q\mathbb{Z} = \mathbb{Q}$, so there is no $p = qx$ such that $qx(\mathbb{Z} + x\mathbb{Q}[x]) = x\mathbb{Q}[x]$.

13. $a|b \leftrightarrow b = ax$ for some $x \in R \leftrightarrow$ for any $r \in R, br = axe \in aR \leftrightarrow bR \subset aR$. And then if a is a proper factor of b then $b = ax$ where neither a nor x is a unit, so $bR = axR$ and $1 \notin xR$ since x is not a unit so $a \notin axR \rightarrow a \notin bR$, but $a \in aR$ so $bR \subsetneq aR$. And if a is not a proper factor of b then either a does not divide b, in which case $b \notin aR$ so $bR \not\subseteq aR$, or $b = ax$ where x is a unit so $bR = axR = aR$. You have to suppose a isn't a unit, or the claim doesn't hold.

14. $x|a, x|b \rightarrow x|d \rightarrow x|ud$ for all units u, and ud divides a and b for all u since $a = dx \leftrightarrow ua = udx \leftrightarrow a = (ud)u^{-1}x$. If a and b are associates, then a divides b and b divides a, so they are common divisors of each other, and any d that divides a and b must divide a and b, so a and b are GCDs.

15. Consider the ideal $aR+bR$, then since R is a PID it must equal dR for some d. This d is a greatest common divisor of a and b since $aR \subset dR \rightarrow a \in dR, bR \subset dR \rightarrow b \in dR$, and $d \in dR$ so $d = ar + bs$ for some $r, s \in R$ so any $x \in R$ that divides a and b also divides $ar + bs = d$. Since the GCD in a PID is unique up to multiplication by units, any GCD of a and b must be in $dR = aR + bR$.

    $1 \in aR + bR \leftrightarrow aR + bR = 1R \leftrightarrow d = 1$.

16. Since a is irreducible, the only nonunit that divides a is a, so if a does not divide b the no nonunit divides both a and b, so a and b are relatively prime.

17. Let $x \in abR$. Since $a \in R$, $x \in bR$ and vice versa, so $abR \subset aR \cap bR$. And if $y \in aR, y \in bR$, then $y = ax_1 = bx_2$ for some $x_1, x_2 \in R$, so since a does not divide b it must divide x_2, so $x_2 = ax_2' \rightarrow y = bax_2' \in abR$, so $aR \cap bR \subset abR$, so $abR = aR \cap bR$.

    $aR + bR = 1R = R$ by exercise 16.

    Let $f(x) = (x + aR, x + bR)$ where $x \in R$, then f is a homomorphism from R to $R/aR \oplus R/bR$ with colonel abR, so $R/abR \cong R/aR \oplus R/bR$.

18. (a) The factors of x are x times elements of K, and the factors of y are y times elements of K, and since y does not divide x nor does x divide y, their only common factors are elements of K which are units.

    (b) The constant term of $xp(x)$ is 0, as is the constant term of $yp(y)$, so the constant term of their sum is $0 \neq 1$.

    (c) $xK[x, y]+yK[x, y]$ is an ideal, so if $K[x, y]$ were a PID then it would be principal, but by part b it is not, so $K[x, y]$ is not a PID.

19. If p is not irreducible then $p = ab$ where a and b are not units, so if p is prime then it divides a or b so supposing without loss of generality that p divides a we have $a = a'p \rightarrow p = ab = pa'b \rightarrow b$ is a unit, so p cannot be prime if it is not irreducible, so all primes are irreducible.

20. If $k = 2$, this is the definition of primality. Suppose the statement holds for some k, then $b_1 b_2 \cdots b_{k+1} = (b_1)(b_2 \cdots b_{k+1})$ so p divides either b_1 or $b_2 \cdots b_{k+1}$ and in either case it divides one of the b_i.

21. If f is the quotient map $x \to x + aR$, then f^{-1} maps ideals of R/aR to ideals of R containing aR, so if there are infinite ideals in R/aR then there are infinite ideals in R that contain aR, but by exercise 13 $aR \subsetneq bR \leftrightarrow b$ is a proper factor of a, so there are only as many ideals in R containing aR as there are proper factors of a plus one for aR itself plus one for R, so there are only finitely many ideals since no element of a PID has an infinite number of proper factors.

22. (a) p not prime $\leftrightarrow \exists a, b : p \not| a, p \not| b, p|ab \leftrightarrow, a + pR \neq 0 + pR, b + pR \neq 0 + pR, ab + pR = 0 + pR \leftrightarrow R/pR$ not an integral domain.

    (b) By 6.3.14, R/M is a field iff M is maximal, and by 6.5.18, pR is maximal iff p is irreducible in a PID, so putting these two together we get R/aR is a field if and only if a is irreducible.

    (c) All fields are integral domains. If $R/I = R/aR$ is an integral domain, then by part a, a is prime, so a is irreducible, so by part b, $R/aR = R/I$ is a field.

    (d) This is part of Lemma 6.5.18.

23. (a) Let $A = \sum_i a_i x^i$ be a power series, then we need a sequence $B = \sum_j b_j x^j$ such that for each $n \geq 1$, $(AB)_n = 0$, and $(AB)_0 = 1$. We will construct this sequence inductively. Let $b_0 = a_0^{-1}$, then since $(AB)_0 = a_0 b_0$, this is the only possible value for b_0. Now suppose the first n terms of our B series are defined, so that $(AB)_0 = 0$ and $(AB)_k = 0$ for $1 \leq k \leq n$. The coefficient of x^{n+1} in AB is $A_0 B_{n+1} + \sum_{i=1}^{n} A_i B_{n+1-i}$, so setting $B_{n+1} = -A_0^{-1}(\sum_{i=1}^{n} A_i B_{n+1-i})$ gives us the desired properties. This defines the inverse of any sequence with a nonzero constant term, so those are units in $K[[x]]$, and it is clear that no other element is a unit since if the constant term of A is 0 then the constant term of $AB = 0 \neq 1$ for all B.

    (b) Let J be an ideal of $K[[x]]$, and let n be the least integer such that J has an element of the form $a_n x^n + \sum_{j>n} a_j x^j$ where $a_n \neq 0$. Then $J \subset x^n K[[x]]$. Furthermore, $a_n x^n + \sum_{k>n} a_k x^k = x^n(a_n + \sum_{k>0} a_{k+n} x^k)$, and $A = a_n + \sum_{k>0} a_{k+n} x^k$ is a unit by part a, so for any $B = x^n \sum_i b_i x^i \in x^n K[[x]], B = x^n A A^{-1} \sum_i b_i x^i$, so $x^n K[[x]] \subset J$, so $J = x^n K[[x]]$.

    (c) x is prime so $xK[[x]]$ is maximal by 6.5.18, and if I is some maximal ideal in $K[[x]]$ then $I = x^n K[[x]]$ for some n but the only n such that $x^n K[[x]]$ is prime is 1, so $xK[[x]]$ is unique. $K[[x]]/xK[[x]] \cong K$ since $K[[x]]/xK[[x]]$ it consists of equivalence classes $k + xK[[x]]$ for all $k \in K$.

24. Let I be an ideal in $\mathbb{Q}_p$, and let p^k be the smallest value of p such that I contains an element $p^k a/b$ where p does not divide a. Then $b/a \in I$, so $p^k \in I$, so $p^k a'/b' \in I$ for all $a'/b' \in \mathbb{Q}_p$, so $p^k\mathbb{Q}_p \subset I$. By assumption, $I \subset p^k\mathbb{Q}_p$, so $I = p^k\mathbb{Q}_p$, so $I = p^k\mathbb{Q}_p$, so I is principal.

6 Unique Factorization Domains

1. (a) The GCD of several elements a_i in a UFD is constructed in the proof of lemma 6.6.2; it is the product of the intersection of the common nonunit factors of all the a_i. It is readily apparent that the intersection of the common nonunit factors of the ba_i is the union of b and the intersection of the common factors of the a_i.

   (b) If f is primitive then 1 is the GCD of its coefficients so $b1 = b$ is the gcd of b times its coefficients by part a.

2. (a) Both rings consist of linear combinations of powers of the x_i, and they have the same addition and multiplication rules, so they are the same.

   (b) 6.6.7 is the base case, and part a is the inductive step.

3. $p(r/s) = 0 \leftrightarrow (x - r/s)|p \leftrightarrow sx - r|p$ so if $q = \sum_i q_i x^i$ is $p/(sx - r)$ then $p_n = sq_n \rightarrow s|p_n$ and $p_0 = rq_0 \rightarrow r|p_0$.

4. We didn't use any special properties of the integers in proving the previous exercise, just the general properties of fields of fractions and Gauss's lemma.

5. (a) $\pi_p(h) = 0 \leftrightarrow \forall i, \pi_p(h_i) = 0 \leftrightarrow \forall i, p|h_i$.

   (b) $\pi_p(f) = 0 \leftrightarrow \forall i, p|f_i \leftrightarrow \exists$ an irreducible p dividing all coefficients of $f \leftrightarrow f$ is not primitive.

   (c) p is prime $\rightarrow pR$ is prime $\rightarrow R/pR$ is an integral domain by 6.4.11.

   (d) Iff an irreducible element p divides all the coefficients of fg, then $fg + pR = 0 + pR$, so either $f + pR = 0 + pR$ or $g + pR = 0 + pR$ since R/pR is an integral domain by part c, so p divides all the coefficients of f or all those of g by part a, so one of f and g is not primitive. Thus, fg is primitive $\leftrightarrow f$ and g are primitive.

6. 3 is irreducible but not prime since it divides $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. But $\mathbb{Z}[\sqrt{-5}]$ satisfies the ACC since $a\mathbb{Z}[\sqrt{-5}] \subset b\mathbb{Z}[\sqrt{-5}] \leftrightarrow b|a$. That's because if $a = bx$ then for any $ay \in a\mathbb{Z}[\sqrt{-5}]$, $ay = bxy \in b\mathbb{Z}[\sqrt{-5}]$. Whereas if b does not divide a then $a \notin b\mathbb{Z}[\sqrt{-5}]$.

7. If $f(x) = z + xp(x) \in \mathbb{Z} + x\mathbb{Q}[x]$ is irreducible in $\mathbb{Z} + x\mathbb{Q}[x]$, so it is irreducible in $\mathbb{Z}[x] \subset \mathbb{Z} + x\mathbb{Q}[x]$, so it is irreducible in $\mathbb{Q}[x]$ by Gauss's lemma, so it is prime in $\mathbb{Q}[x]$ since $\mathbb{Q}[x]$ is a UFD, so it is prime in $\mathbb{Z} + x\mathbb{Q}[x] \subset \mathbb{Q}[x]$.

   The sequence $A_n = x/2^n(\mathbb{Z}+x\mathbb{Q}[x]), n = 1, 2, 3 \ldots$ is an infinite sequence of increasing principal ideals in $\mathbb{Z} + x\mathbb{Q}[x]$, since A_n does not contain the polynomials whose x coefficient is $1/2^{n+1}$ whereas A_{n+1} does contain them, and $A_n \subset A_{n+1}$ since $2A_{n+1} = A_n$ and $2 \in \mathbb{Z} + x\mathbb{Q}[x]$.

7 Noetherian Rings

1. Let $ax^k \in J$, then for all $r \in R$, $arx^k \in J$ since J is an ideal, so $aR \subset A_k$, so A_k is an ideal. $A_k \subset A_{k+1}$ because for all $bx^k \in J$, $xb^k = bx^{k+1} \in J$, again since J is an ideal.

2. Let J be an ideal in S, then by 6.3.7, $I = \psi^{-1}(J)$ is an ideal in R, so I is finitely generated since R is Noetherian, so if $\{a_1, a_2 \ldots a_k\}$ are the generators of I then $\{\psi(a_1), \psi(a_2), \ldots \psi(a_n)\}$ are the generators of J since for $j \in J$ we have $j = \psi(i)$ for some $i \in I$, and i is a product of some of the a_k since they generate I, and ψ is a homomorphism so it respects this multiplication. Thus, any ideal in the range of ψ is finitely generated, and since ψ is surjective that means all of the ideals in S are finitely generated, so S is Noetherian.

3. For $f \in \mathbb{Z}[x]$, let $\psi(f) = f(\sqrt{-5})$, then ψ is a homomorphism since it is an evaluation of a polynomial which was shown to be a homomorphism in 6.2.7, and ψ is surjective since $\psi^{-1}(a + b\sqrt{-5}) = \psi(a + bx)$, so $\mathbb{Z}[\sqrt{-5}]$ is Noetherian by 2.

4. We showed in Exercise 6.6.7 that principal ideals don't satisfy the ascending chain condition in $\mathbb{Z} + x\mathbb{Q}[x]$, so it is not Noetherian.

5. If R is Noetherian, then all increasing sequences of ideals are finite, so in particular all increasing sequences of principal ideals are finite. This plus every irreducible element is prime means that R is a unique factorization domain by Proposition 6.6.16.

8 Irreducibility Criteria

1. By Proposition 1.8.22, f has no factor of degree 1 if it has no rational root. So if $f = pq$, where $p, q \in \mathbb{Z}[x]$ have degree between 1 and $n - 1$ exclusive, then $\pi_p(f) = \pi_p(a)\pi_p(b)$, and by assumption $\pi_p(f) = (x + r)(q)$ for some $r \in \mathbb{Z}_p, q \in \mathbb{Z}_p(x)$. But so then modulo p, $ab = (x + r)q$, so since q is irreducible by hypothesis it must divide a or b, which it can't because their degree is lower than q's, so there can exist no such factorization ab of f.

2. $f(x+1) = \sum_{n=0}^{p-1}(x+1)^n = \sum_{n=0}^{p-1}(\sum_{k=0}^{n}\binom{n}{k}x^k)$ by the binomial theorem. So the coefficient of x^k in the expanded product is $\sum_{n=0}^{p-1}\binom{n}{k} = \sum_{n=k}^{p-1}\binom{n}{k} = \binom{p}{k+1}$, so p divides each coefficient except when $k = p-1$ and the coefficient is 1, and p^2 does not divide the zeroth coefficient which is $\binom{p}{1} = p$, so by Eisenstein's criterion f is irreducible. Lemma: $\sum_{n=k}^{p-1}\binom{n}{k} = \binom{p}{k+1} \forall p \in \mathbb{N} \forall k < p$.

   Proof. For $p = 1$, $\sum_{n=0}^{0}\binom{n}{0} = 1 = \binom{1}{1}$. And then if the lemma holds all the way to $p-1$, then $\sum_{n=0}^{p-1}\binom{n}{k} = \sum_{n=0}^{p-2}\binom{n}{k} + \binom{p-1}{k} = \binom{p-1}{k-1} + \binom{p-1}{k} = \binom{p}{k+1}$ by 1.9.3c. □

3. Let $f_n(x)$ be the polynomial under consideration. So $f_n(k) = -1$ for $k = 1, 2, 3, \ldots n$, so if $f_n(x) = g(x)h(x)$ for some proper factors g and h (which then must have degree less than $\deg(f_n) = n$), then $g(k) = \pm 1, h(k) = \mp 1$ for $k = 1, 2, 3, \ldots n$. So $g(k) + h(k) = 0$ at all these points, so $g + h$ has n zeros, and since the degree of $g + h$ is less than n, $g + h = 0 \to g = -h$. So $f_n(x) = -g(x)^2$, but the degree-n term of f_n is 1, and there is no integer polynomial g whose square has degree-n term -1, since the degree-$n/2$ term of g would have to be $\sqrt{-1}$, so f has no proper factorization.

4. The same train of logic as in exercise 3 leads us to the conclusion that $f_n(x) = g(x)^2$ for some polynomial $g(x)$, if f_n has any proper factorization at all. Beyond that, though, you're on your own.

5. Computers can do this crap well enough that I don't need to bother with it.