SECTION 21

1. $(a : a^4 = 1); (a, b : a^4 = 1, b = a^2); (a, b, c : a = 1, b^4 = 1, c = 1)$. (Other answers are possible.)

3. *Octic group:*

	1	a	a^2	a^3	b	ab	a^2b	a^3b
1	1	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	1	ab	a^2b	a^3b	b
a^2	a^2	a^3	1	a	a^2b	a^3b	b	ab
a^3	a^3	1	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	1	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	1	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	1	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	1

Quaternion group: The same as the table for the octic group except that the 16 entries in the lower right corner are

a^2	a	1	a^3
a^3	a^2	a	1
1	a^3	a^2	a
a	1	a^3	a^2

5. $\mathbb{Z}_{21}$. $(a, b : a^7 = 1, b^3 = 1, ba = a^2b)$

SECTION 22

1. 0 **3.** 1 **5.** $(1, 6)$

7. Commutative ring, no unity, not a field

9. Commutative ring with unity, not a field

11. Commutative ring with unity, not a field

13. No. $\{ri | r \in \mathbb{R}\}$ is not closed under multiplication.

15. $(1, 1)$,$(1, -1), (-1, 1), (-1, -1)$

17. All nonzero $q \in \mathbb{Q}$ **19.** 1, 3

21. Let $\mathbb{R} = \mathbb{Z}$ with unity 1 and $\mathrm{R}' = \mathbb{Z} \times \mathbb{Z}$ with unity $1' = (1, 1)$. Let $\phi : R \to R'$ be defined by $\phi(n) = (n, 0)$. Then $\phi(1) = (1, 0) \neq 1'$.

23. $\phi_1 : \mathbb{Z} \to \mathbb{Z}$ where $\phi_1(n) = 0, \phi_2 : \mathbb{Z} \to \mathbb{Z}$ where $\phi_2(n) = n$

25. $\phi_1 : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ where $\phi_1(n, m) = 0, \phi_2 : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ where $\phi_2(n, m) = n$
$\phi_3 : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ where $\phi_3(n, m) = m$

27. The reasoning is not correct since a product $(X - I_3)(X + I_3)$ of two matrices may be the zero matrix 0 without having either matrix be 0. Counterexample:

$$\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}^2 = I_3.$$

29. 2,10. In the ring $\mathbb{Z}_{14}$ there are nonzero elements 2 and 7 which when multiplied give 0. This is not the case in $\mathbb{Z}_{13}$.

33. $a = 2, b = 3$ in $\mathbb{Z}_6$

35. **a.** *T* **c.** *F* **e.** *T* **g.** *T* **i.** *T*

SECTION 23

1. 0, 3, 5, 8, 9, 11 **3.** No solutions **5.** 0 **7.** 0 **9.** 12
11. 1, 5 are units; 2, 3, 4 are 0 divisors.
13. 1, 2, 4, 7, 8, 11, 13, 14 are units; 3, 5, 6, 9, 10, 12 are 0 divisors.
15. (1, 1), (1, 2), (2, 1), (2, 2) are units; (0, 1), (0, 2), (1, 0), (2, 0) are 0 divisors.
17. $a^4 + 2a^2b^2 + b^4$ **19.** $a^6 + 2a^3b^3 + b^6$
23. **a.** F **c.** F **e.** T **g.** F **i.** F
25. **1.** $\text{Det}(A) = 0$. **2.** The column vectors of A are dependent.
3. The row vectors of A are dependent. **4.** Zero is an eigenvalue of A.
5. A is not invertible.

SECTION 24

1. 3 or 5 **3.** Any of 3, 5, 6, 7, 10, 11, 12, or 14. **5.** 2
7.

$\varphi(1) = 1$	$\varphi(7) = 6$	$\varphi(13) = 12$	$\varphi(19) = 18$	$\varphi(25) = 20$
$\varphi(2) = 1$	$\varphi(8) = 4$	$\varphi(14) = 6$	$\varphi(20) = 8$	$\varphi(26) = 12$
$\varphi(3) = 2$	$\varphi(9) = 6$	$\varphi(15) = 8$	$\varphi(21) = 12$	$\varphi(27) = 18$
$\varphi(4) = 2$	$\varphi(10) = 4$	$\varphi(16) = 8$	$\varphi(22) = 10$	$\varphi(28) = 12$
$\varphi(5) = 4$	$\varphi(11) = 10$	$\varphi(17) = 16$	$\varphi(23) = 22$	$\varphi(29) = 28$
$\varphi(6) = 2$	$\varphi(12) = 4$	$\varphi(18) = 6$	$\varphi(24) = 8$	$\varphi(30) = 8$

9. $(p - 1)(q - 1)$ **11.** $1 + 4\mathbb{Z}, 3 + 4\mathbb{Z}$ **13.** No solutions
15. No solutions
17. $3 + 65\mathbb{Z}, 16 + 65\mathbb{Z}, 29 + 65\mathbb{Z}, 42 + 65\mathbb{Z}, 55 + 65\mathbb{Z}$
19. 1 **21.** 9
23. **a.** F **c.** T **e.** T **g.** F **i.** F

SECTION 25

1. $n = pq = 15$, $(p - 1)(q - 1) = 8$, so the pairs are (3, 3), (5, 5)
3. $n = pq = 33$, $(p - 1)(q - 1) = 20$, so the pairs are (3,7), (7,3), (9,9), (11,11), (13,17), (17,13)
5. $s = 77$
7. **a.** $y = 64$ **b.** $r = 13$ **c.** $64^{13} \equiv 25 \pmod{143}$
9. Private key is $p = 257$, $q = 359$, $n = 92263$, $r = 1493$. Public key is $n = 92263$ and $s = 9085$.

SECTION 26

1. $\{q_1 + q_2 i \mid q_1, q_2 \in \mathbb{Q}\}$
15. It is isomorphic to the ring D of all rational numbers that can be expressed as a quotient of integers with denominator some power of 2.
17. It runs into trouble when we try to prove the transitive property in the proof of Lemma 5.4.2, for multiplicative cancellation may not hold. For $R = \mathbb{Z}_6$ and $T = \{1, 2, 4\}$ we have $(1, 2) \sim (2, 4)$ since $(1)(4) = (2)(2) = 4$ and $(2, 4) \sim (2, 1)$ since $(2)(1) = (4)(2)$ in $\mathbb{Z}_6$. However, (1, 2) is not equivalent to (2, 1) because $(1)(1) \neq (2)(2)$ in $\mathbb{Z}_6$.

SECTION 27

1. $f(x) + g(x) = 2x^2 + 5, f(x)g(x) = 6x^2 + 4x + 6$
3. $f(x) + g(x) = 5x^2 + 5x + 1, f(x)g(x) = x^3 + 5x$
5. 16 **7.** 7 **9.** 2 **11.** 0 **13.** 2, 3 **15.** 0, 2, 4
17. 0, 1, 2, 3
21. $0, x - 5, 2x - 10, x^2 - 25, x^2 - 5x, x^4 - 5x^3$. (Other answers are possible.)
23. **a.** T **c.** T **e.** F **g.** T **i.** T
25. **a.** They are the units of D. **b.** $1, -1$ **c.** 1, 2, 3, 4, 5, 6
27. **b.** F **c.** $F[x]$ **31.** **a.** 4, 27 **b.** $\mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

SECTION 28

1. $q(x) = x^4 + x^3 + x^2 + x - 2, r(x) = 4x + 3$
3. $q(x) = 6x^4 + 7x^3 + 2x^2 - x + 2, r(x) = 4$
5. 2, 3 **7.** 3, 10, 5, 11, 14, 7, 12, 6
9. $(x - 1)(x + 1)(x - 2)(x + 2)$
11. $(x - 3)(x + 3)(2x + 3)$
13. Yes. It is of degree 3 with no zeros in $\mathbb{Z}_5$.
$2x^3 + x^2 + 2x + 2$
15. *Partial answer:* $g(x)$ is irreducible over $\mathbb{R}$, but it is not irreducible over $\mathbb{C}$.
19. Yes. $p = 3$ **21.** Yes. $p = 5$
25. **a.** T **c.** T **e.** T **g.** T **i.** T
27. $x^2 + x + 1$
29. $x^2 + 1, x^2 + x + 2, x^2 + 2x + 2, 2x^2 + 2, 2x^2 + x + 1, 2x^2 + 2x + 1$
31. $p(p - 1)^2/2$

SECTION 29

1. 32
3. $\mathbb{Z}_2^5$
5. **a.** $\{(0, 0)\}, \{(0, 0), (1, 1)\}, \mathbb{Z}_2^2$ **b.** $\{0, 0, 0\}, \{(0, 0, 0), (1, 1, 1)\}, \mathbb{Z}_2^3$
c. $\{(0, 0, 0, 0)\}, \{(0, 0, 0, 0), (1, 1, 1, 1)\}, \{(0, 0, 0, 0), (0, 1, 0, 1), (1, 0, 1, 0), (1, 1, 1, 1)\}, \mathbb{Z}_2^4$
7. **a.** $x^7 + 1 = (x^3 + x + 1)(x^4 + x^2 + x + 1)$ **b.** C consists of the cyclic shifts of $x^3 + x + 1, x^4 + x^3 + x^2 + 1$ together with 0 and $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. **c.** A single bit error can be detected and corrected. **d.** A two-bit error can be detected, but not corrected.
9. **a.** Use long division to verify that $(x^3 + 1)(x^6 + x^3 + 1) = x^9 + 1$.
b. $C = \{x^6 + x^3 + 1, x^7 + x^4 + x, x^8 + x^5 + x^2, x^7 + x^6 + x^4 + x^3 + x + 1, x^8 + x^7 + x^5 + x^4 + x^2 + x, x^8 + x^6 + x^5 + x^3 + x^2 + 1, x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x^1 + 1, 0\}$
c. The minimal weight among the nonzero words is 3, so the minimum distance between two different code words is 3. So C detects and corrects a one bit error.
d. A two-bit error would be detected, but it could not be corrected.
11. $x^9 + 1 = (x + 1)(x^2 + x + 1)(x^6 + x^3 + 1)$, so the polynomials $x + 1$, $x^2 + x + 1$, $x^6 + x^3 + 1$, $(x + 1)(x^2 + x + 1)$, $(x + 1)(x^6 + x^3 + 1)$, and $(x^2 + x + 1)(x^6 + x^3 + 1)$ all generated cyclic codes with code word length 9.

SECTION 30

1. There are just nine possibilities:
$\phi(1, 0) = (1, 0)$ while $\phi(0, 1) = (0, 0)$ or $(0, 1)$,
$\phi(1, 0) = (0, 1)$ while $\phi(0, 1) = (0, 0)$ or $(1, 0)$,
$\phi(1, 0) = (1, 1)$ while $\phi(0, 1) = (0, 0)$, and
$\phi(1, 0) = (0, 0)$ while $\phi(0, 1) = (0, 0), (1, 0), (0, 1)$, or $(1, 1)$.
3. $\langle 0\rangle = \{0\}, \mathbb{Z}_{12}/\{0\} \simeq \mathbb{Z}_{12}$
$\langle 1\rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}, \mathbb{Z}_{12}/\langle 1\rangle \simeq \{0\}$
$\langle 2\rangle = \{0, 2, 4, 6, 8, 10\}, \mathbb{Z}_{12}/\langle 2\rangle \simeq \mathbb{Z}_2$
$\langle 3\rangle = \{0, 3, 6, 9\}, \mathbb{Z}_{12}/\langle 3\rangle \simeq \mathbb{Z}_3$
$\langle 4\rangle = \{0, 4, 8\}, \mathbb{Z}_{12}/\langle 4\rangle \simeq \mathbb{Z}_4$
$\langle 6\rangle = \{0, 6\}, \mathbb{Z}_{12}/\langle 6\rangle \simeq \mathbb{Z}_6$
9. Let $\phi : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ be given by $\phi(n) = (n, 0)$ for $n \in \mathbb{Z}$.
11. R/R and $R/\{0\}$ are not of real interest because R/R is the ring containing only the zero element, and $R/\{0\}$ is isomorphic to R.
13. $\mathbb{Z}$ is an integral domain. $\mathbb{Z}/4\mathbb{Z}$ is isomorphic to $\mathbb{Z}_4$, which has a divisor 2 of 0.
15. $\{(n, n) \mid n \in \mathbb{Z}\}$. (Other answers are possible.)
31. The nilradical of $\mathbb{Z}_{12}$ is $\{0, 6\}$. The nilradical of $\mathbb{Z}$ is $\{0\}$ and the nilradical of $\mathbb{Z}_{32}$ is $\{0, 2, 4, 6, 8, \cdots, 30\}$.

35. **a.** Let $R = \mathbb{Z}$ and let $N = 4\mathbb{Z}$. Then $\sqrt{N} = 2\mathbb{Z} \neq 4\mathbb{Z}$
b. Let $R = \mathbb{Z}$ and let $N = 2\mathbb{Z}$. Then $\sqrt{N} = N$.

SECTION 31

1. $\{0, 2, 4\}$ and $\{0, 3\}$ are both prime and maximal.
3. $\{(0, 0), (1, 0)\}$ and $\{(0, 0), (0, 1)\}$ are both prime and maximal.
5. 1 **7.** 2 **9.** 1, 4 **15.** $2\mathbb{Z} \times \mathbb{Z}$ **17.** $4\mathbb{Z} \times \{0\}$
19. Yes. $x^2 - 6x + 6$ is irreducible over $\mathbb{Q}$ by Eisenstein with $p = 2$.
27. Yes. $\mathbb{Z}_2 \times \mathbb{Z}_3$
29. No. Enlarging the domain to a field of quotients, you would have to have a field containing two different prime fields $\mathbb{Z}_p$ and $\mathbb{Z}_q$, which is impossible.

SECTION 32

1. $1e + 0a + 3b$ **3.** $2e + 2a + 2b$ **5.** j **7.** $(1/50)j - (3/50)k$
9. $\mathbb{R}^*$, that is, $\{a_1 + 0i + 0j + 0k \mid a_1 \in \mathbb{R}, a_1 \neq 0\}$
11. **a.** F **c.** F **e.** F **g.** T **i.** T
c. If $|A| = 1$, then $\mathrm{End}(A) = \{0\}$. **e.** $0 \in \mathrm{End}(A)$ is not in $\mathrm{Iso}(A)$.
19. **a.** $K = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$.
b. Denoting by B the matrix with coefficient b and by C the matrix with coefficient c and the 2×2 identity matrix by I, we must check that

$$B^2 = -I, C^2 = -I, K^2 = -I,$$
$$CK = B, KB = C, CB = -K, KC = -B, \text{ and } BK = -C.$$

c. We should check that ϕ is one-to-one.

SECTION 33

1. $\{(0, 1), (1, 0)\}, \{(1, 1), (-1, 1)\}, \{(2, 1), (1, 2)\}$. (Other answers are possible.)
3. No. $2(-1, 1, 2) - 4(2, -3, 1) + (10, -14, 0) = (0, 0, 0)$
5. $1, \sqrt{2}$ (answers can vary)
7. Infinite Dimensional
9. Infinite Dimensional
15. **a.** T **c.** T **e.** F **g.** F **i.** F
17. **a.** The **subspace of** V **generated by** S is the intersection of all subspaces of V containing S.
19. *Partial answer:* A basis for F^n is

$$\{(1, 0, \cdots, 0), (0, 1, \cdots, 0), \cdots, (0, 0, \cdots, 1)\}$$

where 1 is the multiplicative identity of F.
25. **a.** A homomorphism
b. *Partial answer:* The **kernel** (or **nullspace**) of ϕ is $\{\alpha \in V \mid \phi(\alpha) = 0\}$.
c. ϕ is an isomorphism of V with V' if $\mathrm{Ker}(\phi) = \{0\}$ and ϕ maps V onto V'.

SECTION 34

1. Yes **3.** No **5.** No. **7.** Yes
9. In $\mathbb{Z}[x]$: only $2x - 7, -2x + 7$
In $\mathbb{Q}[x]$: $4x - 14, x - \frac{7}{2}, 6x - 21, -8x + 28$
In $\mathbb{Z}_{11}[x]$: $2x - 7, 10x - 2, 6x + 1, 3x - 5, 5x - 1$
11. $26, -26$ **13.** $198, -198$
15. It is already "primitive" because every nonzero element of $\mathbb{Q}$ is a unit. Indeed $18ax^2 - 12ax + 48a$ is primitive for all $a \in \mathbb{Q}, a \neq 0$.

17. $2ax^2 - 3ax + 6a$ is primitive for all $a \neq 0$ in $\mathbb{Z}_7$ because every such element a is a unit in $\mathbb{Z}_7$.
21. **a.** T **c.** T **e.** T **g.** F **i.** F
i. Either p or one of its associates must appear in every factorization *into irreducibles*.
23. $2x + 4$ is irreducible in $\mathbb{Q}[x]$ but not in $\mathbb{Z}[x]$.
31. *Partial answer:* $x^3 - y^3 = (x - y)(x^2 + xy + y^2)$

SECTION 35

1. Yes **3.** No. (1) is violated. **5.** Yes
7. 61 **9.** $x^3 + 2x - 1$ **11.** 66
13. **a.** T **c.** T **e.** T **g.** T **i.** T
23. *Partial answer:* The equation $ax = b$ has a solution in $\mathbb{Z}_n$ for nonzero $a, b \in \mathbb{Z}_n$ if and only if the positive gcd of a and n in $\mathbb{Z}$ divides b.

SECTION 36

1. $5 = (1 + 2i)(1 - 2i)$ **3.** $4 + 3i = (1 + 2i)(2 - i)$
5. $6 = (2)(3) = (-1 + \sqrt{-5})(-1 - \sqrt{-5})$ **7.** $7 - i$
15. **c.** **i)** order 9, characteristic 3 **ii)** order 2, characteristic 2
iii) order 5, characteristic 5

SECTION 37

1. $\{x, y\}$
3. $\{x + 4, y - 5\}$
5. By multiplying the first polynomial by -2 and adding to the second polynomial, we have $I = \langle x + y + z, -y + z - 4\rangle$. The algebraic variety is $\{4 - 2z, z - 4, z) \mid z \in \mathbb{R}\}$ which is a line through $(4, -4, 0)$.
7. After two careful long divisions, $I = \langle x^2 + x - 2\rangle$. The algebraic variety is $\{1, -2\}$.
9. F^2
11. **a.** $\emptyset$, **b.** $\{i, -i\}$
13. **a.** T **c.** T **e.** T **g.** T **i.** T

SECTION 38

1. $-3x^3 + 7x^2y^2z - 5x^2yz^3 + 2xy^3z^5$
3. $2x^2yz^2 - 2xy^2z^2 - 7x + 3y + 10z^3$
5. $2z^5y^3x - 5z^3yx^2 + 7zy^2x^2 - 3x^3$
7. $10z^3 - 2z^2y^2x + 2z^2yx^2 + 3y - 7x$
9. $1 < z < y < x < z^2 < yz < y^2 < xz < xy < x^2 < z^3 < yz^2 < y^2z < y^3 < xz^2 < xyz < xy^2 < x^2z < x^2y < x^3 < \cdots$
11. $3y^2z^5 - 8z^7 + 5y^3z^3 - 4x$ **13.** $3yz^3 - 8xy - 4xz + 2yz + 38$
15. $\langle y^5 + y^3, y^3 + z, x - y^4\rangle$ **17.** $\langle y^2z^3 + 3, -3y - 2z, y^2z^2 + 3\rangle$
19. $\{1\}$ **21.** $\{x - 1\}$
23. $\{2x + y - 5, y^2 - 9y + 18\}$
The algebraic variety is $\{(1, 3), (-\frac{1}{2}, 6)\}$.
25. $\{x + y, y^3 - y + 1\}$
The algebraic variety consists of one point $(a, -a)$ where $a \approx 1.3247$.
27. **a.** F **c.** T **e.** T **g.** T **i.** F
29. Any order with d_1 and d_2 (in either order) the largest.