

Answers

CHAPTER 0

(1) $\{1, 4\}$; (2) 6; (3) not 1-1 but onto; (4) $2^9, 2^{16}$; (5) 2, 3; (6) $\sqrt{5}, -2 - i, -\frac{2+i}{\sqrt{5}}$; (7) -1 ; (8) $1, \varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4$ where $\varepsilon = e^{2\pi i/5}$; (9) ε^4 ; (10) -1 ; (11) $y = 4x - 7$ and $x^2 + y^2 - 2x + 6y - 58 = 0$; (12) YES; (13) NO since if $\alpha = 2^{1/3}$ the set contains α but not α^2 it does not contain α (if $\alpha^2 = a + b\alpha$ then cubing both sides we can show that $2^{1/3}$ is rational); (14) YES; (15) NO since these are 3 vectors in a 2-dimensional vector space; (16) 5; (17) $-2, -3$; (18) Non-real zeros come in conjugate pairs; (19) This has real coefficients and odd degree so there must be a real zero; (20) The product of the linear factors for α and its conjugate is real: $x^2 - 2\operatorname{Re}(\alpha)x + |\alpha|^2$; (21) Only quadratics with negative discriminants; (22) $\operatorname{GCD} = x + 1$, $h(x) = 1/3$ and $k(x) = (2 - x)/3$; (23) 8; (24) 4; (25) $\{\pm 1\}$; (26) 6 doesn't divide 100; (27) Just G itself and the trivial subgroup; (28) C_n exists for all n and for $n = 3, 5, 7$ (all primes) there's no other group of order n ; (29) $H = \{1, 11\}$, $3H = \{3, 13\}$, $7H = \{7, 17\}$, $9H = \{9, 19\}$ and $G/H \cong C_4$; (30) $(xy)^f = \log((xy)^2) = \log(x^2) + \log(y^2) = x^f + y^f$, $\ker f = \{\pm 1\}$, $\operatorname{im} f = \mathbf{R}, G/\{\pm 1\}$. We can't write $\log(x^2) = 2\log x$ if $x < 0$; (31) All of them; (32) Both groups of order 4 are abelian and so G' is abelian and hence $G'' = 1$; (33) $D_{60}' = \langle A^{15} \rangle$ and $D_{60}'' = 1$; (34) There is at least one proper non-trivial subgroup for each of the following prime power orders: 2, 4, 5, 8 and 16; (35) 125; (36) $ab = (2\ 3\ 4\ 5)$ so $(ab)^{-2}b(ab)^2 = (14)$; (37) YES (odd \times even \times odd = even); (38) S_4/A_4 and A_4/V_4 have prime orders 2, 3 and so are cyclic and hence abelian. Thus $S_4'' \leq V$. Having order 4, V must be abelian so $S_4''' = 1$; (39) $n \leq 4$ only; (40) 5040 ($= 7!$) since a, b must generate S_7 .

Answers to the Exercises Chap 1

Exercise 1:

- (i) Eisenstein with $p = 3$ (Note: $p = 2$ doesn't work).
(ii) mod 2 it is $x^4 + x + 1$ which is prime over \mathbf{Z}_2 .
(iii) If $f(x) = x^4 + x^2 - 1$ then $f(0) = -1$, $f(\pm 1) = 1$, $f(\pm 2) = 19$, $f(\pm 3) = 89$, $f(\pm 4) = 271$.
(iv) Mod 2 the polynomial becomes $x^6 + x^5 + x^4 + x^3 + 1$ which factorizes into primes as $(x^2 + x + 1)(x^4 + x + 1)$. Mod 3 it is $x^6 + x^5 + 2x^4 + 2x^3 + x^2 + x + 2$ which factorizes into primes as $(x^3 + x^2 + 2)(x^3 + 2x + 1)$. Thus no factorization over \mathbf{Z} can give rise to consistent prime factorizations over both \mathbf{Z}_2 and \mathbf{Z}_3 .

Exercise 2:

- (i) **PRIME** A linear polynomial over any field is prime.
(ii) **COMPOSITE** It is $(x + 1)(x + 3)$
(iii) **PRIME** The discriminant is -8 and so the polynomial has no real zeros. Being a quadratic it must be prime over \mathbf{R} .
(iv) **COMPOSITE** The only prime polynomials over \mathbf{R} are the linear ones and the prime quadratics. This one is $(x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$.
(v) **COMPOSITE** $x - 1$ is a factor.

(vi) **PRIME** The zeros of $x^3 + 4$ over \mathbf{Q} are $-4^{1/3}$, $-4^{1/3}\omega$, $-4^{1/3}\omega^2$. None of these is rational and so the polynomial, being a cubic, must be prime.

(vii) **COMPOSITE** It is $(x^2 + 1)(x^3 - x + 1)$.

(viii) **COMPOSITE** $x = 1$ is a zero.

(ix) **PRIME** $x^4 + 1$ has no zeros so if composite it would have to be the product of two prime quadratics (including the case of a prime quadratic squared). These prime quadratics over \mathbf{Z}_3 are $x^2 + 1$, $x^2 + x + 2$ and $x^2 + 2x + 2$. No product of two of these is equal to $x^4 + 1$.

(x) **PRIME** By Eisenstein for $p = 5$.

(xi) **PRIME** Mod 2 it becomes $x^4 + x + 1$ which is prime over \mathbf{Z}_2 . Note that Eisenstein fails.

(xii) **PRIME** Putting $x = y + 1$ the polynomial becomes $(y + 1)^4 + (y + 1)^3 + (y + 1)^2 + (y + 1) = y^4 + 5y^3 + 10y^2 + 10y + 5$ which is prime over \mathbf{Q} by Eisenstein for $p = 5$. Hence the given polynomial must be prime over \mathbf{Q} .

Exercise 3: The monic quartics with non-zero constant terms are:

10001, 10002, 10011, 10012, 10021, 10022, 10101, 10102, 10111, 10112, 10121, 10122,
 10201, 10202, 10211, 10212, 10221, 10222, 11001, 11002, 11011, 11012, 11021, 11022,
 11101, 11102, 11111, 11112, 11121, 11122, 11201, 11202, 11211, 11212, 11221, 11222,
 12001, 12002, 12011, 12012, 12021, 12022, 12101, 12102, 12111, 12112, 12121, 12122,
 12201, 12202, 12211, 12212, 12221, 12222.

Eliminating those with $x = \pm 1$ as a zero we get:

10001, 10012, 10022, 10102, 10111, 10121, 10201, 10202, 11002, 11012, 11021, 11101,
 11111, 11122, 11221, 11222, 12002, 12011, 12022, 12101, 12112, 12121, 12211, 12212.

These are either prime or the product of two monic prime quadratics. By a similar process we find that the monic prime quadratics are: 101, 112, 122.

Their products (including their squares) are:

	101	112	122
101	10201	11012	12022
112		12211	10001
122			11221

Eliminating these we have the monic prime quartics:

10012, 10022, 10102, 10111, 10121, 10202, 11002, 11021, 11101, 11111, 11122, 11222, 12002, 12011, 12101, 12112, 12121, 12212.

Find all the monic prime quartics over \mathbf{Z}_3 .

(To save writing, represent the quartics by their sequence of coefficients, e.g. 10221 represents $x^5 + 2x^3 + 2x + 1$. List your polynomials, in this compact way and in some lexicographic order, and then provide details of your working.)

Exercise 4: Over \mathbf{C} it is clearly $x - (\pi + i)$. Let $\alpha = \pi + i$. Then $(\alpha - \pi)^2 + 1 = 0$ so α is a zero of $f(x) = x^2 - 2\pi x + (1 + \pi^2)$. The zeros of $f(x)$ are $\pi \pm i$ so $f(x)$ has no real zeros and, being quadratic, it is prime over \mathbf{R} .

Exercise 5:

(i)	$x^4 + 2x^3 + 5x^2 + 4x + 1$
(ii)	$x^4 + x^3 + x^2 + x + 1$
(iii)	$x^2 - 6x + 7$
(iv)	$x^4 - 10x^2 + 5$
(v)	$x^6 - 9x^4 - 4x^3 + 27x^2 - 36x - 23$

(i) Let $\alpha = i + \omega$. Then $1 + (\alpha - i) + (\alpha - i)^2 = 0$ and so $i(2\alpha + 1) = \alpha^2 + \alpha$. Squaring we get:

$(2\alpha + 1)^2 + (\alpha^2 + \alpha)^2 = 0$, so α is a zero of $f(x) = x^4 + 2x^3 + 5x^2 + 4x + 1$.

Now $f(0) = f(-1) = 1$, $f(1) = f(-2) = 13$, $f(2) = f(-3) = 61$, $f(3) = f(-4) = 193$ and $f(5) = f(-6) = 1021$ giving 10 values for which $f(x)$ is ± 1 or prime. Hence $f(x)$ is prime over \mathbf{Q} and so is the minimum polynomial of $i + \omega$ over \mathbf{Q} .

(ii) Let $\alpha = e^{2\pi i/5}$. Then $\alpha^5 - 1 = 0$. However this factorizes as $(\alpha - 1)(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1) = 0$ and since $\alpha \neq 1$, α is a zero of $f(x) = x^4 + x^3 + x^2 + x + 1$.

By Exercise 3 this is prime over \mathbf{Z}_3 , and hence over \mathbf{Q} and so it is the minimum polynomial of α over \mathbf{Q} .

(iii) Let $\alpha = \sqrt{11 + 6\sqrt{2}}$. Then $\alpha^2 = 11 + 6\sqrt{2}$ and hence $(\alpha^2 - 11)^2 = 72$. Thus α is a zero of $f(x) = x^4 - 22x^2 + 49$. But $f(x)$ factorizes as $(x^2 - 6x + 7)(x^2 + 6x + 7)$ and in fact α is a zero of $x^2 - 6x + 7$. This certainly prime over \mathbf{Q} since its roots, $3 \pm \sqrt{2}$, are not rational. Hence the minimum polynomial is $x^2 - 6x + 7$.

Note: if we had observed at the outset that $\sqrt{11 + 6\sqrt{2}}$ is simply $3 + \sqrt{2}$ we would have reached this much more quickly!

(iv) Let $c = \cos(\pi/5)$ and $s = \sin(\pi/5)$. Then $(c + is)^5 = 1$. Expanding, and equating the imaginary parts we get: $5c^4s - 10c^2s^3 + s^5 = 0$. Clearly $s \neq 0$ and so $5c^4 - 10c^2s^2 + s^4 = 0$. Hence $\tan(\pi/5) = s/c$ is a zero of $f(x) = x^4 - 10x^2 + 5$. This is prime over \mathbf{Q} by Eisenstein's Theorem with $p = 5$ and so is the required minimum polynomial.

(v) Let $\alpha = \sqrt[3]{2} + \sqrt{3}$. Then $\alpha - \sqrt{3} = \sqrt[3]{2}$ and so $(\alpha - \sqrt{3})^3 = 2$ and so $\alpha^3 - 3\sqrt{3}\alpha^2 + 9\alpha - 3\sqrt{3} = 2$. This isn't yet a polynomial with rational coefficients. But we can write this equation as $\alpha^3 + 9\alpha - 2 = 3\sqrt{3}(1 + \alpha^2)$.

Squaring both sides gives $(\alpha^3 + 9\alpha - 2)^2 = 27(1 + \alpha^2)^2$ and so simplifying we get:

$$\alpha^6 - 9\alpha^4 - 4\alpha^3 + 27\alpha^2 - 36\alpha - 23 = 0.$$

So α is a zero of $x^6 - 9x^4 - 4x^3 + 27x^2 - 36x - 23$.

Now our usual methods don't seem very promising. Once we introduce field extensions in the next chapter we will have a very simple way of establishing the primeness over \mathbf{Q} of this polynomial.