

Instructions. Answer each of the questions on your own paper and be sure to show your work so that partial credit can be adequately assessed. Put your name on each page of your paper.

1. [24 Points] Suppose that Q is the group defined by the following multiplication table. We are denoting the identity of Q by the symbol 1, and we have also outlined the rows and columns beginning with the element a , to facilitate the reading of the multiplication by a . This may be useful in some of the questions that follow.

\cdot	1	a	b	c	d	e	f	g
1	1	a	b	c	d	e	f	g
a	a	1	c	b	e	d	g	f
b	b	c	a	1	f	g	e	d
c	c	b	1	a	g	f	d	e
d	d	e	g	f	a	1	b	c
e	e	d	f	g	1	a	c	b
f	f	g	d	e	c	b	a	1
g	g	f	e	d	b	c	1	a

- (a) Verify that $H = \{1, a\}$ is a subgroup of Q .

► **Solution.** From the multiplication table, $1 \cdot 1 = 1$, $1 \cdot a = a \cdot 1 = a$, and $a^2 = 1$. Thus, H is closed under the group multiplication of Q , and since H is finite, it follows that H is a subgroup of Q . ◀

- (b) List all of the *distinct* left cosets of H in Q .

► **Solution.** $1H = \{1, a\}$, $bH = \{b, c\}$, $dH = \{d, e\}$, and $fH = \{f, g\}$. ◀

- (c) Is H a normal subgroup of Q ? *Hint: Observe from the multiplication table that $ax = xa$ for all $x \in Q$.*

► **Solution.** H is normal in Q provided $ghg^{-1} \in H$ for all $g \in Q$ and $h \in H$. Since $g1g^{-1} = 1 \in H$ and since $ga = ag$ for all $g \in Q$ (by comparing the entries in the second row (ag) and second column (ga)), we have $gag^{-1} = a$ for all $g \in Q$. Since $H = \{1, a\}$ we have shown that $ghg^{-1} = h \in H$ for all $h \in H$ and $g \in Q$. Hence H is normal in Q . ◀

- (d) Write the multiplication table for the factor group Q/H .

► **Solution.** The multiplication rule for cosets of a normal group N in a group G is $(aN)(bN) = (ab)N$, i.e., multiply the corresponding representatives. Thus, using the multiplication table for Q we have:

\cdot	H	bH	dH	fH
H	H	bH	dH	fH
bH	bH	H	fH	dH
dH	dH	fH	H	bH
fH	fH	dH	bH	H

(e) Is Q/H a cyclic group? Explain. ◀

► **Solution.** Q/H is not cyclic, since $|Q/H| = 4$ but every nonidentity element has order 2, as seen from the multiplication table above. ◀

2. [12 Points] For each of the following statements, fill in the appropriate hypotheses or conclusions to ensure that the statement is a theorem proved in class.

(a) If F is a field, the space of congruence classes $F[x]/\langle p(x) \rangle$ is a field if and only if $p(x)$ is an irreducible polynomial over F .

(b) A polynomial $p(x)$ of degree 2 or 3 is irreducible over the field F if and only if $p(x)$ has no roots in F .

(c) (**Remainder Theorem**). Let $f(x) \in F[x]$ be a nonzero polynomial, and let $c \in F$. Then there exists a polynomial $q(x) \in F[x]$ such that

$$f(x) = q(x)(x - c) + \boxed{f(c)}.$$

3. [20 Points] Let $f(x) = x^2 - 1$ and let $g(x) = x^3 + 1$ be polynomials in $\mathbb{Q}[x]$.

(a) Use Euclid's Algorithm to find $d(x) = \gcd(f(x), g(x))$.

► **Solution.** $x^3 + 1 = x(x^2 - 1) + (x + 1)$ and $x^2 - 1 = (x + 1)(x - 1)$ so $d(x) = \gcd(x^2 - 1, x + 1) = x + 1$. ◀

(b) Express $d(x)$ in the form $d(x) = a(x)f(x) + b(x)g(x)$. From the previous calculation,

$$x + 1 = (x^3 + 1) + (-x)(x^2 - 1).$$

4. [20 Points] Determine whether each of the following polynomials is irreducible over the given field. Justify your answers. If the polynomial is reducible, find a factorization into irreducible polynomials.

(a) $x^3 + x^2 + 2x + 2$ over \mathbb{Z}_3 .

► **Solution.** Since $1^3 + 1^2 + 2 + 2 = 6 \equiv 0 \pmod{3}$, it follows that 1 is a root of this polynomial. Long division gives

$$x^3 + x^2 + 2x + 2 = (x - 1)(x^2 + 2x + 1) = (x - 1)(x + 1)^2$$

for the complete factorization in $\mathbb{Z}_3[x]$. ◀

(b) $3x^5 + 4x^3 + 6$ over \mathbb{Q} .

► **Solution.** Apply Eisenstein's criterion with $p = 2$: $2|4$, $2|6$, $2 \nmid 3$, $4 \nmid 6$. Hence, this polynomial is irreducible over \mathbb{Q} . ◀

5. [24 Points] Let $E = \mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle$.

(a) List all of the distinct elements of E .

► **Solution.** Since $\deg(x^3 + x + 1) = 3$, the elements of E are uniquely represented by $[ax^2 + bx + c]$ where $a, b, c \in \mathbb{Z}_2$. Hence,

$$E = \{[0], [1], [x], [x + 1], [x^2], [x^2 + 1], [x^2 + x], [x^2 + x + 1]\}.$$

◀

(b) Calculate the product $[x^2 + 1][x^2 + x + 1]$ and identify this element on the list produced in part (a).

► **Solution.** In E there are the identities $[x^3 + x + 1] = [0]$ and $[x^3] = [-x - 1] = [x + 1]$ (recall that $-1 = 1$ in \mathbb{Z}_2). Hence

$$\begin{aligned} [x^2 + 1][x^2 + x + 1] &= [x^4 + x^3 + x^2 + x + 1] \\ &= [x^4 + x^3 + x + 1] \\ &= [x^4] = [x(x^3)] \\ &= [x(x + 1)] = [x^2 + x]. \end{aligned}$$

◀

(c) Find the multiplicative inverse of $[x + 1]$.

► **Solution.** Dividing $x + 1$ into $x^3 + x + 1$ gives $x^3 + x + 1 = (x + 1)(x^2 + x) + 1$ so that $1 = (x + 1)(x^2 + x) + (x^3 + x + 1)$. Hence, in E ,

$$[x + 1]^{-1} = [x^2 + x].$$

◀