# SOLUTIONS TO PRACTICE FINAL

**1.** Let $\alpha \in \mathbb{C}$ be a complex number satisfying the equation $\alpha^3 - 3\alpha + 1 = 0$. Compute $[\mathbb{Q}(\sqrt{-5}, \alpha) : \mathbb{Q}]$.

By the rational root criterion, the only possible roots of $Q(X) := X^3 - 3X + 1$ in $\mathbb{Q}$ are $\pm 1$ which one checks are not actually roots. As $Q$ is cubic, if it were reducible it would have a linear factor. As it has no roots, it is irreducible. Hence, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. The square root of negative five satisfies the polynomial $R(X) = X^2 + 5 \in \mathbb{Q}(\alpha)[X]$. Hence, $[\mathbb{Q}(\alpha, \sqrt{-5}) : \mathbb{Q}(\alpha)] = 1$ or 2. If this degree were one, then $\mathbb{Q}(\sqrt{-5}) \subseteq \mathbb{Q}(\alpha)$ so that $3 = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{-5})][\mathbb{Q}(\sqrt{-5}) : \mathbb{Q}]$. But we know that $X^2 + 5$ is irreducible over $\mathbb{Q}$ so that $[\mathbb{Q}(\sqrt{-5}) : \mathbb{Q}] = 2$, which does not divide 3. Hence, $[\mathbb{Q}(\alpha, \sqrt{-5}) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \sqrt{-5}) : \mathbb{Q}(\sqrt{-5})][\mathbb{Q}(\sqrt{-5}) : \mathbb{Q}] = 3 \times 2 = \mathbf{6}$.

**2.** Prove or disprove: If $K$ is an extension field of $\mathbb{Q}$ and $[K : \mathbb{Q}] < \infty$, then there is an irreducible polynomial $P(X) \in K[X]$.

**Easy solution:** I meant to include the condition that $\deg(P) > 1$. Clearly, $P(X) = X \in K[X]$ is irreducible. The rest of the solution deals with the intended question.

**Proof**: Let $p > [K : \mathbb{Q}]$ be any prime number greater than the degree of the field extension. Let $Q(X) := X^p - 2$. By the Eisenstein criterion, $Q$ is irreducible over $\mathbb{Q}$. Let $R$ be an irreducible factor of $Q$ over $K$ and set $L := K[X]/(R)$. Let $\alpha \in L$ be the image of $X$. As $Q(\alpha) = 0$, we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$. Thus, $[L : K]d = [L : K][K : \mathbb{Q}] = [L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)]p$. Hence, $p$ divides $[L : K]$ which being no more than $p$ as $\deg(R) \leq p$ must be equal to $p$. That is, $Q$ is irreducible over $K$.

**3.** Let $g(X) = X^4 - X^2 + X + 1 \in \mathbb{Z}_3[X]$. Write $g$ as a product of irreducible polynomials.

Observe that $g(2) = 16 - 4 + 2 + 1 = 0 \in \mathbb{Z}_3$ Hence, $x - 2 = x + 1$ divides $g$. Using long division, one computes $g(x) = (x + 1)(x^3 - x^2 + 1)$. Substituting 0, 1, and 2 for $x$ in the cubic factor, we find that it has no roots in $\mathbb{Z}_3$. As $\mathbb{Z}_3$ is a field, we know that a cubic polynomial with no roots is irreducible. Hence, we have expressed $g$ as a product of irreducible polynomials.

**4.** Write $\frac{5 - \sqrt[3]{49}}{1 + \sqrt[3]{7}}$ in the form $a + b\sqrt[3]{7} + c\sqrt[3]{49}$ for rational numbers $a$, $b$, and $c$.

$\frac{3}{2} - \frac{3}{2}\sqrt[3]{7} + \frac{1}{2}\sqrt[3]{49}$

**5.** Show that if $\phi : R \to S$ is a homomorphism of commutative rings and $a \in S$ is any element, then there is a unique homomorphism $\widetilde{\phi} : R[X] \to S$ for which $\widetilde{\phi}(X) = a$ and $\widetilde{\phi}(r) = \phi(r)$ for all $r \in R$.

We prove uniqueness first. The map $\widetilde{\phi}$ is a homomorphism. Hence, if $f = \sum b_i X^i \in R[X]$, we must have $\widetilde{\phi}(f) = \widetilde{\phi}(\sum b_i X^i) =^{\text{preservation of addition}} \sum \widetilde{\phi}(b_i X^i) =^{\text{preservation of multiplication}} \sum \widetilde{\phi}(b_i)\widetilde{\phi}(X)^i =^{\text{hypotheses on } \widetilde{\phi}} \sum \phi(b_i) a^i$. Now, we check that this formula correctly defines a homomorphism. Let $f = \sum b_i X^i$ and $g = \sum c_j X^j$. Then

$$\begin{aligned}
\widetilde{\phi}(f+g) &= \widetilde{\phi}(\sum(b_i+c_i)X^i) \\
&= \sum \phi(b_i+c_i)a^i \\
&= \sum(\phi(b_i)+\phi(c_i))a^i \\
&= \sum(\phi(b_i)a^i+\phi(c_i)a^i) \\
&= \sum \phi(b_i)a^i + \sum \phi(c_i)a^i \\
&= \widetilde{\phi}(f)+\widetilde{\phi}(g)
\end{aligned}$$

$$\begin{aligned}
\widetilde{\phi}(fg) &= \widetilde{\phi}(\sum_k(\sum_{i+j=k} b_ic_j)X^k) \\
&= \sum_k \phi(\sum_{i+j=k} b_ic_j)a^k \\
&= \sum_k(\sum_{i+j=k} \phi(b_ic_j))a^k \\
&= \sum_k(\sum_{i+j=k} \phi(b_i)\phi(c_j))a^k \\
&= \sum_i\sum_k \phi(b_i)\phi(c_j)a^{i+j} \\
&= (\sum b_ia^i)(\sum c_ja^j) \\
&= \widetilde{\phi}(f)\widetilde{\phi}(g)
\end{aligned}$$

Of course, $\widetilde{\phi}(1)=1$.

**6.** Express the quotient group $(\mathbb{Z}_{60}\times\mathbb{Z}_{24}\times\mathbb{Z}_{40})/\langle(5,16,25)\rangle$ as a direct sum of cyclic groups.

$\mathbb{Z}_4\times\mathbb{Z}_8\times\mathbb{Z}_3\times\mathbb{Z}_5\times\mathbb{Z}_5$

[How did I find this? Write $\mathbb{Z}_{60}\times\mathbb{Z}_{24}\times\mathbb{Z}_{40}$ as $\mathbb{Z}_4\times\mathbb{Z}_3\times\mathbb{Z}_5\times\mathbb{Z}_8\times\mathbb{Z}_3\times\mathbb{Z}_8\times\mathbb{Z}_5$ and the group by which we are factoring as $\langle(1,2,0,0,1,1,0)\rangle$. One easily computes that the least common multiple of the orders of the components is twenty four. Hence, the factor group may be expressed as a product of abelian groups of order thirty-two, three, and twenty-five. One checks that the images of $(0,0,0,1,0,0,0)$ and $(0,0,0,0,0,1,0)$ have orders eight and four, respectively, and are independent while the images of $(0,0,1,0,0,0,0)$ and $(0,0,0,0,0,0,1)$ have order five and are independent.]

**7.** There is no question seven.

**8.** Compute $13^{5,389}$ in $\mathbb{Z}_{305}$.

As $305=5\times 61$, we see that $\mathbb{Z}_{305}^\times\cong\mathbb{Z}_5^\times\times\mathbb{Z}_{61}^\times\cong\mathbb{Z}_4\times\mathbb{Z}_{60}$. Hence, $13^{60}=1$. Computing the powers of 13, we find that $13^{12}=1$. Dividing, we see that $5389\equiv 1 \pmod{12}$. Hence, $13^{5,389}=13$ in $\mathbb{Z}_{305}$.

**9.** Prove or disprove: If $\phi: R\to S$ is a homomorphism of rings and $\mathfrak{p}\subsetneq S$ is a prime ideal, then $\phi^{-1}\mathfrak{p}:=\{x\in R:\phi(x)\in\mathfrak{p}\}$ is a prime ideal.

**Proof:** As $\mathfrak{p}$ is prime, the factor ring $S/\mathfrak{p}$ is an integral domain. Let $\pi : S \to S/\mathfrak{p}$ be the quotient map. Then the composite $\pi \circ \phi : R \to S/\mathfrak{p}$ is a homomorphism and $\phi^{-1}\mathfrak{p} = \ker(\pi \circ \phi)$ is the kernel of a homomorphism to an integral domain and therefore must be a prime ideal.

**10.** Find (with proof) all automorphisms of $\mathbb{Z}$.

There are two automorphisms of $(\mathbb{Z}, +)$: The identity map and the map $x \mapsto -x$.

To prove this we note that if $G$ is any group and $\alpha$ and $\beta$ are two homomorphisms from $\mathbb{Z}$ to $G$ for which $\alpha(1) = \beta(1)$, then $\alpha = \beta$. We prove by induction on $n \geq 0$ that $\alpha(n) = \beta(n)$. The case of $n = 0$ is automatic as both map to the identity element of $G$. For $n+1$ we have $\alpha(n+1) = \alpha(n)\alpha(1) =^{\text{by IH and the original hypothesis}}$ $\beta(n)\beta(1) = \beta(n+1)$. Thus for $n \geq 0$ we have $\alpha(n) = \beta(n)$ but of course $\alpha(-n) = \alpha(n)^{-1} = \beta(n)^{-1} = \beta(-n)$.

Thus, an automorphism $\alpha : \mathbb{Z} \to \mathbb{Z}$ is determined by $\alpha(1) =: N$. As $\alpha(n) = n\alpha(1) = nN$ for every $n \in \mathbb{Z}$ we see that the image of $\alpha$ is contained in the ideal $N\mathbb{Z}$ which is all of $\mathbb{Z}$ only in case $N$ is a unit, 1 or $-1$.

The identity map is clearly an automorphism. The map $x \mapsto -x$ is its own compositional inverse and it satisfies $-(x+y) = -x + -y$.

[The question as stated is ambiguous, if we asked about ring automorphisms, then only the identity map would be an automorphism, as any ring automorphism would also be a group automorphism and the map $x \mapsto -x$ is not a ring automorphism since $-1 \neq (-1)(-1)$.]

**11.** Prove or disprove: every group of order twelve has a subgroup of order six.

**Disproof:** The group $A_4$ has order twelve but no subgroup of order six. Let $G < A_4$ be a purported subgroup of order six. Considering cycles, we see that the elements of $S_4$ can have order 1, 2, 3 and 4. Hence, $G \ncong \mathbb{Z}_6$. Thus, $G \cong S_3$ and has two elements of order three and three elements of order two. At the cost of permuting the set $\{1, 2, 3, 4\}$, we may assume that $G$ contains the cycle $(1, 2, 3)$, and thus also $(1, 3, 2)$. The elements of $A_4$ of order two have the form $(a, b)(c, d)$ where $(a, b)$ and $(c, d)$ are *disjoint* transpositions and $\{a, b, c, d\} = \{1, 2, 3, 4\}$. $G$ must contain some element of order two. Hence, there is an element of the form $(a, 4)(c, d)$ with $\{a, c, d\} = \{1, 2, 3\}$. But then $(1, 2, 3)(a, 4)(c, d)$ is a three-cycle with 4 in its orbit. This product belongs to $G$ but is not $(1, 2, 3)$ or $(1, 3, 2)$ contrary to the above considerations. Hence, $G$ does not exist.

**12.** Prove or disprove: If $G$ is a nonempty set with a binary operations $*$ which satisfies left and right cancelation for all $a$ and $b$ in $G$ there is some $x \in G$ with $a * x = b$ and some $y$ with $y * a = b$, then $(G, *)$ is a group.

**Disproof:** Consider the following multiplication table.

| * | a | b | c |
|---|---|---|---|
| a | a | b | c |
| b | c | a | b |
| c | b | c | a |

In each row and in each column each element appears exactly once so that cancelation holds, but $(b * c) * a = b * a = c \neq a = b * b = b * (c * a)$ so that associativity fails meaning that $(G, *)$ is not a group.

**13.** How many elements of the group $\mathbb{Z}_{12} \times \mathbb{Z}_{16} \times S_5$ have order four?

792 [We compute the number of elements of order dividing four and then subtract the number of elements of order dividing two. There are four elements of $\mathbb{Z}_{12}$ of order dividing four: $0, 3, 6, 9$; four in $\mathbb{Z}_{16}$: $0, 4, 8, 12$; and seventy-six in $S_5$: count the four cycles (30), transpositions (10), products of two disjoint transpositions (15), and the identity (1). Hence, in the product group there are $4 \times 4 \times 56 = 896$ elements of order dividing 4. Similarly, there are $2 \times 2 \times 26 = 104$ elements of order dividing 2. Thus, there are $896 - 104 = 792$ elements of order exactly four.]

In **14.** Prove or disprove: If $R = \mathcal{C}([0,1])$ is the ring of continuous real-valued

functions on the closed interval $[0,1] := \{x \in \mathbb{R} : 0 \le x \le 1\}$, then $I := \{f \in R : f(\frac{1}{2}) = 0\}$ is a maximal ideal.

**Proof:** The map $R \to \mathbb{R}$ given by $f \mapsto f(\frac{1}{2})$ is a homomorphism onto a field. Hence, its kernel, $I$, is a maximal ideal.

**15**. How many subgroups of $S_5$ have exactly three elements?

Ten.

**16**. Let $G$ be the set of functions from $\mathbb{R}$ to $\mathbb{R}$ of the form $x \mapsto ax + b$ for some real numbers $a$ and $b$ with $a \neq 0$. Prove or disprove: $G$ is a group under the binary operation of composition.

**Proof:** Let $(ax+b) \circ (cx+d) = acx + (ad+b)$ and if $a$ and $c$ are nonzero, then so is $ac$. Thus, $G$ is closed under the operation of composition. The identity function is $(1)x + 0$ and $(ax+b)^{-1} = (1/a)x + (-b/a)$ while composition of functions is always commutative.

**17**. Write the following permutation as a product of disjoint cycles.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 8 & 2 & 6 & 9 & 7 & 1 & 3 & 4 \end{pmatrix}$$

$(1, 5, 9, 4, 6, 7)(2, 8, 3)$

**18**. Prove or disprove: If $G$ is a group and $H < G$ is a subgroup with $\#(G/H) = 3$, then $H \lhd G$.

**Disproof:** Consider $G = S_3$ and $H = \{\iota, (1,2)\}$. Then $\#(G/H) = 3$ by $H \ntriangleleft G$ as $(1,2,3)H = \{(1,2,3), (1,3,2)\} \neq \{(1,2,3), (2,3)\} = H(1,2,3)$.

**19**. Prove or disprove: If $K$ is a field and $f$ and $g$ are polynomials over $K$ and $K[X]/(f) \cong K[X]/(g)$, then $(f) = (g)$.

**Disproof:** Consider $K = \mathbb{R}$ and $f(X) = X^2 + 1$ and $g(X) = X^2 + 2$. Each of the fields $K[X]/(f)$ and $K[X]/(g)$ is isomorphic to $\mathbb{C}$ bu $X^2 + 1$ is not a multiple of $X^2 + 2$ for if it were, $i\sqrt{2}$ would be a zero of $X^2 + 1$.

**20**. Prove or disprove: There is a nontrivial homomorphism $\phi : \mathbb{Z}_4 \to S_3$

**Proof:** Recall that for any group $G$ and element $g \in G$, the function $\alpha : \mathbb{Z} \to G$ defined by $n \mapsto g^n$ is a homomorphism. Consider the case of $G = S_3$ and $a = (1,2)$. Then the kernel of $\alpha$ is $2\mathbb{Z} \supseteq 4\mathbb{Z}$. Hence, there is a homomorphism $\bar{\alpha} : \mathbb{Z}_4 \to S_3$ given by $n \mapsto (1,2)^n$. As $\bar{\alpha}(1) = (1,2) \neq \iota$, $\bar{\alpha}$ is nontrivial.

**21**. Let $p$ be a prime number. Suppose that $G := \mathbb{Z}_p$ acts on the set $X$. Let $Y := \{x \in X : (\forall g \in \mathbb{Z}_p) g \cdot x = x\}$. Show that $\#Y \equiv \#X \pmod{p}$.

We may express $X$ as a disjoint union of orbits. Each orbit has the form $Gx$ for some $x \in X$ and as such $Gx \cong G/G_x$ as a $G$-set. As $\#G = p$ is prime, if $x$ is not fixed by $G$, then $Gx$ has $p$ elements. Hence, $X$ may be expressed as a disjoint union of $Y$ and a disjoint union of sets each of size $p$. Therefore, the number of elements of $X$ is the same as that of $Y$ modulo $p$.

**22**. Let $K$ be a field and $g(x) \in K[x] \smallsetminus K$ a nonconstant polynomial over $K$ of degree $d$. Prove that there are at most $d$ elements $a$ of $K$ satisfying $g(a) = 0$.

**Prood:** By induction on $d$. If $d = 1$, then $g(x) = cx + d$ for some $c \in K^\times$ and $d \in K$. If $g(a) = 0$, then $ca + d = 0$ so that $a = \frac{-d}{c}$. Thus, there is only one zero. More generally, if $a$ is a zero of $g$, then let $q$ and $r$ be polynomials with $g(x) = q(x)(x - a) + r$ and $\deg(r) < 1$. As $0 = g(a) = q(a)(a - a) + r = r$, we must have $g = q(x)(x - a)$. As $\deg(q) < \deg(g)$, by induction $q$ has at most $\deg(g) - 1$ zeros. As $K$ is an integral domain, if $g(b) = 0$, then either $q(b) = 0$ or $b = a$. Thus, there are no more than $\deg(g)$ zeros to $g$.

**23**. Let $g(x) := x^3 + x + 1 \in \mathbb{Z}_2$. Let $K := \mathbb{Z}_2[x]/(g)$. Prove that $K$ is a field. Let $\alpha \in K$ be a solution to $\alpha^3 + \alpha + 1 = 0$. Write the polynomial $x^3 + \alpha + 1$ as a product of irreducible polynomials over $K$.

$(x + \alpha)(x^2 + \alpha x + \alpha^2)$

**24**. Prove or disprove: If $\phi : R \to S$ is a homomorphism of rings, $a \in R$ and $\phi(a) \in S^\times$, then $a \in R^\times$.

**Disproof:** Consider $R = \mathbb{Z}$, $S = \mathbb{Q}$, $\phi$ the natural inclusion and $a = 2$.

**25**. How many elements of the factor group $\mathbb{Q}/\mathbb{Z}$ have order *dividing* $5,239,290$?

$5,239,290$ [Why? $q + \mathbb{Z}$ has order dividing $5,239,290$ if and only if $5,239,290q$ is an integer if and only if $q = a/5,239,290$ for some integer $a$. Every element of $\mathbb{Q}/\mathbb{Z}$ may be expressed uniquely in the form $q + \mathbb{Z}$ for some rational number $q$ with $0 \leq q < 1$ . Thus, we may take for $a$ any integer with $0 \leq a < 5,239,290$ and there are $5,239,290$ such.]