COMPS

Name: Quin Darcy
Instructor: NONE

Due Date: NONE
Assignment: PRACTICE

AL.1.2 Let G be a finite group.

(a) If $[G : Z(G)] = n$ where n is positive, show that every conjugacy class has at most n elements.

Proof. Our premise implies that

$$G/Z(G) = \{Z(G), g_1Z(G), \ldots, g_{n-1}Z(G)\},$$

where $g_i \notin Z(G)$ for all $1 \leq i \leq n-1$. Now let $x \in G$. Then if $x \in Z(G)$, it follows that x commutes with every $g \in G$. Thus

$$c(x) = \{gxg^{-1} : g \in G\} = \{gg^{-1}x : g \in G\} = \{x\}.$$

Assume $x \notin Z(G)$. Let $y \in c(x)$ such that $y \neq x$ and $y \in Z(G)$. Then since $y \in c(x)$, there is some $g \in G$ such that $y = gxg^{-1}$. Then $g^{-1}yg = g^{-1}gy = y = x$, a contradiction. Thus, if $x \notin Z(G)$, then for all $y \in c(x)$, $y \notin Z(G)$. Hence $y = g_i$ for some $1 \leq i \leq n-1$. Therefore $|c(x)| \leq n$. □

(b) Suppose the size of each conjugacy class in G is at most 2. Show that for all $g \in G$, the centralizer $C_G(g)$ is a normal subgroup of G.

Proof. Let $g \in G$. Then by assumption $c(g) = \{g\}$ or $c(g) = \{g, x\}$, where $x \neq g$. If the only conjugate of g is itself, then $C_G(g) = G$ and $G \trianglelefteq G$ trivially. Assume that $c(g) = \{g, x\}$. Then for any $h \in G$, $hgh^{-1} = g$ or $hgh^{-1} = x$. This implies that

$$G/C_G(g) = \{C_G(g), G \backslash C_G(g)\}.$$

Hence $[G : C_G(g)] = 2$ and therefore $C_G(g) \trianglelefteq G$. □

AN.1.1

(a) Prove that the set of isolated points of a subset $S \subseteq \mathbb{R}^k$ is countable.

Proof. Let $A \subseteq S$ be the set of all isolated points of S. For any $x \in A$, there exists some $r_x \in \mathbb{R}^+$ such that $N_{r_x}(x) \cap S = \{x\}$. With this define the following set

$$R = \{r_x : x \in A\}.$$

This set is bounded below by 0 and thus its infimum exists. Let $r = \inf R/2$. The set $T = \{N_r(x) : x \in A\}$ is a set of disjoint open sets and is therefore countable

(since from each open set, we can select a unique rational k-tuple and from this create an injective map into $\mathbb{Q}^k$ which is countable.) Finally, if $f : A \to T$ is a map defined by $x \mapsto N_r(x)$, then since each neighborhood is dijoint, it follows that f is injective. Moreover, for each neighborhood there is an isolated point which maps to it. The map f is therefore a bijection. Thus $A \sim T$ and so A is countable. □

(b) Prove that the set of all binary sequences is uncountable.

Proof. Let S be the set of all binary sequences and let $A \subseteq S$ be any countable subset of S. Suppose the elements of A are the sequences $s_1, s_2, \ldots$. Define a new sequence s in the following way: If the first digit of s_1 is a 1, then let the first digit of s be 0, whereas if the first digit is 0, then let the first digit of s be 1. Generally, if the nth digit of s_n is 1, the let the nth digit of s be 0 and if the nth digit is 0, let the nth digit of s be 1. In this way, s differs from each sequence in A by at least one digit and so $s \notin A$. However, as s is still a binary sequence, then $s \in S$. This means that A is a proper subset of S. Hence, every countable subset of S is a proper subset of S. Therefore S is uncountable. □

AL.1.4

(a) If G is a cyclic group, prove that every subgroup of G is also cyclic.

Proof. If G is cyclic, then there is some $g \in G$ such that $G = \langle g \rangle$. Let $H \leq G$ be a subgroup of G. Let k be the smallest nonzero positive integer such that $g^k \in H$. We claim that $H = \langle g^k \rangle$. Let $h \in H$. Then for some $m \in \mathbb{N}$, $h = g^m$. If $k \mid m$, then $m = tk$ for some $t \in \mathbb{N}$ and hence

$$h = g^m = g^{tk} = (g^k)^t \in \langle g^k \rangle.$$

If $k \nmid m$, then by the QR theorem, there exists $q, r \in \mathbb{Z}$ such that $m = qk + r$ and $0 \leq r < k$. Hence

$$h = g^m = g^{qk+r} = g^{qk} g^r \Rightarrow g^{-qk} h = g^r.$$

We have that $g^{-qk}, h \in H$ but g^r cannot be in H as that would contradict that k is the smallest nonzero integer such that $g^k \in H$. Thus $k \mid m$ and $H \subseteq \langle g^k \rangle$.

Let $(g^k)^t \in \langle g^k \rangle$. Then since $g^k \in H$, $(g^k)^t = (g^k) \cdots (g^k) \in H$ by closure. Hence $H = \langle g^k \rangle$ and so H is cyclic. □

(b) Suppose $a \in G$ and $\text{ord}(a) = n$. Given a positive integer m, if $d = \gcd(n, m)$, prove that

$$\text{ord}(a^m) = \text{ord}(a^d).$$

Proof. Let $x = \text{ord}(a^m)$ and $y = \text{ord}(a^d)$. Since $d \mid m$, then $m = kd$ for some $k \in \mathbb{Z}$. Thus

$$(a^m)^y = (a^{kd})^y = ((a^d)^y)^k = e^k = e.$$

Thus $x \mid y$. Since $d = \gcd(n, m)$, then by the Euclidien algorithm, there exists $t_1, t_2 \in \mathbb{Z}$ such that $d = nt_1 + mt_2$. Thus

$$(a^d)^x = (a^{nt_1+mt_2})^x = (a^n)^{xt_1}((a^m)^x)^{t_2} = e^{xt_1}e^x = e.$$

Thus $y \mid x$. Therefore $x = y$. □

AN.4.9 Let $f : \mathbb{R} \to \mathbb{R}$ be defined as follows

$$f(x) = \begin{cases} x^5 \sin\left(\frac{1}{x^3}\right) & \text{if } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases}$$

Study the continuity and differentiability of f on $\mathbb{R}$. How many times is f differentiable?

Proof. Let $x \in \mathbb{R} - \{0\}$. Then $f(x) = x^5 \sin(1/x^3)$. Since x^5, $\sin(x)$, and $1/x^3$ are all differentiable for $x \neq 0$, then f is differentiable as the product and composition of differentiable functions. This further implies that f is continuous. Using the product and chain rule we obtain

$$f'(x) = 5x^4 \sin(\frac{1}{x^3}) - 3x \cos(\frac{1}{x^3})$$

for all $x \in \mathbb{R} - \{0\}$. To see if $f'(0)$ is defined we check

$$\lim_{x\to 0} \frac{f(x+0) - f(0)}{x} = \lim_{x\to 0} \frac{x^5 \sin(\frac{1}{x^3})}{x} = \lim_{x\to 0} x^4 \sin(\frac{1}{x^3}).$$

Since $|\sin(1/x^3)| \leq 1$ for all x, then it follows that $0 \leq |x^4 \sin(1/x^3)| \leq x^4$. Thus by the Squeeze theorem, $f'(0) = 0$. We can now write

$$f'(x) = \begin{cases} 5x^4 \sin\left(\frac{1}{x^3}\right) - 3x \cos\left(\frac{1}{x^3}\right) & \text{if } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases}$$

By the same reasoning above, for all $x \neq 0$, f is differentaible as the product, difference, and composition of differentiable functions. Using the product and chain rules we obtain

$$f''(x) = \left(20x^3 - \frac{9}{x^3}\right) \sin\left(\frac{1}{x^3}\right) - (15x + 3) \cos\left(\frac{1}{x^3}\right)$$

for all $x \neq 0$. Using the same method before, we use the limit definition of the derivative to see if $f'(x)$ is differentiable at $x = 0$.

$$\begin{aligned} f''(0) &= \lim_{x\to 0} \frac{f'(x+0) - f'(0)}{x} \\ &= \lim_{x\to 0} \frac{5x^4 \sin\left(\frac{1}{x^3}\right) - 3x \cos\left(\frac{1}{x^3}\right)}{x} \\ &= \lim_{x\to 0} 5x^3 \sin\left(\frac{1}{x^3}\right) - 3\cos\left(\frac{1}{x^3}\right) \\ &= \lim_{x\to 0} -3\cos\left(\frac{1}{x^3}\right). \end{aligned}$$

Seeing as the limit of $\cos(1/x^3)$ as $x \to 0$ does not exist, then we can conclude that $f''(x)$ is not differentiable at $x = 0$. Hence, f is twice differentiable. □

AL.2.10 Let $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, so ω is a primitive cube root of unity.

(a) Let

$$\begin{aligned}\alpha_1 &= \omega^{1/3} + \omega^{-1/3}\\ \alpha_2 &= \omega^{2/3} + \omega^{-2/3}\\ \alpha_3 &= \omega^{4/3} + \omega^{-4/3}\end{aligned}$$

Show that α_1 is a root of $f(x) = x^3 - 3x + 1$. (After this you may assume that α_2 and α_3 are each roots of $f(x)$.)

Proof. To show that α_1 is a root of $f(x)$, we must show that $f(\alpha_1) = 0$. With this we have

$$\begin{aligned}f(\alpha_1) &= \alpha_1^3 - 3\alpha_1 + 1\\ &= (\omega^{1/3} + \omega^{-1/3})^3 - 3(\omega^{1/3} + \omega^{-1/3}) + 1\\ &= \omega + 3(\omega^{1/3} + \omega^{-1/3}) - 3(\omega^{1/3} + \omega^{-1/3}) + \omega^{-1} + 1\\ &= \omega + \omega^{-1} + 1\\ &= \frac{\omega^2 + \omega + 1}{\omega}\\ &= \frac{0}{\omega} = 0.\end{aligned}$$

□

(b) Show that the splitting field for $f(x)$ over $\mathbb{Q}$ is $E = \mathbb{Q}(\alpha_1)$. (Hint consider $(\alpha_1)^2$).

Proof. Part (a) showed us that $(x-\alpha_1)$ is a factor of $f(x)$. To show that $E = \mathbb{Q}(\alpha_1)$ is the splitting field for $f(x)$ over $\mathbb{Q}$, we must show that E contains all the roots of $f(x)$ and that any proper subfield of E does not contain all the roots of $f(x)$.

Clearly $\alpha_1 = 0 + 1 \cdot \alpha_1 \in \mathbb{Q}(\alpha_1)$. The question now is if we can obtain α_2 and α_3 from the elements in $\mathbb{Q}(\alpha_1)$. Notice that $\alpha_1^2 = \alpha_2 + 2$ and so $\alpha_2 \in \mathbb{Q}(\alpha_1)$. Similarly, $\alpha_2^2 = \alpha_3 + 2$ and so $\alpha_3 \in \mathbb{Q}(\alpha_1)$. This shows that all of the roots of f are in E. We now need to show that it is the smallest field which contains these roots. The smallest field which contains $\alpha_1, \alpha_2, \alpha_3$ and $\mathbb{Q}$ is $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ and so we must show that $E = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$. Since the left-to-right inclusion is clear, we will prove the inclusion $\supseteq$ holds.

Let $x \in \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$. Then

$$x = a + b\alpha_1 + c\alpha_2 + d\alpha_3 + e\alpha_1\alpha_2 + f\alpha_1\alpha_3 + g\alpha_2\alpha_3 + h\alpha_1\alpha_2\alpha_3$$

for some $a, b, c, d, e, f, g, h \in \mathbb{Q}$. Based on the equalities we used before, we have that

$$\alpha_2 = \alpha_1^2 - 2 \qquad \begin{aligned}\alpha_3 &= \alpha_2^2 - 2\\ &= (\alpha_1^2 - 2)^2 - 2\\ &= \alpha_1^4 - 4\alpha_1^2 - 2.\end{aligned}$$

Thus x can be written in terms of only the element α_1 using multiplication, addition, and subtraction. Therefore $x \in \mathbb{Q}(\alpha_1)$. Hence E is the splitting field for $f(x)$. □

(c) Determine, with proof, the degree of $\mathbb{Q}(\omega^{1/3})$ over $\mathbb{Q}(\omega)$.

Proof. We first wish to compute $[\mathbb{Q}(\omega^{1/3}) : \mathbb{Q}]$. Letting $x - \omega^{1/3} = 0$, then manipulating until all radicals are removed, we get that $x^6 + x^3 + 1 = 0$. Seeing that this polynomial is in $\mathbb{Z}[x]$, its degree is greater than 1, then we note that the polynomial is irreducible over $\mathbb{Z}_2[x]$ and that its degree over that field is the same as the degree of the original polynomial. It then follows from the $\mathbb{Z}_p$ test, that this polynomial is irreducible over $\mathbb{Q}$ is is therefore the minimal polynomial of $\omega^{1/3}$ over $\mathbb{Q}$. Therefore $[\mathbb{Q}(\omega^{1/3}) : \mathbb{Q}] = 6$. Next, we consider $[\mathbb{Q}(\omega) : \mathbb{Q}]$.

Doing the same as we did above, we let $x - \omega = 0$ and manipulate until we remove the radicals to obtain $x^2 + x + 1 = 0$. This polynomial is irreducible over $\mathbb{Z}_2$ and is therefore irreducible over $\mathbb{Q}$. Hence, $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$.

Finally, we note that $\omega \in \mathbb{Q}(\omega^{1/3})$ and so $\mathbb{Q}(\omega) \subseteq \mathbb{Q}(\omega^{1/3})$. Thus we have that

$$[\mathbb{Q}(\omega^{1/3}) : \mathbb{Q}] = [\mathbb{Q}(\omega^{1/3}) : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}]$$
$$\Rightarrow [\mathbb{Q}(\omega^{1/3}) : \mathbb{Q}(\omega)] = \frac{[\mathbb{Q}(\omega^{1/3}) : \mathbb{Q}]}{[\mathbb{Q}(\omega) : \mathbb{Q}]} = \frac{6}{2} = 3$$

□

AN.1.14

(a) Suppose $\{f_n\}$ is a sequence of continuous real-valued functions on a metric space X and $f_n \to f$ uniformly. Let $\{x_n\}$ be a sequence of points in X converging to $x \in X$. Prove that $\lim_{n\to\infty} f_n(x_n) = f(x)$.

Proof. Let $\varepsilon > 0$. Since $\{f_n\}$ converges uniformly on X, then there exists N_1 such that for any $n > N_1$ we have

$$|f_n(y) - f(y)| < \frac{\varepsilon}{2}$$

for all $y \in X$. It also follows from the uniform convergence (and that each f_n is continuous) that f is continuous on X. Specifically, f is continuous at x. This means there is some δ such that for any $y \in X$ such that $|x - y| < \delta$, then $|f(y) - f(x)| < \varepsilon/2$. Moreover, since $x_n \to x$, then there exists some N_2 such that for all $n > N_2$, $|x_n - x| < \delta$. Letting $N > \max\{N_1, N_2\}$, then for any $n > N$, we have

$$|x_n - x| < \delta \Rightarrow |f(x_n) - f(x)| < \frac{\varepsilon}{2}$$

and since $n > N > N_1$, then

$$|f_n(x_n) - f(x_n)| < \frac{\varepsilon}{2}.$$

Finally, from the triangle inequality it follows that

$$|f_n(x_n) - f(x)| \leq |f_n(x_n) - f(x_n)| + |f(x_n) + f(x)| < \varepsilon.$$

Therefore $\lim_{n\to\infty} f_n(x_n) = f(x)$. □

(b) Suppose $\{f_n\}$ is a uniformly bounded sequence of Riemann integrable functions on $[a, b]$. Let $F_n : [a, b] \to \mathbb{R}$ be defined by $F_n(x) = \int_a^x f_n(t)dt$. Prove that $\{F_n\}$ contains a uniformly convergent subsequence.

Proof. Since $\{f_n\}$ is uniformly bounded, then there exists some $M \in \mathbb{R}$ such that $|f_n(x)| < M$ for all n and for all $x \in [a, b]$. For each n, f_n is Riemann integrable and so for any $x \in [a, b]$, since $\sup_{[a,b]} f_n < M$, it follows that

$$|F_n(x)| = \int_a^x f_n(t)dt < M(b - a).$$

Thus $\{F_n\}$ is uniformly bounded on $[a, b]$. Letting $\varepsilon > 0$, then we want to show there exists some δ such that for any $x, y \in [a, b]$, that if $|y - x| < \delta$, then $|F_n(y) - F_n(x)| < \varepsilon$. And this is to apply for all n. Note that if $x < y$, then

$$|F_n(y) - F_n(x)| = \int_a^y f_n(t)dt - \int_a^x f_n(t)dt = \int_x^y f_n(t)dt < M|y - x|. \quad (1)$$

Hence, if we choose $\delta = \varepsilon/M$, then for any $x < y$ such that $|y - x| < \delta$, it follows from (1) that

$$|F_n(y) - F_n(x)| < \varepsilon.$$

Since this is for every n, then $\{F_n\}$ is equicontinuous. Thus we have that $[a, b]$ is compact, $\{F_n\}$ is uniformly continuous (and thus pointwise continous), and that $\{F_n\}$ is equicontiuous. By Theorem 7.25, $\{F_n\}$ contains a convergent subsequence. □

AL.3.2

(a) Let G be a group with $|G| = 520 = 2^3 \cdot 5 \cdot 13$. Prove that G is not simple.

Proof. By the third Sylow Theorem, we have that the number of Sylow 5-subgroups, n_5, and the number of Sylow 13-subgroups, n_{13}, must satisfy

$$\begin{aligned} n_5 \mid 2^3 \cdot 13 \quad &\wedge \quad n_5 \equiv 1 (\text{mod } 5), \\ n_{13} \mid 2^3 \cdot 5 \quad &\wedge \quad n_{13} \equiv 1 (\text{mod } 13). \end{aligned}$$

This implies that $n_5 \in \{1, 26\}$ and $n_{13} \in \{1, 40\}$. Assuming that neither n_5 and n_{13} are equal to 1, then it follows that there are $26(5-1) = 104$ elements in G of order 5, and $40(13-1) = 480$ elements in G of order 13. A total of 584 distict elements. As this is a contradiction, it follows that either $n_5 = 1$ or $n_{13} = 1$ is whichever it is presents a nontrivial normal subgroup. Therefore G is not simple. □

(b) Let G be a group with $|G| = 36 = 2^2 \cdot 3^2$. Prove that G is not simple.

Proof. By the third Sylow Theorem, the number of Sylow 3-subgroups, n_3, must satisfy

$$n_3 \mid 2^2 \quad \wedge \quad n_3 \equiv 1 (\text{mod } 3).$$

This implies that $n_3 = 1$ $n_3 = 4$. If $n_3 = 1$, then there is only one such subgroup and by Corollary 20 (Dummit & Foote), it is normal. If $n_3 = 4$, then let H and K be two distinct subgroups of order 9. By Proposition 13 (Dummit & Foote),

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{81}{|H \cap K|}.$$

Since $HK \subseteq G$, then $|HK| \leq 36$ which implies that $|H \cap K| \geq 3$. Also note that the normalizer $N(H \cap K)$ includes H and K and since these are both distinct groups of order 9, then $N(H \cap K)$ must have at least 18 elements. Moreover, since $N(H \cap K) \leq G$, then its order must divide 36. Thus $|N(H \cap K)| = 18$ or $|N(H \cap K)| = 36$. If it is 18, then it has index 2 in G any is thus a normal subgroup. If it has order 36, then $N(H \cap K) = G$ which implies that $H \cap K$ is normal in G. Therefore G is not simple. □

AN.1.6

(a) Suppose $a_n \geq 0$ for all $n \in \mathbb{N}$. Let $s_k = \sum_{n=1}^{k} a_n$. Prove $\sum_{n=1}^{\infty} a_n$ converges if and only if its sequence of partial sums $\{s_k\}$ is bounded.

Proof. Assume that $\sum a_k$ converges. Then by definition

$$\lim_{n \to \infty} s_n = s \in \mathbb{R}.$$

For contradiction assume that $\{s_k\}$ is not bounded. Then for each $M \in \mathbb{R}$ there exists $k \in \mathbb{N}$ such that $s_k > M$. Thus letting $M = s$, then for all $n \geq k$

$$s_n = \sum_{i=1}^{n} a_i = \sum_{i=1}^{k} a_i + \sum_{i=k+1}^{n} a_k \geq s.$$

This contradicts that $\lim_{n \to \infty} s_n = s$.

Now assume that $\{s_k\}$ is bounded. Then because the terms of $\{a_k\}$ are all nonnegative, then $\{s_k\}$ is a monotone increasing sequence which is bounded above. Thus $\{s_k\}$ is convergent and so $\sum a_k$ converges. □

(b) Let $\alpha = \limsup_{n \to \infty} \sqrt[n]{|a_n|}$. Prove that if $\alpha > 1$ then $\sum_{n=1}^{\infty} a_n$ diverges.

Proof. We assume that $\alpha < \infty$. If $\alpha > 1$, then since α is the limit of some subsequence,

$$\lim_{k \to \infty} \sqrt[n_k]{|a_{n_k}|} = \alpha > 1.$$

This implies that there are infinitely many terms $\sqrt[n_k]{|a_{n_k}|} > 1$ which implies that for infinitely terms $|a_{n_k}| > 1$. Thus $\lim_{n \to \infty} a_n > 0$ which, by contrapositive, implies that $\sum a_k$ does not converge. □

AL.4.3 Let G be a group of order $539 = 7^2 \cdot 11$.

(a) Prove that G is Abelian.

Proof. By the third Sylow theorem, the number of Sylow 7-subgroups, n_7, and the number of Sylow 11-subgroups, n_{11} must satisfy

$$n_7 \mid 11 \ \wedge \ n_7 \equiv 1(\bmod 11).$$
$$n_{11} \mid 7 \ \wedge \ n_{11} \equiv 1(\bmod 11).$$

With these conditions, it follows that $n_7 = n_{11} = 1$. Thus there is one unique Sylow 7-subgroup, call it S, and one unique Sylow 11-subgroup, call it E. Since S and E are unique, then $S \trianglelefteq G$ and $E \trianglelefteq G$. Moreover, since E is of prime order, then E is cyclic and thus abelian.

Now let $g_1, \ldots, g_r$ be representatives of the distinct non-central conjugacy classes. Then by the class equation

$$|S| = |Z(S)| + \sum_{i=1}^{r} [S : C_S(g_i)].$$

Since each conjugacy class is noncentral, then $C_S(g_i) \neq S$ for all $i = 1, \ldots, r$. We have that 7 divides the left hand side and 7 divides $[S : C_S(g_i)]$, then 7 divides $Z(S)$. Thus $Z(S)$ is nontrivial. Since S is the only Sylow 7-subgroup, then either $|Z(S)| = 7$ or $|Z(S)| = 49$. If the latter is true, then S is abelian and so since $E \trianglelefteq G$, then $ES \leq G$ and since both groups are normal and there intersection is the identity, then $ES \cong E \times S$ which is abelian. If $|Z(S)| = 7$, then $|S/Z(S)| = 7$ and thus is cyclic. Thus $S/Z(S) = \langle xZ(S) \rangle$ for some $x \in S$. Letting $g, h \in S$ then for some $m, n \in \mathbb{Z}$ we have that $gZ(S) = x^m Z(S)$ and $hZ(S) = x^n Z(S)$. This implies that there exists $z_1, z_2 \in Z(S)$ such that $g = x^m z_1$ and $h = x^n z_2$. Thus

$$\begin{aligned} gh &= x^m z_1 x^n z_2 \\ &= x^{m+n} z_1 z_2 \\ &= x^{m+n} z_2 z_1 \\ &= x^n z_2 x^m z_1 \\ &= hg. \end{aligned}$$

Thus S is abelian. Since $S \cap E = \{e\}$ then $SE = G$ and G is therefore abelian as the product of abelian groups. □

(b) Give an example from each isomorphism class of groups of order 539.

Solution. Since G was shown to be abelian in part (a), and since it is finite, then by the Fundamental Theorem of Finite Abelian Groups we have that

$$G \cong \mathbb{Z}_{49} \times \mathbb{Z}_{11}, \quad G \cong \mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_{11}.$$

■

(c) For each isomorphism class of groups of order 539, determine (with explanation) the number of elements of order 7.

Solution. For $\mathbb{Z}_{49} \times \mathbb{Z}_{11}$, we note that the order of an element $(a, b) \in \mathbb{Z}_{49} \times \mathbb{Z}_{11}$ is $o(a, b) = lcm(o(a), o(b))$. Thus if

$$o(a, b) = 7$$

and since $o(a) = 1, 7, 49$ and $o(b) = 1, 11$ then we are looking for (a, b) such that $o(a) = 7$ and $o(b) = 1$. The only element in $\mathbb{Z}_{11}$ with order 1 is 1. Thus we are looking for elements of the form $(a, 1)$. The only element in $\mathbb{Z}_{49}$ with order 1 is 1. Every other element in $\mathbb{Z}_{49}$ either has order 7 or order 49. The elements with order 49 are those elements which are relatively prime to 49. The elements which are not relatively prime to 49 are $7, 14, 21, 28, 35, 42$. Thus there are 6 elements of order 7 in $\mathbb{Z}_{49} \times \mathbb{Z}_{11}$.

For $\mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_{11}$, we are looking for elements (a, b, c) such that

$$lcm(o(a), o(b), o(c)) = 7.$$

Since $\mathbb{Z}_7 \times \mathbb{Z}_7$ is a group of order 49 and no element can have order 49, then there are $49 - 1 = 48$ many elements order 7. ■

AN.1.13 Suppose that $\{f_n\}$ is a sequence of real-valued functions on a compact metric space K. Suppose $\{f_n\}$ is equicontinuous and pointwise convergent. Prove that $\{f_n\}$ is uniformly convergent.

Proof. Let $\varepsilon > 0$, then since $\{f_n\}$ is equicontinuous, there exists $\delta > 0$ such that for all $x, y \in K$ with $|x - y| < \delta$,

$$|f_n(x) - f_n(y)| < \frac{\varepsilon}{4}$$

for all $n \in \mathbb{N}$. Define

$$K \subseteq S = \bigcup_{x \in K} N_\delta(x).$$

Then this forms an open cover of K and since K is compact, there exists a finite subcover. That is, there exists $x_1, \ldots, x_n \in K$ such that

$$K \subseteq \bigcup_{i=1}^{n} N_\delta(x_i).$$

For each $x_i \in K$, by the assumed pointwise convergence, there exists $N_i \in \mathbb{N}$ such that for any $n \geq N_i$, we have

$$|f_n(x_i) - f(x_i)| < \frac{\varepsilon}{4}.$$

Let $N = \max\{N_1, \ldots, N_n\}$ and take $n, m \geq N$. For each $x \in K$, there exists $x_i \in K$ such that $x \in N_\delta(x_i)$ and

$$\begin{aligned}|f_n(x) - f_m(x)| &= |f_n(x) - f_n(x_i) + f_n(x_i) - f(x_i) + f(x_i) - f_m(x_i) + f_m(x_i) - f_m(x)| \\ &\leq |f_n(x) - f_n(x_i)| + |f_n(x_i) - f(x_i)| + |f(x_i) - f_m(x_i)| + |f_m(x_i) - f_m(x)| \\ &< \frac{\varepsilon}{4} + \frac{\varepsilon}{4} + \frac{\varepsilon}{4} + \frac{\varepsilon}{4} = \varepsilon.\end{aligned}$$

Therefore $\{f_n\}$ is uniformly convergent over K. □

AL.3.3 Note: $675 = 3^3 \cdot 5^2$.

(a) Up to isomorphism, describe all the Abelian groups of order 675.

Proof. By the Fundamental Theorem of Abelian groups, every finite abelian group is isomorphic to the direct product of cyclic groups of prime power order. Thus we have the following groups

$$\begin{aligned}\mathbb{Z}_{27} \times \mathbb{Z}_{25} \qquad & \mathbb{Z}_{27} \times \mathbb{Z}_5 \times \mathbb{Z}_5 \\ \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_{25} \qquad & \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \\ \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25} \qquad & \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5.\end{aligned}$$

□

(b) Consider $G = \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$.

i. Determine, with explanation, the number of elements of order 15 in G.

Proof. Note that $15 = 3 \cdot 5$. Since for any $(a, b, c) \in \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$, we have that

$$|(a, b, c)| = lcm(|a|, |b|, |c|)$$

then we are looking for (a, b, c) such that $|(a, b, c)| = 15$. This gives us the following options

$$\begin{aligned}1 \cdot 3 \cdot 5 \rightarrow &(0,1,5), (0,1,10), (0,1,15), (0,1,20), \\ &(0,2,5), (0,2,10), (0,2,15), (0,2,20) \\ 3 \cdot 1 \cdot 5 \rightarrow &(3,0,5), (3,0,10), (3,0,15), (3,0,20), \\ &(6,0,5), (6,0,10), (6,0,15), (6,0,20).\end{aligned}$$

There are 16 elements of order 15. □

ii. Determine, with explanation, the number of elements of order 45 in G.

Proof. Note that $45 = 9 \cdot 5$. So we are in need of elements with orders: $9, 1, 5$; This gives the following:

$$\begin{aligned} 9 \cdot 1 \cdot 5 \to &(1,0,5),(1,0,10),(1,0,15),(1,0,20),\\ &(2,0,5),(2,0,10),(2,0,15),(2,0,20),\\ &(4,0,5),(4,0,10),(4,0,15),(4,0,20),\\ &(5,0,5),(5,0,10),(5,0,15),(5,0,20),\\ &(7,0,5),(7,0,10),(7,0,15),(7,0,20),\\ &(8,0,5),(8,0,10),(8,0,15),(8,0,20). \end{aligned}$$

There are 24 elements of order 45. □

AL.6.6 Assume that R is a commutative ring with identity, and that M is an ideal of R.

(a) Prove that M is a maximal ideal of R iff R/M is a field.

Proof. ($\Rightarrow$) Assume that M is a maximal ideal of R. Let $a \in R$ and define

$$S = \{ar + m : r \in R, m \in M\}.$$

We claim that S is an ideal of R containing M.

[Supply proof if there is time]

Since M is maximal, then $S = R$ and thus $1 \in S$. Hence, for some $r \in r$ and $m \in M$ we have that $1 = ar + m$ which implies that $(a + M)(r + M) = 1 + M$. Since $r \in R$ was arbirary, then every element of R/M is a unit and therefore R/M is a field.

($\Leftarrow$) Assume that R/M is a field and that B is an ideal of R properly containing M. Let $b \in B - M$. Then $b + M$ is a nonzero element of R/M and is therefore a unit. Then for some $c \in R$ we have that $(b+M)(c+M) = bc+M = 1+M$. This implies that $1 - bc \in M \subset B$. And since $b \in B$ and $c \in R$, then $bc \in B$. Thus $(1 - bc) + bc = 1 \in B$. Hence $B = R$. Therefore M is a maximal ideal. □

(b) Assume that R is a PID. Prove that $r \in R$ is prime iff $R/(r)_i$ is a field.

Proof. ($\Rightarrow$) Assume that $r \in R$ is prime. Then $(r)_i$ is a prime ideal. We want to show that $(r)_i$ is maximal. Let I be an ideal of R that properly contains $(r)_i$. Since R is a PID, then for some $a \in R$, $I = (a)_i$. By the assumed inclusion, $r \in (a)_i$ and so for some $t \in R$ we have that $r = ta$. Thus $ta \in (r)_i$, which is a prime ideal, and so either $t \in (r)_i$ or $a \in (r)_i$. If $t \in (r)_i$, then $t = rs$ for some $s \in R$ and so $r = ta = rsa$ thus

$$r(1 - sa) = 0 \to 1 = sa.$$

Thus $1 \in (a)_i$ and so $(a)_i = R$. Otherwise, if $a \in (r)_i$, then $(r)_i = (a)_i$ which contradicts the proper inclusion we assumed. Therefore $(r)_i$ is maximal and $R/(r)_i$ is a field.

($\Leftarrow$) Assume that $R/(r)_i$ is a field. Let $a, b \in R$ be nonzero such that $ab \in (r)_i$. Then $(ab+(r)_i) = (r)_i$. This implies that $(a+(r)_i)(b+(r)_i) = (r)_i$. However, since $R/(r)_i$ is a field, then there are no zero divsors and thus either $(a+(r)_i) = (r)_i$ or $(b+(r)_i) = (r)_i$. That is, either $a \in (r)_i$ or $b \in (r)_i$. Therefore $(r)_i$ is a prime ideal and so $r \in R$ is prime. □

AL.6.7 Let $I = (x^4 + 7x^2)_i$ in $\mathbb{Q}[x]$.

(a) Assume that J is an ideal of $\mathbb{Q}[x]$. Prove that $I \subseteq J$ iff $J = (f(x))_i$ for some monic $f(x) \in \mathbb{Q}[x]$ such that $f(x) \mid x^4 + 7x^2$.

Proof. ($\Rightarrow$) Assume that $I \subseteq J$. We first note that since $\mathbb{Q}$ is a field, then $\mathbb{Q}$ is a PID. Thus for some $f(x) \in \mathbb{Q}[x]$, we have that $J = (f(x))_i$. Since $I \subseteq J$, then $x^4 + 7x^2 = h(x)f(x)$ for some $h(x) \in \mathbb{Q}[x]$. Hence $f(x) \mid x^4 + 7x^2$.
($\Leftarrow$) Assume that $J = (f(x))_i$ for some monic $f(x) \in \mathbb{Q}[x]$ such that $f(x) \mid x^4+7x^2$. This implies that $x^4 + 7x^2 = h(x)f(x)$ for some $h(x) \in \mathbb{Q}[x]$. Hence $x^4 + 7x^2 \in (f(x))_i$. Thus $I \subseteq J$. □

(b) Determine, with explanation, all ideals J in $\mathbb{Q}[x]$ such that $I \subseteq J$.

Proof. By part (a), if $I \subseteq J$, then J must be generated by a monic factor of $x^4 + 7x^2$. Given that $x^4 + 7x^2 = x^2(x^2 + 7)$, then the only possiblities for J are

$$J = (x)_i \qquad J = (x^2)_i$$
$$J = (x^2 + 7)_i \qquad J = (x^3 + 7x)_i$$
$$J = (x^4 + 7x)_i.$$

□

(c) Determine, with explanation, all ideals J from (b) such that $\mathbb{Q}[x]/J$ is a field, and express each of these fields in the form $\mathbb{Q}(d)$ for some $d \in \mathbb{C}$.

Proof. In order for $\mathbb{Q}[x]/J$ to be a field, we need for J to be generated by an irreducible polynomial over $\mathbb{Q}$. Of the options from (b), we have $J = (x)_i$ and $J = (x^2 + 7)_i$. This gives the following fields: $\mathbb{Q}(0) = \mathbb{Q}$ and $\mathbb{Q}(\sqrt{7})$. □

AL.6.8 Assume that F is finite field.

(a) Indicate why $\text{char}(F)$ is a prime number, p.

Proof. For contradiction, assume that $\text{char}(F) = mn$ for $m, n \in \mathbb{N}$ such that $m, n > 1$. Then for any $\alpha \in F$ we have that

$$(mn)\alpha = m(n\alpha) = m(n \cdot 1 \cdot \alpha) = 0.$$

Since $n\alpha = \beta \in F$, then $m\beta = 0$. Since $m < n$, then this contradicts that mn is the smallest integer such that $mn \cdot 1 = 0$. Therefore the characteristic must be a prime p. □

(b) Indicate why F is a vector space over $\mathbb{Z}_p$.

Proof. Let $m, n \in \mathbb{Z}_p$ and $\alpha, \beta \in F$. Then we have that

$$\begin{aligned} m\alpha &\in F \\ (m+n)\alpha &= m\alpha + n\alpha \\ (\alpha+\beta)m &= m\alpha + m\beta. \end{aligned}$$

This coupled with the facts that F is an abelian additive group shows that F is a vector space over $\mathbb{Z}_p$. □

(c) Assume that $[F : \mathbb{Z}_p] = n$. Determine (with proof) $|F|$.

Proof. By part (b), F is a vector space over $\mathbb{Z}_p$. Let $\{1, \alpha_1, \ldots, \alpha_n\}$ be a basis for this vector space. Then $\text{span}\{1, \alpha_1, \ldots \alpha_n\} = F$. Thus every element of F can be expressed as a linear combination of the n many basis elements. Each basis element can take on any one of p many coefficients from $\mathbb{Z}_p$. Thus, there are p^n many possible linear combinations and so $|F| = p^n$. □

(d) Explain why F is the splitting field over $\mathbb{Z}_p$ of a seperable polynomial.

Proof. Let $\alpha \in F$, then if $\alpha = 0$, we have that $\alpha^{p^n} = 0 = \alpha$. Note that the nonzero elements of F form a group under multiplication of order $p^n - 1$ and from this it follows that for any nonzero $\alpha \in F$, we have that $\alpha^{p^n-1} = 1$ and so $\alpha^{p^n} - \alpha = 0$. Now consier the polynomial $x^{p^n} - x$ in $\mathbb{Z}_p$. This polynomial has at most p^n roots and each element of F is a root, of which there are exactly p^n many of them. Therefore F is the splitting field of $x^{p^n} - x$ and since all the roots are distinct, then the polynomial is seperable. □

AL.6.9

(a) Find the splitting field of $x^3 - 2$ over $\mathbb{Q}$. Also, if we denote the splitting field by L, then find $[L : \mathbb{Q}]$.

Proof. Using DeMoivre's theorem, we can write $x = r(\cos\theta + i\sin\theta)$ and so we have that $r^3(\cos 3\theta + i\sin 3\theta) = 2$. This implies that $r = \sqrt[3]{2}$ and $\theta = 0, 2\pi/3, 4\pi/3$. Thus, the roots of $x^3 - 2$ are

$$c_1 = \sqrt[3]{2}, \quad c_2 = \omega\sqrt[3]{2}, \quad c_2 = \omega^2\sqrt[3]{2},$$

where $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. The splitting field must therefore contain $\sqrt[3]{2}$. Note that $1, \sqrt[3]{2}, \sqrt[3]{4}$ is a basis of $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$. Also note that if $i\sqrt{3} \in \mathbb{Q}$, then $-\frac{1}{2} + i\frac{\sqrt{3}}{2} = \omega \in \mathbb{Q}$. Since $1, i\sqrt{3}$ is a basis for $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ over $\mathbb{Q}(\sqrt[3]{2})$, then it follows that the product of these two bases give us a basis: $1, \sqrt[3]{2}, \sqrt[3]{4}, i\sqrt{3}, \sqrt[3]{2}i\sqrt{3}, \sqrt[3]{4}i\sqrt{3}$ over $\mathbb{Q}$. Letting $L = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$, then clearly $x^3 - 2$ splits over L. Given the number of basis elements, it follows that $[L : \mathbb{Q}] = 6$. □

(b) If we denote the roots of $x^3 - 2$ by c_1, c_2, c_3, then express each element of $G(L/\mathbb{Q})$ as a permutation of the subscripts of c_1, c_2, c_3.

Proof. Given any $\sigma \in \mathrm{Aut}(L/\mathbb{Q})$, it is completely determined by where it sends the basis elements. The pair $\{\sqrt[3]{2}, \omega\}$ generates the basis mentioned above and so we will then consider what each map does to $\sqrt[3]{2}$ and ω. We have 6 possibilities

$$\sigma_1 := \begin{cases} \sqrt[3]{2} & \mapsto \sqrt[3]{2} \\ \omega & \mapsto \omega \end{cases} \qquad \sigma_2 := \begin{cases} \sqrt[3]{2} & \mapsto \omega\sqrt[3]{2} \\ \omega & \mapsto \omega \end{cases} \qquad \sigma_3 := \begin{cases} \sqrt[3]{2} & \mapsto \omega^2\sqrt[3]{2} \\ \omega & \mapsto \omega \end{cases}$$

$$\sigma_4 := \begin{cases} \sqrt[3]{2} & \mapsto \sqrt[3]{2} \\ \omega & \mapsto \omega^2 \end{cases} \qquad \sigma_5 := \begin{cases} \sqrt[3]{2} & \mapsto \omega\sqrt[3]{2} \\ \omega & \mapsto \omega^2 \end{cases} \qquad \sigma_6 := \begin{cases} \sqrt[3]{2} & \mapsto \sqrt[3]{2} \\ \omega & \mapsto \omega^2. \end{cases}$$

With these in hand, we see the following correspondances with the index permutations:

$$\sigma_1 : (1) \qquad \sigma_2 : (123) \qquad \sigma_3 : (132)$$
$$\sigma_4 : (23) \qquad \sigma_5 : (12) \qquad \sigma_6 : (13).$$

□

(c) For $H = \langle(123)\rangle$, find the subfield of L that corresponds to H as given by the Fundamental Theorem of Galois Theory.

Proof. By part (b), we see that $H = \langle(123)\rangle$ corresponds to the following automorphisms $\{\sigma_1, \sigma_2, \sigma_3\}$. By the definitions of each of these mappings, we see that each one of them fix ω and only fix ω. Therefore the corresponding fixed field is $\mathbb{Q}(\omega)$. □

AL.6.10 Assume that F is a subfield of $\mathbb{C}$, n is a positive integer, and that ξ is a primitive nth root of unity. Assume that $\xi \in F$.

(a) Let $c \in F$, let E be the splitting field of $x^n - c$ over F, and let δ be any root of $x^n - c$. Prove that $E = F(\delta)$.

Proof. Using DeMoive's Theorem, we can deduce that the roots of $x^n - c$ are of the form $\xi^k \sqrt[n]{c}$ for $0 \leq k \leq n-1$. Seeing as $\xi \in F$, then adjoining $\delta = \xi^m \sqrt[n]{c}$ to F, we obtain all the terms needed to generate all n roots of the polynomial. And so $x^n - c$ splits in $F(\delta)$. □

(b) Prove that $G(E/F)$ is Abelian.

Proof. Because $\xi \in F$, then any $\sigma \in \mathrm{Aut}(E/F)$ will fix ξ. Thus the only basis elements to be permuted are those generated by $\sqrt[n]{c}$. This implies that $\sigma_i(\sqrt[n]{c}) = \xi^i \sqrt[n]{c}$ for all $0 \leq i \leq n-1$. This induces a cyclic group of automorphisms and therefore $G(E/F)$ is Abelian. □