Math 350, Sections 01,03, Fall 2021

Solutions to the Final Exam

1. **(20 points)** For each of the following groups G, decide whether or not G has an element of order 6. If so, give an example of such an element, and prove that it indeed has order 6. If not, prove that there is no such element.

(a) C_{98} (b) $C_3 \times C_{15}$ (c) $C_9 \times Q_8$ (d) S_5

Solutions. (a): $\boxed{\text{NO}}$ The group $G = C_{98}$ has order 98, so by a corollary of Lagrange, we have $o(x)|98$ for every $x \in G$. Since $6 \nmid 98$, G has no such element.

(b): $\boxed{\text{NO}}$ The group $G = C_3 \times C_{15}$ has order $3 \cdot 15 = 45$. So by a corollary of Lagrange, we have $o(x)|45$ for every $x \in G$. Since $6 \nmid 45$, G has no such element.

(c): $\boxed{\text{YES}}$ Let $x = (3, -1) \in C_9 \times Q_8$. By Theorem 4.4(iii), the order of $3 \in C_9$ is $o(3) = 9/(3, 9) = 9/3 = 3$. Meanwhile, $-1 \in Q_8$ has $-1 \neq 1$ but $(-1)^2 = 1$, so $o(-1) = 2$.
Thus, by Theorem 6.1(i), we have $o(x) = \text{lcm}(o(3), o(-1)) = \text{lcm}(3, 2) = 6$.

(d): $\boxed{\text{YES}}$ Let $\sigma = (1, 2, 3)(4, 5) \in S_5$. Since σ consists of a(disjoint) 3-cycle and 2-cycle, we have $o(\sigma) = \text{lcm}(3, 2) = 6$.

---

2. **(10 points)** Let G be a nonabelian group of order 27, and let $a \in G$. Prove that $a^9 = e$.

Proof. By a Corollary to Lagrange, we have $o(a)|27$, so $o(a)$ is one of $1, 3, 9, 27$.
If $o(a) = 27$, then $|\langle a \rangle| = 27 = |G|$, so by the pigeonhole principle we have $\langle a \rangle = G$. But then G is cyclic (with generator a) and hence abelian, a contradiction. So $o(a) \neq 27$.
Thus $m = o(a)$ is one of $1, 3, 9$, all of which divide 9, i.e., there is an integer $k \geq 1$ such that $mk = 9$.
Therefore, $a^9 = a^{mk} = (a^m)^k = e^k = e$ QED

---

3. **(20 points)** Let G and H be groups, and let $\varphi : G \to H$ be a homomorphism. Recall that $Z(G)$ denotes the center of G, and $Z(H)$ denotes the center of H.

(a) If φ is injective, prove that $\varphi^{-1}(Z(H)) \subseteq Z(G)$.

(b) If φ is sujective, prove that $\varphi(Z(G)) \subseteq Z(H)$.

Proof. (a): Given $a \in \varphi^{-1}(Z(H))$, we wish to show a commutes with every element of G. Given $b \in G$, we have

$$\varphi(ab) = \varphi(a)\varphi(b) = \varphi(b)\varphi(a) = \varphi(ba),$$

because φ is a homomorphism, and because $\varphi(a) \in Z(H)$. Since φ is injective, it follows that $ab = ba$, as desired. Because this holds for all $b \in G$, we have $a \in Z(G)$. QED

(b): Given $x \in \varphi(Z(G))$, we have $x = \varphi(a)$ for some $a \in Z(G)$. We wish to show x commutes with every element of H. Given $y \in H$, there is some $b \in G$ such that $y = \varphi(b)$, since φ is surjective. Therefore,

$$xy = \varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a) = yx,$$

because φ is a homomorphism, and because $a \in Z(G)$. Sincee this holds for all $y \in H$, we have $x \in Z(H)$. QED

---

4. **(30 points)** Let G be an abelian group, and define

$$K = \{x \in G \,|\, x^{2^n} = e \text{ for some integer } n \geq 0\}.$$

Equivalently, an element $x \in G$ belongs to K if and only $o(x)$ is a power of 2.

(a) Prove that K is a subgroup of G.

(b) Prove that no element of G/K has even order.

Proof. (a) **(Nonempty)**: We have $e \in K$ because $e^1 = 0$ and $1 = 2^0$ is a power of 2.
(Closed): Given $x, y \in K$, there are integers $m, n \geq 0$ such that $x^{2^m} = y^{2^n} = e$. Let $k = \max\{m, n\} \geq 0$ be the larger of m and n. Then $x^{2^k} = y^{2^k} = e$, since 2^k is divisible by both 2^m and 2^n. Thus,

$$(xy)^{2^k} = x^{2^k} y^{2^k} = ee = e,$$

so $xy \in K$, as desired.
(Inverses): Given $x \in K$, there is an integer $n \geq 0$ such that $x^{2^n} = e$. Then

$$(x^{-1})^{2^n} = x^{-2^n} = \left(x^{2^n}\right)^{-1} = e^{-1} = e,$$

so $x^{-1} \in K$. QED

(b) Suppose that there is some $Ky \in G/K$ such that $o(Ky)$ is even. Then $o(Ky) = 2m$ for some integer $m \geq 1$.
In particular, we have $(Ky)^{2m} = Ke$, and hence $Ky^{2m} = Ke$, or equivalently, $y^{2m}e^{-1} \in K$. That is $y^{2m} \in K$.
By definition of K, then, there is some integer $n \geq 0$ such that $\left(y^{2m}\right)^{2^n} = e$. It follows that

$$(y^m)^{2^{(n+1)}} = y^{2^{(n+1)}m} = \left(y^{2m}\right)^{2^n} = e,$$

and hence, by definition of K, we have $y^m \in K$. Therefore $y^m e^{-1} \in K$, and hence $(Ky)^m = Ky^m = Ke$. However, we said $o(Ky) = 2m$, so in particular, $(Ky)^j \neq Ke$ for any integer j with $1 \leq j < 2m$. Since $1 \leq m < 2m$, this is a contradiction. Thus, no such $Ky \in G/K$ exists, as desired. QED

---

5. **(30 points)** Let R be a commutative ring with unity, and let $I, J \subseteq R$ be ideals. The **product ideal** IJ is defined to be

$$IJ = \{x_1y_1 + \cdots + x_ny_n \,|\, n \geq 1,\ x_i \in I,\ \text{and } y_i \in J\}.$$

(a) Prove that IJ **is** an ideal of R.

(b) Prove that $IJ \subseteq I \cap J$.

(c) If $I + J = R$, prove that $IJ = I \cap J$.

Proof. (a) (**Nonempty**): we have $0 = 0 \cdot 0 \in IJ$.
(**Closed under** $+$): Given $a, b \in IJ$, write $a = x_1y_1 + \cdots + x_my_m$ and $b = x_1'y_1' + \cdots + x_n'y_n'$ where $m, n \geq 1$, $x_i, x_i' \in I$, and $y_i, y_i' \in J$. Then $a + b = x_1y_1 + \cdots + x_my_m + x_1'y_1' + \cdots + x_n'y_n' \in IJ$.
(**Closed under** $-$): Given $a \in IJ$, write $a = x_1y_1 + \cdots + x_my_m$. Then
$-a = -x_1y_1 - \cdots - x_my_m = (-x_1)y_1 + \cdots + (-x_m)y_m \in IJ$.
(**Ideal property**): Given $a \in IJ$ and $r \in R$, write $a = x_1y_1 + \cdots + x_my_m$. Then
$ar = (x_1y_1)r + \cdots + (x_my_m)r = x_1(y_1r) + \cdots + x_m(y_mr) \in IJ$, because $y_ir \in J$ for all i. Similarly, $ra = (rx_1)y_1 + \cdots + (rx_m)y_m \in IJ$. QED

(b) First, for any $x \in I$ and $y \in J$, we have $xy \in I$ since $x \in I$ and $y \in R$, and $xy \in J$ since $x \in R$ and $y \in J$. Thus, $xy \in I \cap J$.
Given any $a \in IJ$, write $a = x_1y_1 + \cdots + x_my_m$, with $m \geq 1$, $x_i \in I$, and $y_i \in J$. Then $x_iy_i \in I \cap J$ for each i, by the previous paragraph. Hence, $a \in I$ (because it is a sum of elements of I, which is closed under $+$) and $a \in J$ (similarly), so $a \in I \cap J$. QED

(c) By part (b), it suffices to show ($\supseteq$). First, note that since R has unity 1, then by hypothesis, there is some $x \in I$ and $y \in J$ such that $x + y = 1$. Thus, given $a \in I \cap J$, by commutativity we have $a = a \cdot 1 = ax + ay = xa + ay \in IJ$, since $x, a \in I$ and $a, y \in J$.

---

6. **(25 points)** Let R be a commutative ring with unity, and let $I \subseteq R$ be an ideal. Prove that **the following two statements are equivalent**:

(i) $R^\times = R \setminus I$. (That is, the set of units of R is precisely the complement of I.)

(ii) I is a maximal ideal of R, and every proper ideal of R is contained in I.

Proof. (**(i)** $\Longrightarrow$ **(ii)**): First note that $1 \in R^\times = R \setminus I$; so I is a **proper** ideal of R.
Let $J \subseteq R$ be any ideal of R. Suppose $J \not\subseteq I$; we will show that $J = R$. By assumption, there is some $a \in J$ such that $a \notin I$. So $a \in R \setminus I = R^\times$, meaning that a^{-1} exists. We already have $J \subseteq R$; to show the reverse inclusion, pick $x \in R$. Then $x = a(a^{-1}x) \in J$ because $a \in J$ and $a^{-1}x \in R$, and because J is an ideal. Thus, $J = R$.
We have just shown that any ideal not contained in I must be R. Thus, on the one hand, if J is an ideal such that $I \subsetneq J \subseteq R$, then $J = R$; since we already know I is a proper ideal, this means I is maximal. And on the other hand, every proper ideal of R is contained in I, giving the second statement of (ii).
(**(ii)** $\Longrightarrow$ **(i)**): ($\subseteq$): Given $a \in R^\times$, so that $a^{-1} \in R$ exists. If $a \in I$, then for any $x \in R$, we have $x = a(a^{-1}x) \in I$, so that $I = R$, contradicting the assumption that I is maximal (and therefore proper). Thus, $a \notin I$; that is, $a \in R \setminus I$.
($\supseteq$): Given $a \in R \setminus I$, let $J = \langle a \rangle$ be the principal ideal generated by a. Then J is not contained in I (since $a \in J$ but $a \notin I$). By assumption, then, J is not proper, which means that $J = R$. Thus, $1 \in \langle a \rangle$, meaning that there is some $b \in R$ such that $1 = ba$. Since R is commutative, $ab = ba = 1$. That is, b is a multiplicative inverse of a, so a is a unit, i.e., $a \in R^\times$. QED

---

7. **(35 points)** Let R be a commutative ring, and let $I \subseteq R$ be an ideal. Define

$$J = \{r \in R \,|\, \text{there is an integer } n \geq 1 \text{ such that } r^n \in I\}.$$

(a) Prove that J is an ideal of R.

(b) Prove that the quotient ring R/J contains no nonzero nilpotent elements.

Proof. (a): (**Nonempty**): We have $0^1 = 0 \in I$, and hence $0 \in J$.
Before the next step, we state a lemma:
Lemma: For any integer $k \geq 1$ and any $x, y \in R$, there are integers $c_0, \ldots, c_k \in \mathbb{Z}$ such that $(x - y)^k = \sum_{i=0}^{k} c_i x^i y^{k-i}$.
[Here, $c_0 x^k y^0$ means $c_0 x^k$, and $c_k x^0 y^k$ means $c_k y^k$. I'm noting this in case R does not have unity.]
Proof of Lemma: By induction on k. For $k = 1$, $(x - y)^1 = x - y$ is already of the desired form. Given the statement for a particular $k \geq 1$, we have

$$\begin{aligned}(x-y)^{k+1} = (x-y)(x-y)^k = (x-y)\sum_{i=0}^{k} c_i x^i y^{k-i} &= \sum_{i=0}^{k} c_i x^{i+1} y^{k-i} - \sum_{i=0}^{k} c_i x^i y^{k-i+1} \\ &= c_0 x^{k+1} + \sum_{i=1}^{k} (c_{i+1} - c_i) x^i y^{k-i+1} - c_k y^{k+1},\end{aligned}$$

which is of the desired form. QED Lemma

Returning to the main proof:
(**Closed under** $-$): Given $x, y \in J$, there are integers $m, n \geq 1$ such that $x^m, y^n \in I$. Then by the Lemma applied to $k = m + n$, there are integers c_i such that $(x-y)^k = \sum_{i=0}^{k} c_i x^i y^{k-i}$. For each $i = 0, 1, \ldots, m$, we have $c_i x^i y^{k-i} = y^n (c_i x^i y^{m-i}) \in I$, since $y^n \in I$ and $c_i x^i y^{m-i} \in R$. [As before, if $i = m$, so that $m - i = 0$, then by $c_m x^m y^0$, we simply mean $c_m x^m$.] Similarly, for each $i = m+1, \ldots, k$, we have $c_i x^i y^{k-i} = x^m (c_i x^{i-m} y^{k-i}) \in I$, since $x^m \in I$ and $c_i x^{i-m} y^{k-i} \in R$.

Thus, $(x-y)^k = \sum_{i=0}^{k} c_i x^i y^{k-i}$ is a sum of elements of I, and hence $(x-y)^k \in I$. Therefore, $x - y \in J$.
(**Ideal Property**): Given $x \in J$ and $r \in R$, there is an integer $n \geq 1$ such that $x^n \in I$. Then because R is commutative, we have $(rx)^n = r^n x^n \in I$. Thus, $xr = rx \in J$.

(b): Given a nilpotent element $(J + a) \in R/J$, there is [by definition of nilpotent] some integer $n \geq 1$ such that $(J + a)^n = J + 0$. Therefore, $J + a^n = J + 0$, or equivalently, $a^n - 0 \in J$. Thus, there is some integer $m \geq 1$ such that $(a^n - 0)^m \in I$; that is, $a^{mn} \in I$. Since $mn \geq 1$ is an integer, then, we also have $a \in J$. Hence, $J + a = J + 0$.
We have just shown that the only nilpotent element in R/J is zero, as desired. QED

---

8. **(30 points)** Recall that $\mathbb{F}_2 = \{0, 1\}$ denotes the field of two elements. List all polynomials in $\mathbb{F}_2[X]$ of degree 4, and determine which of them are irreducible.
Make sure your list is complete; and as always, you must justify your answer for each polynomial.

Answer/Proof. A polynomial of degree 4 in $\mathbb{F}_2[x]$ is an expression of the form

$$a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0$$

with each $a_i \in \mathbb{F}_2$ and $a_4 \neq 0$. Thus, $a_4 = 1$, and each of the other four coefficients is one of the two elements $\{0, 1\}$ of $\mathbb{F}_2$. Thus, there are $1 \cdot 2^4 = 16$ such polynomials; the full list is:

x^4,	$x^4 + x^3$,	$x^4 + x^2$,	$x^4 + x^3 + x^2 + x$
$x^4 + x$,	$x^4 + x^3 + x^2$,	$x^4 + x^3 + x$,	$x^4 + x^2 + x$,
$x^4 + 1$,	$x^4 + x^3 + x^2 + 1$,	$x^4 + x^3 + x + 1$,	$x^4 + x^2 + x + 1$,
$x^4 + x + 1$,	$x^4 + x^2 + 1$,	$x^4 + x^3 + 1$,	$x^4 + x^3 + x^2 + x + 1$.

All such polynomials with $a_0 = 0$ (i.e., the first eight above) have 0 as a root; so they are divisible by x (Theorem 19.3), and hence the are reducible.
Similarly, all such polynomials with $1 + a_3 + a_2 + a_1 + a_0 = 0$ (i.e., the next four above, along with some of the first eight) have 1 as a root; so they are divisible by $x - 1 = x + 1$ (by the same Theorem), and hence they are reducible.
The only remaining polynomials are:

$$f_1(x) = x^4 + x^3 + x^2 + x + 1 \qquad f_2(x) = x^4 + x^2 + 1$$
$$f_3(x) = x^4 + x^3 + 1 \qquad f_4(x) = x^4 + x + 1$$

None of these four has a linear factor, because the only degree one polynomials are x and $x + 1$. If a polynomial g of degree four factors but does not have a linear factor, then it must factor as $g = h_1 h_2$, with $\deg h_1 = \deg h_2 = 2$. Furthermore, h_1 and h_2 must both be irreducible, or else (Theorem 19.8) one of them would have a zero, and therefore g would have a zero and hence a linear factor.

So let us find the irreducible polynomials of degree 2. There are only four polynomials of degree 2 in $\mathbb{F}_2[x]$, namely x^2, x^2+x, x^2+1, and x^2+x+1. The first three all have zeros, so only x^2+x+1 could possibly be irreducible. (And it is, by Theorem 19.8, because neither $x=0$ nor $x=1$ is a zero of it.) So the only way to produce a polynonial g like that described in the previous paragraph would be to multiply x^2+x+1 by itself. That gives

$$f_2(x) = x^4 + x^2 + 1 = (x^2+x+1)(x^2+x+1),$$

so that f_2 is reducible. But we have also shown that f_1, f_3, f_4 cannot factor at all.
So f_1, f_3, f_4 are the only irreducible polynomials of degree 4 in $\mathbb{F}_2[x]$. QED

BONUS A. **(2 points)** Recall that A_6 denotes the alternating group on 6 objects, and S_3 is the symmetric group on 3 objects. Find an **injective** homomorphism $\varphi : S_3 \to A_6$.

Answer/Proof. Each $\sigma \in S_3$ is a bijective function from $\{1,2,3\}$ to itself. For each such σ, define $\varphi(\sigma)$ as a function from $\{1,2,3,4,5,6\}$ to itself by

$$\big(\varphi(\sigma)\big)(i) = \begin{cases} \sigma(i) & \text{if } i \in \{1,2,3\}, \\ 3+\sigma(i-3) & \text{if } i \in \{4,5,6\}. \end{cases}$$

That is,

$$\begin{array}{ccc} \sigma(e) = e, & \sigma((1,2,3)) = (1,2,3)(4,5,6), & \sigma((1,3,2)) = (1,3,2)(4,6,5), \\ \sigma((1,2)) = (1,2)(4,5), & \sigma((1,3)) = (1,3)(4,6), & \sigma((2,3)) = (2,3)(5,6). \end{array}$$

The six outputs above are all even permutations, so we have indeed defined a function $\varphi : S_3 \to A_6$. In addition, since the outputs are all different, φ is one-to-one. It remains to show that φ is a homomorphism.
Given $\sigma, \tau \in S_3$, we claim that $\varphi(\sigma \circ \tau) = \varphi(\sigma) \circ \varphi(\tau)$. Observe that the function $\varphi(\sigma)$ maps $\{1,2,3\}$ into itself, while also mapping $\{4,5,6\}$ into itself; and similarly for $\varphi(\tau)$ and for $\varphi(\sigma\tau)$. Thus, for $i \in \{1,2,3\}$, we have

$$\big(\varphi(\sigma\tau)\big)(i) = \sigma\tau(i) = \sigma(\tau(i)) = \varphi(\sigma)\big(\varphi(\tau)(i)\big) = \big(\varphi(\sigma)\circ\varphi(\tau)\big)(i),$$

and for $i \in \{4,5,6\}$, we have

$$\big(\varphi(\sigma\tau)\big)(i) = 3+\sigma\tau(i-3) = 3+\sigma(\tau(i-3)) = \varphi(\sigma)\big(3+\tau(i-3)\big) = \varphi(\sigma)\big(\varphi(\tau)(i)\big) = \big(\varphi(\sigma)\circ\varphi(\tau)\big)(i).$$

Thus, we have shown that the two functions $\varphi(\sigma\tau)$ and $\varphi(\sigma)\circ\varphi(\tau)$ agree at every $i \in \{1,2,3,4,5,6\}$. That is, $\varphi(\sigma\circ\tau) = \varphi(\sigma)\circ\varphi(\tau)$, as claimed. QED

BONUS B. **(2 points)** Let $R = \big\{a + b\sqrt{7} \,\big|\, a,b \in \mathbb{Z}\big\}$, viewed as a subset of $\mathbb{R}$, with addition and multiplication as in $\mathbb{R}$. You may take my word for it that R is a commutative ring with unity. Prove that R has infinitely many units.

Proof. Let $u = 8+3\sqrt{7} \in R$ and $v = 8-3\sqrt{7} \in R$. Then $uv = 64 - 9\cdot 7 = 1$, so that u is a unit in R. Moreover, for every integer $n \geq 1$, the element $u^n \in R$ is also a unit, because $(u^n)(v^n) = (uv)^n = 1^n = 1$.
On the other hand, viewed as an element of the real line $\mathbb{R}$, we have $u > 1$, and hence $u < u^2 < u^3 < \cdots$, so that $u^n \neq u^m$ for any distinct positive integers $m \neq n$. Thus, $\{u^n \,|\, n \geq 1\}$ is an infinite set of units in R. QED