Groups and Rings: Solutions to Problem Sheet 5

Please email any questions or corrections to
hannah.tillmann-morris15@ic.ac.uk

December 2021

Question 1

(a) A coset $m + n\mathbb{Z}$ has order n in $\mathbb{Z}/n\mathbb{Z}$ if and only if it generates $\mathbb{Z}/n\mathbb{Z}$, which means that $1 + n\mathbb{Z} = km + n\mathbb{Z}$ for some $k \in \mathbb{Z}$. This means that $\exists k, l \in \mathbb{Z}$ such that $km + ln = 1$, which is true if and only if $(m, n) = 1$.

(b) Let $m+n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$. Then $(m, n) = 1$ iff $\exists k, l \in \mathbb{Z}$ such that $km+ln = 1$. But $km + ln = 1$ for some $l \in \mathbb{Z}$ if and only if $(k + n\mathbb{Z})(m + n\mathbb{Z}) = km + n\mathbb{Z} = 1 + n\mathbb{Z}$.

(c) If p is a prime then $(m, p^k) = 1$ if and only if p does not divide m.

$$\begin{aligned} |\{m \in \{1, 2, ..., p^k - 1\} \, : \, p \nmid m\}| &= |\{1, ..., p^k\} \setminus \{p, 2p, ..., (p^{k-1})p\}| \\ &= |\{1, ..., p^k\}| - |\{p, 2p, ..., (p^{k-1})p\}| \\ &= p^k - p^{k-1} \end{aligned}$$

(d) We want to use part (a), and to do this we notice that if $(m, n) = 1$ then $C_{mn} \cong C_m \times C_n$, so counting elements of order mn in C_{mn} is the same as counting elements of order mn in $C_m \times C_n$. In fact, an element $(g, h) \in C_m \times C_n$ has order mn if and only if g has order m and h has order n. Indeed, if $\mathrm{ord}(g) = m$ and $\mathrm{ord}(h) = n$ then $\mathrm{ord}\left((g, h)\right) = \mathrm{lcm}(m, n)$. But $\mathrm{lcm}(m, n) = mn$ since $(m, n) = 1$. For the other direction, suppose that $\mathrm{ord}((g, h)) = mn$ but $(\mathrm{ord}(g), \mathrm{ord}(h)) \neq (m, n)$. Then either $\mathrm{ord}(g) < m$ or $\mathrm{ord}(h) < n$. But then $\mathrm{ord}((g, h)) = \mathrm{lcm}(\mathrm{ord}(g), \mathrm{ord}(h)) \leq \mathrm{ord}(g)\mathrm{ord}(h) < mn$, contradicition.

For the second part of part (d), write out n as its unique prime factorisation $n = p_1^{k_1} p_2^{k_2} ... p_m^{k_m}$, where the order of the p_is doesn't matter, but each p_i is distinct. Since each of the prime power factors $p_i^{k_i}$ is coprime to the others, we can apply the first part of the question inductively to get

$$\varphi(n) = \varphi(p_1^{k_1})\varphi(p_2^{k_2})...\varphi(p_m^{k_m}).$$

Then we can apply part (c) to each factor to get

$$\varphi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1})...(p_m^{k_m} - p_m^{k_m-1}).$$

Taking the factor $p_i^{k_i}$ outside each of the brackets gives the desired expression.

Question 2

We will use Question 1(a), and consider $\varphi(\delta)$ as the number of elements of order δ in C_δ. We know by Lagrange's Theorem that $\text{ord}(x)$ divides d for all $x \in C_d$.

$$\begin{aligned} d = |C_d| &= \sum_{\delta | d} |\{x \in C_d : \text{ord}(x) = \delta\}| \\ &= \sum_{\delta | d} |\{x \in C_\delta : \text{ord}(x) = \delta\}| \\ &= \sum_{\delta | d} \varphi(\delta). \end{aligned}$$

To prove the second equality we need to show that every element of order δ in C_d is contained in the unique subgroup $H \subset C_d$ isomorphic to C_δ. To do this you can show that $H \cong C_\delta \implies H = \{y^{\frac{d}{\delta}} : y \in C_d\}$, and that if $x \in C_d$ has order δ then $x = y^{\frac{d}{\delta}}$ for some generator y of C_d.

Question 3

Since $x^{q-1} - 1$ is a polynomial of degree $q - 1$, we know it has at most $q - 1$ roots. Any solution to the equation $x^{q-1} = 1$ must be in $F^\times$. In fact, since F is a field of order q, we know that every nonzero element has a multiplicative inverse so $|F^\times| = q - 1$. $F^\times$ is a finite group of order $q - 1$ under multiplication so by Lagrange's Theorem every element of $F^\times$ has order dividing $q - 1$. But this is the same as saying $x^{q-1} = 1$ for all $x \in F^\times$.

Question 4

The idea is to use Question 3 by expressing $x^d - 1$ in terms of $x^{q-1} - 1$. Since d divides $q - 1$, $x^{q-1} = (x^d)^n$ for some n, so

$$x^{q-1} - 1 = (x^d)^n - 1 = (x^d - 1)((x^d)^{(n-1)} + (x^d)^{(n-2)} + ... + x^d + 1).$$

We know from Question 3 that this polynomial as exactly $q-1$ roots in F. The number of roots of the two factors must sum to $q-1$. Since x^d-1 is a polynomial of degree d it has at most d roots in F. Since $(x^d)^{(n-1)} + (x^d)^{(n-2)} + ... + x^d + 1$ is a polynomial of degree $d(n-1) = q - 1 - d$ it has at most $q - 1 - d$ roots in F, so $x^d - 1$ has at least d roots in F. So $x^d - 1$ has exactly d roots in F.

Question 5

We will follow the hint to use induction on d. The base case is $d = 1$. Clearly

$$|\{x \in F^\times : x = 1\}| = 1 = \varphi(1)$$

For the inductive step, suppose that

$$|\{x \in F^\times : x^k = 1\}| = \varphi(k)$$

for all $k < d$ such that $k|q-1$, where $d|q-1$. By Question 2 we have

$$d = \sum_{\delta|d} \varphi(\delta) = \varphi(d) + \sum_{\delta|d,\ \delta<d} \varphi(\delta)$$

but by Question 4 we also have

$$\begin{aligned} d &= |\{x \in F^\times : x^d = 1\}| \\ &= \sum_{\delta|d} |\{x \in F^\times : \operatorname{ord}(x) = \delta\}| \\ &= |\{x \in F^\times : \operatorname{ord}(x) = d\}| + \sum_{\delta|d,\ \delta<d} |\{x \in F^\times : \operatorname{ord}(x) = \delta\}|. \end{aligned}$$

Since we know by assumption that for all $\delta|d, \delta < d$ that

$$|\{x \in F^\times : \operatorname{ord}(x) = \delta\}| = \varphi(\delta),$$

we can equate the two sums over $\delta < d$ and be left with

$$|\{x \in F^\times : \operatorname{ord}(x) = d\}| = \varphi(d).$$

Question 6

Apply Question 4 with $d = q-1$. If F is a finite field of order q, then $F^\times$ is a finite group of order $q-1$, where the operation is multiplication. It's a cyclic group if and only if it contains an element of order $q-1$. By Question 4, the number of elements of $F^\times$ with order $q-1$ is $\varphi(q-1)$. As stated in Question 1, $\varphi(q-1) \geq 1$, so there exists an element of order $q-1$ in $F^\times$.

Question 7

Suppose $n = 1$. Then $(F, +)$ is an abelian group of prime order, so must be cyclic. Suppose $n > 1$. If $(F, +) \cong \mathbb{Z}/p^n\mathbb{Z}$ as additive groups then by distributivity $F \cong \mathbb{Z}/p^n\mathbb{Z}$ as rings (i.e. the multiplication on F must be the same as multiplication on $\mathbb{Z}/p^n\mathbb{Z}$ as well). But now from Question 1 parts (b) and (c) we have

$$|(\mathbb{Z}/p^n\mathbb{Z})^\times| = p^n - p^{n-1} < p^n - 1$$

This implies that there is a nontrivial element of F which has no multiplicative inverse. This contradicts F being a field. So $(F, +)$ cannot be cyclic if $n > 1$.

Question 8

(a) We use the binomial theorem to get $(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}$. Note that since p is prime, p divides $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ if and only if $i \neq p$. Since k has characteristic p, we know $pz = z + ... + z = 0$ for all $z \in k$, where the sum is p

copies of z, so $\binom{p}{i}x^i y^{p-i} = 0$ for all $i \neq p$. Thus $(x+y)^p = x^p + y^p$. The second part follows by induction: $(x+y)^{p^m} = ((x+y)^p)^{p^{m-1}} = (x^p + y^p)^{p^{m-1}}$.

(b) Part (a) shows that the Frobenius map preserves addition on a field of characteristic p, and since multiplication on fields is commutative, it clearly preserves multiplication. So the Frobenius map is a homomorphism of rings. To see that it is bijective on finite fields, note that k must have order p^m, and so by Question 3 every element of $k^\times$ satisfies the equation $x^{p_m - 1} = 1$. Thus every element of the whole field k satisfies $x^{p^m} = x$, so composing the Frobenius map m times gives the identity map on k. So the Frobenius map must be a bijection, and thus an automorphism.

(c) The fixed points of the Frobenius map are the elements of F satisfying $x^p - x = 0$. From Question 3 we know that every one of the p elements of the subfield $\mathbb{F}_p \subset F$ satisfies this equation. There are at most p roots of the polynomial $x^p - x$ since it's of degree p. So the elements of the subfield $\mathbb{F}_p$ are all the fixed points of the Frobenius map.

Question 9

Suppose $\phi \in \mathrm{Aut}(\mathbb{Q})$. Then $\phi(1)$ must be 1 to preserve the multiplicative structure in $\mathbb{Q}$. The additive structure is also preserved, so for any $n \in \mathbb{Z} \subset \mathbb{Q}$

$$\phi(n) = \phi(1 + 1 + ... + 1) = \phi(1) + \phi(1) + ... + \phi(1) = 1 + 1 + ... + 1 = n.$$

ϕ must preserve inverses, that is $\phi(\frac{1}{n}) = \phi(n)^{-1} = \frac{1}{n}$ for all $n \in \mathbb{Z}$. So for any $\frac{a}{b} \in \mathbb{Q}$,

$$\phi\left(\frac{a}{b}\right) = \phi(a)\phi\left(\frac{1}{b}\right) = \frac{a}{b},$$

so $\phi \equiv \mathrm{id}_{\mathbb{Q}}$. We've proved that $\mathrm{Aut}(\mathbb{Q})$ is the trivial group.