7210 Review

Duncan Wilkie

5 December 2022

Problem 1. *If $x^2 = 1$ for all $x \in G$, then G is Abelian.*

Proof. Take $a, b \in G$. $x^2 = 1 \Leftrightarrow x = x^{-1} \Rightarrow 1 = (ab)^2 = abab = aba^{-1}b^{-1} \Leftrightarrow ab = ba$. □

Problem 2. *Any finite group G of even order contains an element of order 2.*

Proof. Consider the set A of all self-inverse elements in G. Its complement must be of even cardinality, since every element of it has a distinct inverse, so the set can be gathered into distinct inverse pairs. Accordingly, $|A|$ is even. This means there exists a non-identity element that's self-inverse, which is necessarily of order 2. □

Problem 3. *If $n = 2k$ is even and $n \geq 4$, then $z = r^k$ is an element of order 2 which commutes with all elements of D_{2n}. Also, z is the only nonidentity element which commutes with all elements of D_{2n}.*

Proof. This is a boring computation using the presentation $\langle s, r \mid s^2 = 1, r^n = 1, sr = r^{-1}s \rangle$. □

Problem 4. *If n is odd and $n > 3$, the identity is the only element of D_{2n} that commutes with all other elements.*

Proof. This is a boring computation using the presentation $\langle s, r \mid s^2 = 1, r^n = 1, sr = r^{-1}s \rangle$. □

Problem 5. *Let p be a prime. An element σ has order p in S_n iff its cycle decomposition is a product of commuting p-cycles. There exist composite numbers for which this doesn't hold.*

Proof. □

Problem 6. *For all $\sigma \in S_n$, $|\sigma|$ is the least common multiple l of the lengths of the cycles in its cycle decomposition.*

Problem 7. *If p is prime, $|GL_2(\mathbb{F}_p)| = p^4 - p^3 - p^2 + p$.*

Problem 8. *For any group G, the map from G to itself defined by $f : g \mapsto g^2$ is a homomorphism iff G is Abelian.*

Proof.

$$(ab)^2 = f(ab) = f(a)f(b) = a^2b^2 \Leftrightarrow abab = a^2b^2 \Leftrightarrow ba = ab$$

□

Problem 9. *Let G be a finite group which possesses an automorphism σ such that $\sigma(g) = g$ iff $g = 1$. If σ^2 is the identity map from G to G, prove that G is Abelian.*

Proof.

$$\sigma(\sigma(a)) = a \Leftrightarrow \sigma(a) = \sigma^{-1}(a)$$

□

Problem 10. *If $H \circlearrowright A$, show that the relation $\sim$ on A defined by*

$$a \sim b \Leftrightarrow \exists h \in H : a = hb$$

is an equivalence relation.

Problem 11. *A group G with $n = |G| > 2$ cannot have a subgroup H with $|H| = n - 1$.*

Problem 12. *If G is an Abelian group, then $G_T = \{g \in G \mid |G| < \infty\} \leq G$. Give a counterexample when G is not Abelian.*

Problem 13. *Prove that $SL_2(\mathbb{F}_3)$ is the subgroup of $GL_2(\mathbb{F}_3)$ generated by $r = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ and $s = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$*

Problem 14. *A group H is called finitely generated if $H = \langle A \rangle$ for some finite set A. Every finite group is finitely generated, $\mathbb{Z}$ is finitely generated, and every finitely generated subgroup of the additive group $\mathbb{Q}$ is cyclic.*

Problem 15. *A subgroup N of a group G is normal iff $gNg^{-1} \subseteq N$ for all $g \in G$.*

Problem 16. *If G is a group such that $G/Z(G)$ is cyclic, then G is Abelian.*

Problem 17. *Let G be a group. Then $N = \langle x^{-1}y^{-1}xy \mid x, y \in G \rangle$ is a normal subgroup of G and G/N is Abelian.*

Problem 18. *If p is prime then $a^p \equiv a \pmod{p}$ for all $a \in \mathbb{Z}$.*

Problem 19. *If N is a normal subgroup of the finite group G and $|N|$ and $|G : N|$ are relatively prime then N is the unique subgroup of G of order $|N|$.*

Problem 20. *$\mathbb{Q}$ has no proper subgroups of finite index, as does $\mathbb{Q}/\mathbb{Z}$.*

Problem 21. *If H is a normal subgroup of G of prime index p then for all $K \leq G$ either $K \leq H$ or $G = HK$ and $|K : K \cap H| = p$.*

Problem 22. *For a finite group G, the following are equivalent:*

1. *G is solvable*
2. *G has a chain of subgroups $1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_s = G$ such that H_{i+1}/H_i is always cyclic*
3. *all composition factors of G are of prime order*
4. *G has a chain of subgroups $1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_t = G$ such that each N_i is a normal subgroup of G and N_{i+1}/N_i is always Abelian.*

Problem 23. *Write a composition series for A_4 and deduce that A_4 is solvable.*

Problem 24. *Let Q_8 be the quaternion group of order 8. Q_8 is isomorphic to a subgroup of S_8, but not to any subgroup of S_n for $n \leq 7$.*

Problem 25. *If $H \leq G$ has finite index n then there is a normal subgroup K of G with $K \leq H$ and $|G : K| \leq n!$*

Problem 26. *Every non-Abelian group of order 6 has a non-normal subgroup of order 2. Classify groups of order 6.*

Problem 27. *No finite group G of composite order n with the property that G has a subgroup of order k for each positive integer k dividing n is simple.*

Problem 28. *If the center of G is of index n, then every conjugacy class has at most n elements.*

Problem 29. *Find all finite groups with exactly 2 conjugacy classes.*

Problem 30. *Let A be a nonempty set and let X be any subset of S_A. Let*

$$F(X) = \{a \in A \mid \sigma(a) = a \text{ for all } \sigma \in X\}$$

be the set of elements fixed by X. Correspondingly, $M(X) = A - F(X)$ are the elements moved by X. Let $D = \{\sigma \in S_A \mid |M(\sigma)| < \infty\}$. Then D is a normal subgroup of S_A.

Problem 31. *Let p be a prime and let G be a group of order p^α. Then G has a subgroup of order p^β for every β with $0 \leq \beta \leq \alpha$.*

Problem 32. *All groups of order 56 have a normal Sylow p-subgroup for some prime p dividing their order.*

Problem 33 (D&F 7.1.30)**.** *Let $A = \mathbb{Z} \times \mathbb{Z} \times \cdots$ be the direct product of copies of $\mathbb{Z}$ indexed by the positive integers (so A is a ring under componentwise addition and multiplication) and let R be the ring of all group homomorphisms from A to itself with addition pointwise and multiplication defined as function composition. Let ϕ be the element of R defined by $\phi(a_1, a_2, a_3, ...) = (a_2, a_3, ...)$. Let ψ be the element of R defined by $\psi(a_1, a_2, a_3, ...) = (0, a_1, a_2, a_3, ...)$*

1. *Prove that $\phi\psi$ is the identity of R but $\psi\phi$ is not the identity of R (i.e. ψ is a right, but not a left, inverse for ϕ).*

2. *Exhibit infinitely many right inverses for ϕ.*

3. *Find a nonzero element π in R such that $\phi\pi = 0$ but $\pi\phi \neq 0$.*

4. *Prove that there is no nonzero element $\lambda \in R$ such that $\lambda\phi = 0$ (i.e. ϕ is a left zero divisor but not a right zero divisor).*

Problem 34 (D&F 7.3.29)**.** *Let R be a commutative ring. Recall that an element $x \in R$ is nilpotent if $x^n = 0$ for some $n \in \mathbb{Z}^+$. Prove that the set of nilpotent elements from an ideal—called the nilradical of R and denoted $\eta(R)$.*

Problem 35 (D&F 7.3.33)**.** *Assume R is commutative. Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be an element of the polynomial ring $R[x]$.*

1. *Prove that $p(x)$ is a unit in $R[x]$ iff a_0 is a unit and $a_1, a_2, \ldots, a_n$ are nilpotent in R.*

2. *Prove that $p(x)$ is nilpotent in $R[x]$ iff $a_0, a_1, \ldots, a_n$ are nilpotent elements of R.*

Problem 36 (D&F 7.4.15)**.** *Let $x^2 + x + 1$ be an element of the polynomial ring $E = \mathbb{F}_2[x]$ and use the bar notation to denote passage to the quotient ring $\mathbb{F}_2[x]/(x^2 + x + 1)$.*

1. *Prove that $\overline{E}$ has 4 elements: $\bar{0}, \bar{1}, \bar{x}$, and $\overline{x+1}$.*

2. *Write out the 4×4 addition table for $\overline{E}$ and deduce that the additive group $\overline{E}$ is isomorphic to the Klein 4-group.*

3. *Write out the 4×4 multiplication table for $\overline{E}$ and prove that $\overline{E}^{\times}$ is isomorphic to Z_3. Deduce that $\overline{E}$ is a field.*

Problem 37 (D&F 7.4.27)**.** *Let R be a commutative ring with $1 \neq 0$. Prove that if a is a nilpotent element of R then $1 - ab$ is a unit for all $b \in R$.*

Problem 38 (D&F 7.4.30)**.** *Let I be an ideal of the commutative ring R and define*

$$\mathcal{R}(I) = \{r \in R \mid r^n \in I \text{ for some } n \in \mathbb{Z}^+\}$$

called the radical of I. Prove that $\mathcal{R}(I)$ is an ideal containing I and that $\mathcal{R}(I)/I$ is the nilradical of the quotient ring R/I, i.e. $\mathcal{R}/I = \eta(R/I)$.

Problem 39 (D&F 7.4.37)**.** *Prove that a subset X of $[0, 1]$ is a Zariski closed set iff it is closed in the usual sense as a subset of $\mathbb{R}$.*

Problem 40 (D&F 7.5.2)**.** *Let R be an integral domain and let D be a nonempty subset of R that is closed under multiplication. Prove that the ring of fractions $D^{-1}R$ is isomorphic to a subring of the quotient field of R (hence is also an integral domain).*

Problem 41 (D&F 8.1.3)**.** *Let R be a Euclidean domain. Let m be the minimum integer in the set of norms of nonzero elements of R. Prove that every nonzero element of norm m is a unit. Deduce that a nonzero element of norm zero (if such an element exists) is a unit.*

Problem 42 (D&F 8.1.7)**.** *Find a generator of the ideal $(85, 1 + 13i)$ in $\mathbb{Z}[i]$, i.e. a greatest common divisor for 85 and $1 + 13i$, by the Euclidean algorithm. Do the same for the ideal $(47 - 13i, 53 + 56i)$.*

Problem 43 (D&F 8.1.10)**.** *Prove that the quotient ring $\mathbb{Z}[i]/I$ is finite for any nonzero ideal I of $\mathbb{Z}[i]$*

Problem 44 (D&F 8.3.1)**.** *Let $G = \mathbb{Q}^{\times}$ be the multiplicative group of nonzero rational numbers. If $\alpha = p/q \in G$, where p and q are relatively prime integers, let $\varphi : G \to G$ be the map which interchanges the primes 2 and 3 in the prime power factorizations of p and q (so, for example, $\varphi(2^4 3^{11} 5^1 13^2) = 3^4 2^{11} 5^1 13^2$, $\varphi(3/16) = \varphi(3/2^4) = 2/3^4 = 2/81$, and φ is the identity on all rational numbers with numerators and denominators relatively prime to 2 and 3).*

1. *Prove that φ is a group isomorphism.*

2. *Prove that there are infinitely many isomorphisms of the group G to itself.*

3. *Prove that none of the isomorphisms above can be extended to an isomorphism of the **ring** $\mathbb{Q}$ to itself. In fact, prove that the identity map is the only ring isomorphism of $\mathbb{Q}$.*

Problem 45 (D&F 8.3.5)**.** *Let $R = \mathbb{Z}[\sqrt{-n}]$ where n is a squarefree integer greater than 3.*

1. *Prove that 2, $\sqrt{-n}$, and $1 + \sqrt{-n}$ are irreducible in R.*
2. *Prove that R is not a U.F.D. Conclude that the quadratic integer ring $\mathcal{O}$ is not a U.F.D. for $D \equiv 2, 3 \pmod 4$, $D < -3$ (so also not Euclidean and not a P.I.D.).*
3. *Give an explicit ideal in R that is not principal.*

Problem 46 (D&F 8.3.10a)**.** *Let R be an integral domain and let $N : R \to \mathbb{Z}^+ \cup \{0\}$ be a norm on R. The ring R is Euclidean with respect to N if for any $a, b \in R$ with $b \neq 0$, there exist elements q and r in R with*

$$a = qb + r \text{ with } r = 0 \text{ or } N(r) < N(b).$$

Suppose now that this condition is weakened, namely that for any $a, b \in R$ with $b \neq 0$, there exist elements q, q' and r, r' in R with

$$a = qb + r, b = q'r + r' \text{ with } r' = 0 \text{ or } N(r') < N(b),$$

i.e., the remainder after two divisions is smaller. Call such a domain a ***2-stage Euclidean domain.*** *Prove that iterating the divisions in a 2-stage Euclidean domain produces a greatest common divisor of a and b which is a linear combination of a and b. Conclude that every finitely generated ideal of a 2-stage Euclidean domain is principal.*

Problem 47 (D&F 8.3.11)**.** *Prove that R is a P.I.D iff R is a U.F.D. that is also a Bezout domain, that is, a domain in which every ideal generated by two elements is principal.*

Problem 48 (D&F 9.3.3)**.** *Let F be a field. Prove that the set R of polynomials in $F[x]$ whose coefficient of x is equal to 0 is a subring of $F[x]$ and that R is not a U.F.D.*

Problem 49 (D&F 9.3.4)**.** *Let $R = \mathbb{Z} + x\mathbb{Q}[x] \subseteq \mathbb{Q}[x]$ be the set of polynomials in x with rational coefficients whose constant term is an integer.*

1. *Prove that R is an integral domain and its units are ± 1.*
2. *Show that the irreducibles in R are $\pm p$ where p is a prime in $\mathbb{Z}$ and the polynomials $f(x)$ that are irreducible in $\mathbb{Q}[x]$ and have constant term ± 1. Prove that these irreducibles are prime in R.*
3. *Show that x cannot be written as the product of irreducibles in R (in particular, x is not irreducible) and conclude that R is not a U.F.D.*
4. *Show x is not prime in R and describe the quotient ring $R/(x)$.*

Problem 50 (D&F 9.4.1)**.** *Determine whether the following polynomials are irreducible in the rings indicated. For those that are reducible, determine their factorization into irreducibles. The notation $\mathbb{F}_p$ denotes the finite field $\mathbb{Z}/p\mathbb{Z}$, p a prime*

1. *$x^2 + x + 1$ in $\mathbb{F}_2[x]$.*
2. *$x^3 + x + 1$ in $\mathbb{F}_3[x]$.*
3. *$x^4 + 1$ in $\mathbb{F}_5[x]$.*

4. $x^4 + 10x^2 + 1$ *in* $\mathbb{Z}[x]$.

Problem 51 (D&F 10.1.8)**.** *An element m of the R-module M is called a **torsion element** if $rm = 0$ for some nonzero element $r \in R$. The set of torsion elements is denoted*

$$\operatorname{Tor}(M) = \{m \in M \mid rm = 0 \text{ for some nonzero } r \in R\}$$

1. *Prove that if R is an integral domain then $\operatorname{Tor}(M)$ is a submodule of M (called the **torsion** submodule of M).*

2. *Give an example of a ring R and an R-module M such that $\operatorname{Tor}(M)$ is not a submodule.*

3. *Show that if R has zero divisors then every nonzero R-module has torsion elements.*

Problem 52 (D&F 10.1.15)**.** *If M is a finite Abelian group then M is naturally a $\mathbb{Z}$-module. Can this action be extended to make M into a $\mathbb{Q}$-module?*

Problem 53 (D&F 10.2.6)**.** $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/(n,m)\mathbb{Z}$.

Problem 54 (D&F 10.3.2)**.** *Assume R is commutative. Prove that $R^n \cong R^m$ iff $n = m$, i.e. two free R-modules of finite rank are isomorphic iff they have the same rank.*

Problem 55 (D&F 10.3.9)**.** *An R-module M is called **irreducible** if $M \neq 0$ and if 0 and M are the only submodules of M. Show that M is irreducible iff $M \neq 0$ and M is a cyclic module with any nonzero element as a generator. Determine all the irreducible $\mathbb{Z}$-modules.*

Problem 56 (D&F 12.1.2)**.** *Let M be a module over the integral domain R.*

- *Suppose that M has rank n and that $x_1, x_2, \ldots, x_n$ is any maximal set of linearly independent elements of M. Let $N = Rx_1 + \cdots Rx_n$ be the submodule generated by $x_1, x_2, \ldots, x_n$. Prove that N is isomorphic to R^n and that the quotient M/N is a torsion R-module (equivalently, the elements $x_1, \ldots, x_n$ are linearly independent and for any $y \in M$ there is a nonzero element $r \in R$ such that ry can be written as a linear combination $r_1x_1 + \cdots + r_nx_n$ of the x_i).*

- *Prove conversely that if M contains a submodule N that is free of rank n (i.e., $N \cong R^n$) such that the quotient M/N is a torsion R-module then M has rank n.*

Problem 57 (D&F 12.1.4)**.** *Let R be an integral domain, let M be an R-module, and let N be a submodule of M. Suppose M has rank n, N has rank r, and the quotient M/N has rank s. Prove that $n = r + s$.*

Problem 58 (D&F 12.1.6)**.** *Show that if R is an integral domain and M is any non-principal ideal of R then M is torsion-free of rank 1 but is not a free R-module.*

Problem 59 (D&F 12.1.11)**.** *Let R be a P.I.D., let a be a nonzero element of R and let $M = R/(a)$. For any prime p of R prove that*

$$p^{k-1}M/p^kM \cong \begin{cases} R/(p) & \text{if } k \leq n \\ 0 & \text{if } k > n, \end{cases}$$

where n is the power of p dividing a in R.

Problem 60 (D&F 12.3.19)**.** *Prove that all $n \times n$ matrices with characteristic polynomial $f(x)$ are similar iff $f(x)$ has no repeated factors in its unique factorization over $F[x]$.*

Problem 61 (D&F 12.3.21). *Show that if $A^2 = A$ then A is similar to a diagonal matrix which has only 0's and 1's along the diagonal.*

Problem 62 (D&F 13.1.1). *Show that $p(x) = x^3 + 9x + 6$ is irreducible in $\mathbb{Q}[x]$. Let θ be a root of $p(x)$. Find the inverse of $1 + \theta$ in $\mathbb{Q}(\theta)$.*

Problem 63 (D&F 13.5.6). *Prove that $x^{p^n-1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times} (x - \alpha)$. Conclude that $\prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha = (-1)^{p^n}$ so the product of the nonzero elements of a finite field is $+1$ if $p = 2$ and -1 if p is odd. For p odd and $n = 1$ derive **Wilson's Theorem**: $(p-1)! \equiv -1 \pmod p$*

Problem 64 (D&F 13.5.8). *Prove that $f(x)^p = f(x^p)$ for any polynomial $f(x) \in \mathbb{F}_p[x]$.*

Problem 65 (D&F 13.5.9). *Show that the binomial coefficient $\binom{pn}{pi}$ is the coefficient of x^{pi} in the expansion of $(1+x)^{pn}$. Working over $\mathbb{F}_p$ show that this is the coefficient of $(x^p)^i$ in $(1+x^p)^n$ and hence prove that $\binom{pn}{pi} \equiv \binom{n}{i} \pmod p$.*