PROBLEMS FOR PRACTICE - FINAL

1. Groups

List of examples to recall:

- S_n = the symmetric group on n letters.
- D_{2n} = the dihedral group of size $2n$.
- C_n = cyclic group of size n, i.e, $C_n = \langle \sigma | \sigma^n = e \rangle \cong \mathbb{Z}/n\mathbb{Z}$.

(1) Consider the group S_n. Let $X = \{1, 2, \cdots, n\}$ be the set with n elements, on which S_n acts naturally. Let P be the set of two-element subsets of X. Fix $p = \{1, 2\} \in P$. Prove that $\mathrm{Stab}_{S_n}(p) \cong S_2 \times S_{n-2}$. Prove that the action of S_n on P (extended naturally from the S_n–action on X) is transitive (meaning: there is only one orbit). Conclude that $|P| = \begin{pmatrix} n \\ 2 \end{pmatrix}$.

(2) For $m, n \in \mathbb{Z}_{\geq 2}$ such that $\mathrm{g.c.d.}(m, n) = 1$, prove that we have an isomorphism of groups $C_{mn} \cong C_m \times C_n$. Prove or disprove: there is another isomorphism of groups: $\mathrm{Aut}_{\mathrm{group}}(C_{mn}) \cong \mathrm{Aut}_{\mathrm{group}}(C_m) \times \mathrm{Aut}_{\mathrm{group}}(C_n)$.

(3) State the classification theorem of finite abelian groups.

(4) Let G be a simple group (meaning: it has no non-trivial, proper, normal subgroups). If G is abelian, then prove that there is some prime $p \in \mathbb{Z}_{\geq 2}$ such that $G \cong C_p$. If G is not abelian, prove that $[G; G] = G$. Remember: we do not consider the trivial group $\{e\}$ as simple.

(5) Prove that there is no simple group with 126 elements.

(6) Let $p \in \mathbb{Z}_{\geq 2}$ be a prime number. Give an example of a non–abelian group with p^3 elements.

(7) Prove that $D_{2n} \cong C_n \rtimes_{\mathrm{Inv}} C_2$. Here $\mathrm{Inv} : C_2 \to \mathrm{Aut}_{\mathrm{group}}(C_n)$ is the group homomorphism that sends the non-trivial element of C_2 to $g \mapsto g^{-1}$ for every $g \in C_n$.

(8) Recall the presentation of the dihedral group:

$$D_{2n} = \langle \sigma, \rho | \sigma^2 = e = \rho^n \text{ and } \sigma\rho\sigma = \rho^{-1} \rangle.$$

Let $X = \{1, 2, \ldots, n\}$ and consider the following action of D_{2n} on X:

$$\rho(i) = i + 1 \text{ for } 1 \leq i \leq n - 1. \text{ And } \rho(n) = 1.$$

$$\sigma(k) = n - k + 1 \text{ for } 1 \leq k \leq n.$$

Prove that $\mathrm{Stab}_{D_{2n}}(1) \cong C_2$. Identify the non–trivial of this subgroup of D_{2n}.

(9) Let $p \in \mathbb{Z}_{\geq 2}$ be a prime number. Consider the group $G = \mathrm{GL}_2(\mathbb{F}_p)$ of 2×2 invertible matrices with entries from $\mathbb{F}_p$. What is the size (or order) of G? Give an example of a Sylow p–subgroup of G. Is your example a normal subgroup in G?

2. Rings

All rings considered below are commutative and unital. All rings homomorphisms are assumed to preserve identities.

(1) Prove that $\mathbb{Z}[x]$ is not a PID, but is a UFD.

(2) Prove that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

(3) Let K be a field and $f(x) \in K[x]$. Prove that $K[x]/(f)$ is a field if, and only if $f(x)$ is a non–zero irreducible polynomial.

(4) Assume that R is a ring such that $|R| < \infty$. Prove that every prime ideal in R is maximal.

(5) Compute the group of invertible elements (units) in $\mathbb{Q}[x]/(x^6)$.

(6) Let $n \in \mathbb{Z}_{\geq 2}$ and assume that $n = p_1^{a_1} \cdots p_r^{a_r}$ is the prime factorization of n. Prove that we have a ring isomorphism:

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{a_r}\mathbb{Z}$$

(7) Let $R = \mathbb{Z}/125\mathbb{Z}$. Prove that every element in R is either a unit or nilpotent. Recall the general statement and how we proved it: for a ring A, a maximal ideal $M \subsetneq A$, and $n \in \mathbb{Z}_{\geq 1}$, every element of $R = A/M^n$ is either a unit or invertible.

(8) Let R be a domain and $P \subsetneq R$ be a prime ideal. Prove that we have an injective ring homomorphism: $R_P \to F(R)$. Recall that $R_P = (R \setminus P)^{-1}(R)$ and $F(R) = (R \setminus \{0\})^{-1}(R)$ are obtained by inverting elements of R which are not in P, and non–zero elements of R, respectively.

(9) Prove that $\mathbb{Z}[\sqrt{-1}]$ is a Euclidean domain.

(10) Prove that $\mathbb{Z}[\sqrt{-3}]$ is not a UFD, by demonstrating that $(1+\sqrt{-3})(1-\sqrt{-3}) = 4 = 2 \times 2$ contradicts the uniqueness axiom of a unique factorization domain. Or, you can argue that 2 is an irreducible element, and yet (2) is not a prime ideal - a thing that is known to be true for UFD's. Recall $Z[\sqrt{-3}] \subsetneq \mathcal{O}(\sqrt{-3}) = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, the latter is a Euclidean domain, with the norm borrowed from complex numbers!

(11) Prove that every Euclidean domain is a UFD.

(12) State the Eisenstein criterion for checking irreducibility of a polynomial in one variable, with coefficients from a UFD.

(13) Let $f(x) \in k[x]$, where k is a field. Assume that the degree of $f(x)$ is 2 or 3. Prove that $f(x)$ is irreducible if, and only if $f(\alpha) \neq 0$ for every $\alpha \in k$. You may assume that $f(x)$ is monic, if you so wish.

(14) Let $p \in \mathbb{Z}_{\geq 2}$ be a prime number. Consider the polynomial $f(x) = x^p - x \in \mathbb{F}_p[x]$. Prove that $f(x) = \displaystyle\prod_{\alpha \in \mathbb{F}_p} (x - \alpha)$.

(15) Prove that $f(x) = x^3+3x^2+x+1 \in \mathbb{Z}[x]$ is irreducible. (Hint: a linear change $x \to x-a$ can get rid of $3x^2$ term. Determine this $a \in \mathbb{Z}$ and rewrite the polynomial in this new variable.) Which result states that the irreducibility property is same for $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ (under certain

obvious condition)?

(16) Prove that $x^2 + x + 1 \in \mathbb{F}_2[x]$ is irreducible.

(17) Let k be a field and let $k(x)$ be the field of rational functions of x with coefficients from k.

$$k(x) = \left\{ \frac{p(x)}{q(x)} \text{ such that } p(x), q(x) \in k[x] \text{ and } q(x) \neq 0 \right\}$$

Consider the following subring of $k(x)$:

$$R = \left\{ \frac{p(x)}{q(x)} \in k(x) \text{ such that } q(0) \neq 0 \right\}$$

Prove that R is a local ring, by explicitly writing its unique maximal ideal. This includes proving that the set that you have written, is indeed the uniqule maximal ideal. For extra credit: what is the set of prime ideals in R?

(18) Give an example of an ideal $I \subsetneq R$ of a ring R such that $\mathrm{Rad}\,(I) = I$ but I is not a primary ideal. *Hint: it will happen even for $R = \mathbb{Z}$.*

(19) Let $R = \mathbb{Q}[x, y, z]/(z^2 - xy)$ and let $P = (x, z) \subset R$. Prove that P is a prime ideal. Prove that P^2 is not primary.