MATH 502: HOMEWORK #1

DUE IN LECTURE THURSDAY, SEPT. 12, 2019.

I. Equivalence relations and the Euclidean algorithm.

1. Let $f : A \to B$ be a surjective map of sets. Prove that the relation $\dagger$ on the elements of A defined by $a \dagger b$ if and only if $f(a) = f(b)$ is an equivalence relation. Show that the equivalence classes of $\dagger$ are the fibers of f.

2. Use the Euclidean algorithm to show that if $a = 69$ and $n = 89$ then the residue class $[a]$ of a mod n defines an element in the group $(\mathbf{Z}/n)^*$ of invertible residue classes mod n. Find an integer b such that $[b]$ is the inverse of $[a]$ in $(\mathbf{Z}/n)^*$.

II. Group actions and some examples of groups.

3. Determine which of the following binary operation are (a) associative, (b) commutative.
   i. the operation $*$ on $\mathbf{Z}$ defined by $a * b = a - b$.
   ii. the operation $*$ on $\mathbf{R}$ defined by $a * b = a + b + ab$.
   iii. The operation $*$ on $\mathbf{Q}$ defined by $a * b = \frac{a+b}{5}$.
   iv. The operation $*$ on $\mathbf{Z} \times \mathbf{Z}$ defined by $(a, b) * (c, d) = (ad + bc, bd)$.
   v. the operation $*$ on $\mathbf{Q} - \{0\}$ defined by $a * b = \frac{a}{b}$.

4. Which of the following sets are groups under addition?
   i. the set of rational numbers (including $\frac{0}{1}$) in lowest terms whose denominators are odd.
   ii. the set of rational numbers (including $\frac{0}{1}$) in lowest terms whose denominators are even.
   iii. the set of rational numbers of absolute value ≤ 1.
   iv. the set of rational numbers of absolute value ≥ 1 together with 0.
   v. the set of rational numbers with denominators equal to 1 or 2.
   vi. the set of rational numbers with denominators equal to 1, 2 or 3.

5. Let $G = \{a + b\sqrt{2} \in \mathbf{R} : a, b \in \mathbf{Q}\}$.
   i. Show that G is an abelian group under addition.
   ii. Show that the set $G - \{0\}$ of non-zero elements of G is a group under multiplication. (Hint: Rationalize denominators.)

6. Show that if G is a group such that $x^2 = 1$ for all $x \in G$ then G is abelian.

III. Galois groups.

7. Let S_n be the symmetric group on $n \geq 1$ letters. Define $\mathbf{Z}[X_1, \ldots, X_n]$ to be the set of polynomials $F = F(X_1, \ldots, X_n)$ with integer coefficients in the commuting indeterminates $X_1, \ldots, X_n$. For $s \in S_n$, define $(sF) = (sF)(X_1, \ldots, X_n)$ to be the polynomial $F(X_{s(1)}, \ldots, X_{s(n)})$. So, for example, if $F(X_1, \ldots, X_n) = X_i$, then $(sF)(X_1, \ldots, X_n) = X_{s(i)}$.
   i. Show that $s(F + G) = sF + sG$ and $s(F \cdot G) = (sF) \cdot (sG)$ if $F, G \in \mathbf{Z}[X_1, \ldots, X_n]$, where $F + G$ and $F \cdot G$ are the usual sum and product of polynomials.

ii. Show that the map $S_n \times \mathbf{Z}[X_1, \ldots, X_n] \to \mathbf{Z}[X_1, \ldots, X_n]$ defined by $(s, F) \to sF$ defines an action of S_n on $\mathbf{Z}[X_1, \ldots, X_n]$, in the sense that $eF = F$ when e is the identity permutation, and $(st)(F) = s(tF)$ for all $s, t \in S_n$ and $F \in \mathbf{Z}[X_1, \ldots, X_n]$. (Hint: You could use part (i) to reduce to the case in which $F = X_i$ for some i.)

8. Suppose $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_0$ is a monic polynomial with integer coefficients a_i. Write $f(x) = (x - b_1) \cdots (x - b_n)$, where the b_i are complex numbers, and assume the b_i are distinct. Let T be the set of all complex numbers of the form $F(b_1, ..., b_n)$ in which $F = F(X_1, ..., X_n)$ is an element of $\mathbf{Z}[X_1, \ldots, X_n]$. Note that T contains the set of all integers $\mathbf{Z}$, since $F(X_1, ..., X_n)$ can be a constant polynomial. One can define the Galois group $G(f)$ of $f = f(x)$ to be the set of all permutations s of $\{1, ..., n\}$ such that there is a permutation t_s of T such that

(1) $$t_s(F(b_1, \ldots, b_n)) = F(b_{s(1)}, \ldots, b_{s(n)})$$

for all $F(X_1, ..., X_n)$ as above. Note that with the action of S_n on $\mathbf{Z}[X_1, \ldots, X_n]$ defined in problem # 6, we have

(2) $$F(b_{s(1)}, \ldots, b_{s(n)}) = (sF)(b_1, \ldots, b_n)$$

i. Show that the equality $t_s(F(b_1, ..., b_n)) = F(b_{s(1)}, ..., b_{s(n)})$ for all $F(X_1, ..., X_n)$ as above implies t_s fixes each integer, i.e. $t_s(m) = m$ for $m \in \mathbf{Z}$.

ii. Prove that the identity permutation, which fixes each element of $\{1, \ldots, n\}$, lies in $G(f)$.

iii. Suppose that $s \in G(f)$, so that a t_s as above exists. Show s^{-1} lies in $G(f)$. (Hint: You want to show that there is a bijection $t' : T \to T$ such that for each polynomial $H(X_1, \ldots, X_n)$, one has $t'(H(b_1, ..., b_n)) = H(b_{s^{-1}(1)}, ..., b_{s^{-1}(n)})$. Try setting t' equal to the inverse of t_s, and applying (1) to the polynomial $F = s^{-1}H$ in the sense of problem # 7.)

iv. Show that $G(f)$ is a subgroup of the symmetric group S_n of all permuations of $\{1, \ldots, n\}$.

9. Show that the Galois group of $f(x) = x^2 - 2$ is of order 2.

IV. Isometry groups.

10. Show that an isometry $f : \mathbf{R}^n \to \mathbf{R}^n$ which preserves the origin must be linear, i.e. must be represented by multiplication by some matrix. Deduce that $\text{Isom}(\mathbf{R}^n)$ is generated by the group T_n of translations and the orthogonal group $O(n, \mathbf{R})$.

11. Let M be a finite non-empty subset of the Euclidean plane $\mathbf{R}^2$. Give M the Euclidean metric d_M. Show that an element f of $\text{Isom}(M, d_M)$ of order greater than 2 must be the restriction of a rotation about some point of $\mathbf{R}^2$. (Hint: Show there is an $m \in M$ so m, $f(m)$ and $f^2(m)$ are distinct. Consider the possibilities for $f^3(m)$. To what extent is f determined by its action on m, $f(m)$ and $f^2(m)$?)

12. *Bonus Problem (optional)*: With the notations of problem #11, describe the isomorphism classes of groups which can arise as $Isom(M, d_M)$ for some finite non-empty set of points M in $\mathbf{R}^2$.