373K Algebra I, Homework 13

From Artin

Chapter 12 (pages 379–381) 2.1, 2.4, 2.9, 4.1, 4.2, 4.9, 4.12, 5.1, 5.3.

Others:

1. Prove that in a P.I.D., a prime ideal is maximal.

2. Let R be a commutative ring with 1, and $a \in R$. Define $I_a = \{x \in R : ax = 0\}$.

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

(b) Take $R = \mathbf{Z}/100\mathbf{Z}$. Compute $I_{[25]}$ and $I_{[3]}$.

3. Construct a finite field with 25 elements.

4. $\alpha \in \mathbf{C}$ is called an *algebraic number* if there exists a polynomial $p(x) \in \mathbf{Z}[x]$ with $p(\alpha) = 0$. α is called an *algebraic integer* if the polynomial $p(x)$ is monic.

(a) Prove that the set of algebraic numbers forms a subfield (denoted by $\mathbf{F}$) of $\mathbf{C}$, and the the set of algebraic integers forms a subring of $\mathbf{F}$.

(b) What are the algebraic integers in $\mathbf{Q}(i) = \{a + bi : a, b \in \mathbf{Z}\}$ and $\mathbf{Q}(\sqrt{5}) = \{a + b\sqrt{5} : a, b \in \mathbf{Z}\}$?

5. Prove that the function $\mathbf{C} \to \{\text{maximal ideals in } \mathbf{C}[x]\}$ given by $a \mapsto < x - a >$ is a bijection.

6. Let R be commutative ring with 1, and $P \subset R$ a prime ideal. Prove that if there are ideals $I, J \subset R$ such that $IJ \subset P$, then $I \subset P$ or $J \subset P$.

Extra question for the keen

Referring to the notes in the attachment along with HW 13:

7. How many different necklaces with 7 beads can be made with 3 colors?

9. Let G be any group and $H \leq G$. Recall for $x \in G$, $cls(x) = \{gxg^{-1} \mid g \in G\}$.
  i) If G is finite and $H \neq G$, show that there is $x \in G$ so that $cls(x) \cap H = \emptyset$.
  ii) Show G infinite and $[G : H] = n > 1 \Rightarrow cls(x) \cap H = \emptyset$ for some $x \in G$.

9.2 COUNTING ORBITS

The basic problem we consider is akin to the necklace problem mentioned above. How many different necklaces can be made using n beads of k possible colors? To analyze this problem mathematically, fix the positions of the beads as the vertices of the regular n-gon P_n. Each necklace corresponds to specifying an allowable color for each vertex. We might guess there are k^n necklaces: choose any color for each of the n vertices. However, different colorings can give the same necklace. For example, if all the vertices but one are colored green and the remaining vertex is colored blue, these n different colorings all correspond to the one necklace with one blue bead and all other beads green. If instead two vertices are blue and the others are green then all colorings with adjacent blue vertices give the same necklace, but all colorings with the two blue vertices separated by a single green vertex give another necklace, assuming $n > 3$.

Each coloring corresponds to a necklace but different colorings may give the same necklace. Identifying all colorings giving the same necklace clearly partitions the set of all colorings into subsets corresponding to the different necklaces. How can we count the number of sets in the partition and how are group actions used? Suppose we are given two colorings and their corresponding necklaces. The necklaces are the same if we can rotate one or turn it over to match the other. These actions correspond to taking one coloring of P_n and applying elements of D_n to the colored vertices of P_n to see whether we can get the other coloring. Thus the number of necklaces, or subsets in the partition of all colorings, will be the number of orbits of D_n acting on the set of colorings by permutation of the colored vertices of P_n. This explanation will suffice for the applications we will consider, but we will discuss briefly how to make all of this mathematically precise.

Let G be a group (D_n above) acting on a set S(P_n above), and let A be the set of colorings of S using k colors. We need a mathematical way to describe the colorings. Any coloring in A is an assignment of each $s \in S$ to an allowable color. Letting $I(k) = \{1, 2, \ldots, k\}$ represent the colors, each $a \in A$ is a function $a : S \to I(k)$, so $A = I(k)^s = \{f : S \to I(k)\}$. For $a, b \in A$, set $a \sim b$ if for some $g \in G$, $b(gs) = a(s)$ for all $s \in S$. This means that the coloring b is related to a when it is obtained from a by some permutation of the (colored!) elements of S. That is, $a \sim b$ when there is some $g \in G$ so that the coloring b is defined by giving gs the color $a(s)$ for all $s \in S$. It is an exercise to show that this is an equivalence relation on A. When $S = P_n$ as above, this relation identifies colorings corresponding to the same necklace since $a \sim b$ when for some $g \in D_n$ the color that b assigns to vertex gv_j is the same color that a assigns to vertex v_j. Thus if the necklace corresponding to the coloring a is rotated or turned over by applying $g \in D_n$, the result is the necklace corresponding to the coloring b. Consequently, the equivalence classes of $\sim$ correspond to those colorings in A that are essentially different.

How do we get G to act on A? Let $g \cdot a \in A$ be the coloring given by $g \cdot a(s) = a(g^{-1}s)$. It might seem more natural to use $g \cdot a(s) = a(gs)$ but because of our notation for functions, this will not quite give a group action. We use that G acts on S, take $a \in A$, and compute $g \cdot (h \cdot a)(s) = h \cdot a(g^{-1}s) = a(h^{-1}(g^{-1}s)) = a(h^{-1}g^{-1}s) = a((gh)^{-1}s) = gh \cdot a(s)$ for all

$s \in S$, so $g \cdot (h \cdot a) = gh \cdot a$, and also $e \cdot a(s) = a(es) = a(s)$ so $e \cdot a = a$. Thus G acts on / Now G acts like a set of bijections of S by Theorem 9.1, so for $g \in G$, $S = gS$ and if $s =$; then $g \cdot a(gt) = a(t)$ for all $t \in S$. Hence $a \sim g \cdot a$ as above. When $a \sim b$ then for sor $g \in G$ and all $s \in S$, $b(gs) = a(s) = a(g^{-1}gs) = g \cdot a(gs)$, and with $S = gS$ gives $b = g \cdot$ (Therefore the equivalence classes of $\sim$ on A are the same as the orbits of G acting on / so the following are the same: the number of essentially different colorings, the number (equivalence classes of $\sim$ on A, and the number of orbits of G on A.

Clearly, counting the orbits for a group action will solve coloring problems like tl one mentioned above about necklaces. It turns out that this number is the average numb(of fixed points per group element.

THEOREM 9.7 Let G be a finite group acting on the finite set S. The number of orbits for this action is $m = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|$.

Proof Now $|Fix(g)|$ counts the elements of S fixed by $g \in G$, so $\sum_{g \in G} |Fix(g)|$ counts th total number of times elements of S are fixed by elements of G, summed over S. Since s S is represented in the sum $|stab(s)|$ times, $\sum_{g \in G} |Fix(g)| = \sum_S |stab(s)|$. : $T = \{s_1, \ldots, s_m\}$ is a transversal for the orbits of G acting on S then by Theorem 9.: $|stab(s)| = |stab(s_j)|$ when $s \in orb(s_j)$, and also $|orb(s_i)| = [G : stab(s_i)]$. Therefor $\sum_S |stab(s)| = \sum_i |stab(s_i)|[G : stab(s_i)] = \sum_i |G| = m|G|$, using Lagrange's Theoren so $m = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|$ as claimed.

How can we count fixed points for coloring problems? If G acts on S, and on th colorings A of S by permuting S, then for $g \in G$, $a \in Fix(g) \Leftrightarrow a(s) = g \cdot a(s) = a(g^{-1}s)$ s s and $g^{-1}s$ have the same color in a, for all $s \in S$. It follows that all $g^i s$ have the same color i a. Consider $\langle g \rangle$ acting on S, with orbits $orb_{\langle g \rangle}(s)$. Our observation means that all elements i $orb_{\langle g \rangle}(s)$ have the same color in a. Conversely, if for all $s \in S$, all $t \in orb_{\langle g \rangle}(s)$ have the sam color under $a \in A$, then $a \in Fix(g)$. Hence $|Fix(g)| = k^{\lambda(g)}$ where k is the number of availabl colors and $\lambda(g)$ is the number of orbits of $\langle g \rangle$ acting on S. This observation and Theorem 9. give the method for computing different colorings. We state it as a theorem for reference.

THEOREM 9.8 Let the finite group G act on the finite set S and let A be the set of colorings of S using k colors. For $g \in G$, let $\lambda(g)$ be the number of orbits of S under the action of $\langle g \rangle$. If G acts on A by permutation of S then the number of orbits of G acting o: A is $\frac{1}{|G|} \sum_{g \in G} k^{\lambda(g)}$.

Let us see how to use Theorem 9.8.

Example 9.3 A square made of nine equal smaller squares is painted on a piece o wood with each small square painted either red or white. How many paintings ar possible?

By Theorem 9.8 the number of colors does not affect the method of computation so suppose k colors are available. Number the small squares in each row from left t