Homework (*required*):

Prepare for the midterm:

- Reread the assigned sections of Artin.
- Review assigned homework problems and solutions.
- Try the practice midterm included in this document
  (and check your answers against the solutions
  also included in this document).
- Try other problems from the relevant sections of Artin

Practice Midterm 2 Math 122/E222

(1) Let G be a group acting on a set S. Define the *stabilizer* of $s \in S$.

Let G be the group of motions of the plane, and let p be a point in the plane. What is the stabilizer of p in G?

(2) Let G be a finite group. What does it mean for G to be a p*-group*?

Suppose G is a finite p-group. Show that the center of G is nontrivial.

(3) Let G be a finite group of order n, and let F be any field. Prove that G is isomorphic to a subgroup of $GL_n(F)$.

(4) State the *Sylow theorems* for a finite group G of order $p^e a$ where $p \nmid a$ and $e \geq 1$.

Prove that if G has composite order $n = p^e a$ where $1 \leq a < p$ and $e \geq 1$, then G has a proper nontrivial normal subgroup.

(5) Let R be a commutative ring. Define the *unit group* of R.

Let F be a field and let $R = F[X]$ be the ring of polynomials in one variable with coefficients in F. Determine the unit group of R.

(6) Let R be a commutative ring. What does it mean for $I \subset R$ to be an *ideal*?

Let $f : R \to R'$ be a ring homomorphism. Prove that if J is an ideal of R' then

$$f^{-1}(J) = \{r \in R \,:\, f(r) \in J\}$$

is an ideal of R. Show that if f is surjective then for any ideal I of R,

$$f(I) = \{f(r) \in R' \,:\, r \in R\}$$

is an ideal of R'. Find an example to demonstrate that $f(I)$ need not be an ideal if f is not surjective.

Solutions

(1) The stabilizer of $s \in S$ is the subgroup

$$G_s := \{g \in G \,:\, g \cdot s = s\}\,.$$

Now if G is the group of motions in the plane and p is a point in the plane, then

$$G_p = G_{t_p(0)} = t_p G_0 t_p^{-1},$$

where 0 is the origin and t_p is the translation taking the origin to p. Now the set of motions that stabilize the origin is $O(2)$, so the stabilizer of p is

$$t_p O(2) t_p^{-1}.$$

(2) A p-group G is a group of order p^e where $e \geq 1$. If G is a finite p-group with conjugacy class $C_1, \ldots, C_n$, then we may consider its class equation

$$|G| = \sum_{i=1}^{n} |C_i|.$$

Recall that $|C_i| = [G : Z_i]$ where Z_i is the centralizer in G of any element of C_i. It follows that $|C_i|$ divides $|G| = p^e$, and hence is a power of p too.

Now the identity element forms its own conjugacy class, so in the class equation, if every conjugacy class has size p^r with $r \geq 1$, we have

$$p^e = 1 + \sum (\text{nontrivial powers of } p),$$

which is impossible. Thus some conjugacy class has order 1, and the element x of that conjugacy class must be in the center.

(3) G acts on itself by left multiplication: $g \cdot x = gx$. Thus every element of G defines a permutation of G, and we have a homomorphism

$$\rho : G \to S_n$$
$$g \mapsto (\text{permutation defined by } g).$$

ρ is injective since the only element of G which fixes elements under left multiplication is the identity.

Moreover, there is a natural injective homomorphism

$$\varphi : S_n \to GL_n(F)$$

$$\sigma \mapsto (\text{permutation matrix associated to } \sigma).$$

Composing $\phi \circ \rho$ we obtain an injection $G \to GL_n(F)$; its image is a subgroup of $GL_n(F)$ isomorphic to G.

(4) Let $n_p(G)$ denote the number of Sylow p-subgroups, we have that

$$n_p(G) \equiv 1 \bmod p \text{ and } n_p(G)|a.$$

Since $1 \leq a < p$, we have $1 \leq n_p(G) < p$, and so $n_p(G)$ is 1. Hence there is a unique Sylow p-subgroup and it is normal.

(5) The unit group of R is the group of elements of R which have multiplicative inverses:

$$R^\times = \{a \in R : \text{there is } b \in R \text{ s.t. } ab = 1\}.$$

Now letting $R = F[X]$ for some field F, we observe that if $f, g \in F[X]$,

$$\deg(fg) = \deg(f) + \deg(g)$$

where $\deg$ of a polynomial is its degree. Thus if f is a unit with inverse g, we must have $\deg(f)+\deg(g) = 0$, and since degrees are nonnegative, it follows that f and g are just constant polynomials. Conversely, any nonzero constant polynomial is invertible since F is a field. Hence

$$R^\times = F^\times = F - \{0\}.$$

(6) An ideal is a subset $I \subset R$ which is a subgroup of $(R, +)$ and which is stable under multiplication by every element of R. Letting $f : R \to R'$ be a ring homomorphism and J an ideal of R', we see that given $x, y \in f^{-1}(J)$, $f(x - y) = f(x) - f(y) \in J$ so $x - y \in f^{-1}(J)$, from which it's immediate that $f^{-1}(J)$ is a subgroup of $(R, +)$. Moreover, if $r \in R$ and $x \in f^{-1}(J)$, then $f(rx) = f(r)f(x) \in J$, and so $rx \in f^{-1}(J)$, so $f^{-1}(J)$ is stable under multiplication by R.

Similarly, given an ideal I of R, $f(I)$ is an subgroup of R'. If moreover f is surjective, then for any $r' \in R'$, there is $r \in R$ with $f(r) = r'$ and so given $x' = f(x) \in f(I)$, we have $r'x' = f(r)f(x) = f(rx) \in f(I)$, thus showing that $f(I)$ is an ideal. However, the assumption that f is surjective is essential; for example, if $f : \mathbb{Z} \to \mathbb{Q}$ is the natural embedding, then $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$ but not of $\mathbb{Q}$.