Silvain Rideau silvain.rideau@berkeley.edu
1091 Evans `www.normalesup.org/~srideau/en/teaching`

Solutions to the midterm

October 30th

Problem 1 :
Let R be a ring and $I, J \subseteq R$ be two ideals. Using only the definitions and nothing we have proved in class:

1. Show that $I \cap J$ is an ideal of R.

   Solution: Let us first shoz that $I \cap J$ is a subgroup of $(R, +)$. If $x, y \in I \cap J$, then $x - y \in I$ and $x - y \in J$ since both are additive subgroups of R. It follows that $x - y \in I \cap J$, as required. Let us now consider $x \in I \cap J$ and $a \in R$. Then $a \cdot x$ and $x \cdot a$ are both in I and J since they are ideals and hence they are in $I \cap J$.

2. Assume R to be a commutative ring and I, J comaximal. Show that $I \cdot J = I \cap J$.

   Solution: Recall that $I \cdot J = \{\sum_i a_i b_i : a_i \in I \text{ and } b_i \in J\}$. Let us first prove that $I \cdot J \subseteq I \cap J$. Pick any $a_i \in I$ and $b_i \in J$. Then $a_i \cdot b_i$ is in both I and J since they are ideals and hence $sum_i a_i b_i \in I \cap J$. Conversely, if $x \in I \cap J$, since I and J are comaximal $I + J = R$ and there exists $u \in I$ and $v \in J$ such that $u + v = 1$. Then $x = x \cdot 1 = x \cdot (u + v) = u \cdot x + x \cdot v$. Since $u, x \in I$ and $x, v \in J$, $x = u \cdot x + x \cdot v \in I \cdot J$.

Problem 2 :
Let R be an integral domain.

1. Let $\varphi : R \to S$ be a ring homomorphism. We define $\psi : R[X] \to S[X]$ by $\psi(\sum_{i=0}^n a_i X^i) = \sum_{i=0}^n \varphi(a_i) X^i$. Show that ψ is a ring homomorphism.

   Solution: We have:

$$\begin{array}{rcl} \psi(\sum_{i=0}^n a_i X^i + \sum_{i=0}^n b_i X^i) & = & \psi(\sum_{i=0}^n (a_i + b_i) X^i) \\ & = & \sum_{i=0}^n \varphi(a_i + b_i) X^i \\ & = & \sum_{i=0}^n \varphi(a_i) + \varphi(b_i) X^i \\ & = & \sum_{i=0}^n \varphi(a_i) X^i + \sum_{i=0}^n \varphi(b_i) X^i \\ & = & \psi(\sum_{i=0}^n a_i X^i) + \psi(\sum_{i=0}^n b_i X^i) \end{array}$$

   also:

$$\begin{array}{rcl} \psi(\sum_{i=0}^n a_i X^i \cdot \sum_{i=0}^n b_i X^i) & = & \psi(\sum_{k=0}^{2n} (\sum_{i+j=k} a_i \cdot b_j) X^k) \\ & = & \sum_{i=k}^{2n} \varphi(\sum_{i+j=k} a_i \cdot b_j) X^k \\ & = & \sum_{i=k}^{2n} \sum_{i+j=k} \varphi(a_i) \cdot \varphi(b_i) X^k \\ & = & (\sum_{i=i}^n \varphi(a_i) X^i) \cdot (\sum_{i=0}^n \varphi(b_i) X^i) \\ & = & \psi(\sum_{i=0}^n a_i X^i) \cdot \psi(\sum_{i=0}^n b_i X^i) \end{array}$$

   and finally:

$$\begin{array}{rcl} \psi(1X^0) & = & \varphi(1) X^0 \\ & = & 1X^0 \end{array}$$

2. For all $P = \sum_{i=0}^{n} a_i X^i \in R[X] \setminus \{0\}$, we define $v(P) = \min\{i : a_i \neq 0\}$. Show that, for all $P, Q \in R[X] \setminus \{0\}$, $v(P \cdot Q) = v(P) + v(Q)$.

   Solution: Let $P = \sum_{i=0}^{n} a_i X^i$, $Q = \sum_{i=0}^{m} b_i X^i$ and $P{\cdot}Q = \sum_{k=0}^{n+m} c_k X^k$, where $c_k =\sim_{i+j=k} a_i b_j$. Let $p = v(P)$ and $q = v(Q)$. If $k < p + q$, then whenever $i + j < p$, then either $i < p$ or $j < q$. It follows that either $a_i = 0$ or $b_i = 0$ and hence $c_k = 0$, so $v(P \cdot Q) \geqslant p + q$. Now $c_{p+q} = \sum_{i+j} a_i b_j$. As before, id $i < p$ $a_i = 0$ and if $j < q$, $b_j = 0$, so $c_{p+q} = a_p b_q$. Since R is an integral domain and $a_p, b_q \neq 0$, $c_k = a_p b_q \neq 0$.

3. Let $P, Q \in R[X]$ be such that $P \cdot Q = aX^n$ for some $a \in R \setminus \{0\}$ and $n \in \mathbb{Z}_{\geqslant 0}$. Show that there exists $r, s \in R$ and $i, j \in \mathbb{Z}_{\geqslant 0}$ such that $P = rX^i$ and $Q = sX^j$.

   Solution: We have $n = v(aX^n) = v(P \cdot Q) = v(P) + v(Q)$ and $n = \deg(aX^n) = \deg(P \cdot Q) = \deg(P) + \deg(Q)$. Since $0 \leqslant v(P) \leqslant \deg(P)$ and similarly for Q, it follows that $v(P) = \deg(P)$ and $v(Q) = \deg(Q)$. Thus $P = rX^i$ for some $r \in R$ and $i = \deg(P) = v(P)$. Similarly for Q.

Problem 3 :
Let G be a finite group.

1. For all $x \in G$ of order n, show that the action of $\langle x \rangle$ on G by multiplication on the left — i.e. $x^i \star g = x^i \cdot g$ — has $|G|/|x|$ orbits and they are all of size $|x|$.

   Solution: Note that the orbit of any $g \in G$ is exactly the coset of $\langle x \rangle g \subseteq G$. As we showed in class, all cosets are of size $|\langle x \rangle| = |x|$ and there are $[G : \langle x \rangle] = |G|/|x|$ of them.

   We can also reprove that directly by showing that for all $g \in G$, $\mathrm{Stab}_{\langle x \rangle}(g) = \{x^i : x^i \cdot g = g\} = \{x^i : x^i = 1\} = \{1\}$. So, the cardinal of the orbit of G is equal $|\langle x \rangle|/|\mathrm{Stab}_{\langle x \rangle}(g)| = |x|$. Since the orbits form a partition of G, if we have n of them, we have $n \cdot |x| = |G|$, i.e. $n = |G|/|x|$.

2. Let $f : G \to \{\mathbb{Z}/2\mathbb{Z}\}$ be such that $f(x) = \overline{1}$ if and only if $|x|$ is even and $|G|/|x|$ is odd. Show that f is a group homomorphism.

   Hint: Think about the signature of a permutation.

   Solution: Let $\rho : G \to S_G$ the permutation representation associated with left multiplication. Then the orbits of the action of $\langle x \rangle$ on G exactly correspond to the disjoint cycle decomposition of $\rho(x)$. It follows that if $\varepsilon : S_G \to \mathbb{Z}/2\mathbb{Z}$ denotes the signature, then $f = \varepsilon \circ \rho$ which is indeed a group homomorphism.

3. Assume $|G| = 2n$ where n is odd. Show that there exists a normal subgroup of G of index 2.

   Solution: By Cauchy's theorem, there exists $x \in G$ of order 2. Then $|x|$ is even and $|G|/|x| = n$ is odd. So $f(x) = \overline{1}$ and f is surjective. It now follows from the first isomorphism that $\ker(f)$ is a normal subgroup of G and that $G/\ker(f) \cong \mathbb{Z}/2/Zz$, i.e. $[G : \ker(f)] = 2$.