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

Solutions to homework 10

Due November 29th

Problem 1 :

1. Let $P_n = X^n - 1$. Let $\mu_n \subseteq \mathbb{C}$ be the set of roots of P_n in $\mathbb{C}$. The elements of μ_n are called the n-th roots of the unity. Show that

$$P_n = \prod_{\zeta\in\mu_n} X - \zeta.$$

Solution: Since each element of μ_n is a root of P_n, the polynomial $\prod_{\zeta\in\mu_n} X - \zeta$ divides P_n. But $\mu_n = \{e^{\frac{2ik\pi}{n}} : 0 \leqslant k < n\}$ has size n so those two polynomials have the same degree. It follows that there exists $u \in \mathbb{C}^\star$ such that $P_n = u \cdot \prod_{\zeta\in\mu_n} X - \zeta$. But the coefficient of X^n in both P_n and $\prod_{\zeta\in\mu_n} X - \zeta$ is 1, so $u = 1$ and $P_n = \prod_{\zeta\in\mu_n} X - \zeta$.

Note that μ_n is in fact a cyclic subgroup of $\mathbb{C}^\star$.

2. A $\zeta \in \mu_n$ is said to be primitive if it is not a d-th root of the unity for any $d < n$. Show that there are $\varphi(n)$ primitive n-th roots of the unity, where $\varphi(n)$ is Euler's totient function.

Solution: Pick $\zeta = e^{\frac{2ik\pi}{n}} \in \mu_n$. It is a root of P_d for some $d < n$ if and only if $l := \gcd(n, k) \neq 1$ (and in that case it is a root of $P_{\frac{n}{l}}$). Indeed $\zeta^{\frac{n}{l}} = e^{\frac{2ik\pi}{n}\cdot\frac{n}{l}} = e^{\frac{2ik\pi}{l}} = 1$ if and only if $\frac{k}{l} \in \mathbb{Z}$. Since $\varphi(n)$ is, by definition, the number of $0 \leqslant k < n$ that are coprime with n, we do have $\varphi(n)$ primitive n-th roots of the unity.

3. Let

$$\Phi_n(X) = \prod_{\zeta\in\mu_n \text{ primitive}} X - \zeta.$$

Show that $P_n = \prod_{d|n} \Phi_d$. Conclude that $\Phi_n(X) \in \mathbb{Z}[X]$.

Solution: Pick any $\zeta \in \mu_n$, Let $d|n$ be the order of ζ. Then ζ is a primitive d-th root of the unity. Note also that ζ is a primitive d-th root for a unique d so μ_n is the disjoint union of $\mu_{n,d} = \{\zeta \in \mu_n : \zeta \text{ is a primitive } d\text{-th root}\}$ for $d|n$. So $P_n(X) = \prod_{d|n} \prod_{\zeta\in\mu_{n,d}} (X - \zeta)$. Note also that if $d|n$ and ζ is a d-th root of the unity (primitive or not), then $\zeta^n = 1$, so all primitive d-th roots of the unity are in $\mu_{n,d}$ and $\prod_{\zeta\in\mu_{n,d}} (X - \zeta) = \Phi_d(X)$ by definition. It follows that $P_n = \prod_{d|n} \Phi_d$.

Let us first prove that if $P = UV$ where $P, U \in \mathbb{Q}[X]$ and $V \in \mathbb{C}[X]$, then $V \in \mathbb{Q}[X]$. Indeed, let $P = UV' + R$ be its Euclidean division in $\mathbb{Q}[X]$, then it also a Euclidean division in $\mathbb{C}[X]$. But $P = UV$ is also a Euclidean division in $\mathbb{C}[X]$ and we saw that Euclidean division in $\mathbb{C}[X]$ is unique. It follows that $V = V' \in \mathbb{Q}[X]$.

Because $\Phi_n \prod_{d|n,d<n} \Phi_d = P_n \in \mathbb{Q}[X]$, we obtain, by induction on n, that $\Phi_n \in \mathbb{Q}[X]$ for all n. It now follows from Gauss's lemma (and induction), that there exists $c_d \in \mathbb{Q}^\star$ such that $c_d\Phi_d \in \mathbb{Z}[X]$ and $\prod_{d|n} c_d\Phi_d = P_n$. It follows (looking at he coefficient of X^n), that $\prod_{d|n} c_d = 1$. Note also that, since the coefficient of $X^{|\mu_d|}$ in $c_d\Phi_d$ is c_d, we must have that $c_d \in \mathbb{Z}$ and hence, each of the c_d is invertible in $\mathbb{Z}$. It follows that $\Phi_n = c_n^{-1}c_n\Phi_n \in \mathbb{Z}[X]$.

4. (Harder) Let p be a prime number. Show that $\Phi_p(X+1)$ is irreducible in $\mathbb{Z}[X]$. Conclude that Φ_p is irreducible in $\mathbb{Z}[X]$.

   Solution: We have $P_p = X^p - 1 = (X-1)\sum_{i=0}^{p-1} X^i = \Phi_1 \cdot \Phi_p$ so $\Phi_p = \sum_{i=0}^{p-1} X^i = \frac{X^p-1}{X-1}$. So $\Phi_p(X+1) = \frac{(X+1)^p-1}{X} = \frac{\sum_{i=0}^{p}\binom{p}{i}X^i-1}{X} = \sum_{i=0}^{p-1}\binom{p}{i+1}X^i$. The dominant coefficient is $\binom{p}{p} = 1$. The other coefficients are equal to $\binom{p}{i+1} = \frac{p!}{(i+1)!(p-i-1)!}$ for $0 < i+1 < p$ and they are all multiples of p. Indeed, Let p appears in the prime decomposition of $p!$ but, since $i+1$, $p-i-1 < p$, it does not appear in the prime decomposition of the numerator. It follows that p is a prime factor of $\binom{p}{i+1}$ (which we know is an integer!). Moreover, the constant term is $\binom{p}{1} = p$ is not a multiple of p^2. It follows that we can apply the Eisenstein criterion and that $\Phi_p(X+1)$ is irreducible in $\mathbb{Z}[X]$.

   If $\Phi_d = AB$ where A, $B \in \mathbb{Z}[X]$, then $\Phi_d(X+1) = A(X+1)B(X+1)$, where $A(X+1)$, $B(X+1) \in \mathbb{Z}[X]$. By the previous question, we may assume that $A(X+1)$ is a unit (in particular, it is a constant polynomial). So $A = A(X+1)$ is also a unit.

Problem 2 :
Let K be a field. For all $n \in \mathbb{Z}$, let $\overline{n} = n \cdot 1_K \in K$. For all $P = \sum_{i=0}^{n} c_i X^i \in \mathbb{Z}[X]$, let $\overline{P} = \sum_{i=0}^{n} \overline{c_i} X^i \in K[X]$.

1. Show that, if $a \in K^\star$ is order n, then $\overline{\Phi}_n(a) = 0$.

   Solution: If a is order n, then we have $a^n = 1$, i.e. $\overline{P}_n(a) = 0$. If $\overline{\Phi}_d(a) = 0$ for some $d < n$, then since $\overline{\Phi}_d$ divides $\overline{P}_d$, we also have $\overline{P}_d(a) = 0$ and hence $a^d = 1$, contradicting the fact that the order of a is n. Since $\overline{P}_n = \prod_{d|n}\overline{\Phi}_d$, $\overline{\Phi}_d(a) \neq 0$ if $d < n$, $\overline{P}_n(a) = 0$ and K, being a field, is integral, we must have $\overline{\Phi}_n(a) = 0$.

2. Until the end of that problem, we will assume that $|K| = q < \infty$. Show that there are at most $\sum_{d|q-1, d<q-1}\deg(\Phi_d)$ elements in $K^\star$ which are not order $q-1$.

   Solution: The group $K^\star$ is order $q-1$. So, by Lagrange, the order of any element in $K^\star$ divides $q-1$. If the order of $a \in K^\star$ is $d < q-1$, then $\overline{\Phi}_d(a) = 0$ and since $\overline{\Phi}_d$ can have at most $\deg(\overline{\Phi}_d) = \deg(\Phi_d)$ roots, it follows that there are at most $\sum_{d|q-1, d<q-1}\deg(\Phi_d)$ elements in $K^\star$ which are not order $q-1$.

3. Show that $K^\star$ is cyclic.

   Solution: Since $P_{q-1} = \prod_{d|q-1}\Phi_d$, we have $q-1 = \deg(P_{q-1}) = \sum_{d|q-1}\deg(\Phi_d)$, so $\sum_{d|q-1, d<q-1}\deg(\Phi_d) = q-1-\deg(\Phi_{q-1}) < q-1$. It follows that there must be an element of order $q-1$ in $K^\star$ which is therefore cyclic.

Problem 3 :
Recall that $\mathbb{Z}[i]$ is the subring of $\mathbb{C}$ consisting of elements of the form $a+ib$ where a, $b \in \mathbb{Z}$. Let $p \in \mathbb{Z}$ be prime. Recall that $\mathbb{Z}[i]$ is a Euclidian domain.

1. Show that $\mathbb{Z}[X]/(p, X^2+1)$, $\mathbb{Z}[i]/(p)$ and $(\mathbb{Z}/p\mathbb{Z})[X]/(X^2+1)$ are isomorphic.

   Solution: Let $f : \mathbb{Z}[X] \to \mathbb{Z}[i]$ be the evaluation map at i (to be precise, it is the restriction to $\mathbb{Z}[X]$ of the evaluation map at i from $\mathbb{C}[X]$ into $\mathbb{C}$). Since $\mathbb{Z}[i]$ is the subring of $\mathbb{C}$ generated by $\mathbb{Z}$ and i, we do have $f(\mathbb{Z}[X]) = \mathbb{Z}[i]$. Also let π_1 be the reduction map $\mathbb{Z}[i] \to \mathbb{Z}[i]/(p)$ (we have $\pi_1(x) = x + (p)$). Then

$\theta := \pi_1 \circ f : \mathbb{Z}[X] \to \mathbb{Z}[i]/(p)$ is a ring homomorphism. Since both f and π_1 are surjective, so is θ. Let us show that the kernel of θ is (p, X^2+1). We have $f(X^2+1) = i^2+1 = 0$, so $\theta(X^2+1) = 0$. Also $\theta(p) = \pi_1(p) = 0$ so $(X^2+1, p) \subseteq \ker(\theta)$.

Conversely, pick any $P \in \mathbb{Z}[X]$ such that $\theta(P) = 0$, then $f(P) \in \ker(\pi_1) = (p)$. By the same proof as in $\mathbb{Q}[X]$, we can show that there exist Q, $R \in \mathbb{Z}[X]$ such that $P = (X^2+1)Q + R$ and $\deg(R) \leqslant 1$ (note that the dominant coefficient of X^2+1 is 1 so we never have to do any division when doing the long division). Then $f(P) = R(i)$. If $R(i) = a + ib \in (p)$, then $a + ib = p(c + id)$ and thus $a = pc$ and $b = pd$. It follows that $R = pS$ for some $S \in Z[X]$. Since $P = (X^2+1)Q + pS$, we do have that $P \in (X^2+1, p)$. By the first isomorphism theorem, we have that $\mathbb{Z}[X]/(p, X^2+1)$ is isomorphic to $\mathbb{Z}[i]/p$.

Now, let $g : \mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X]$ be the reduction map on the coefficients and $\pi_2 : (\mathbb{Z}/p\mathbb{Z})[X] \to (\mathbb{Z}/p\mathbb{Z})[X]/(X^2+1)$ be the reduction map. Then $\chi := \pi_2 \circ g : \mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X]/(X^2+1)$ is a surjective ring homomorphism. Once again, $\chi(p) = \pi_2(g(p)) = \pi_2(0) = 0$ and $\chi(X^2+1) = \pi_2(X^2+1) = 0$, so $(p, X^2+1) \subseteq \ker(\chi)$. Conversely, pick some $P \in \ker(\chi)$ and write $P = (X^2+1)Q + R$ where $\deg(R) \leqslant 1$. We have $\chi(P) = \pi_2(X^2+1)\chi(Q) + \pi_2(g(R)) = \pi_2(g(R)) = 0$. So $g(R) \in (X^2+1)$. Since $\deg(g(R)) \leqslant 1 < \deg(Xp^2+1)$, $g(R) = 0$ and every coefficient of R is divisible by p. So $R = pS$ for some $S \in \mathbb{Z}[X]$ and $P \in (X^2+1, p)$. By the first isomorphism theorem, $(\mathbb{Z}/p\mathbb{Z})[X]/(X^2+1)$ is isomorphic $\mathbb{Z}[X]/(p, X^2+1)$.

2. Assume that $p \neq 2$, show that the following are equivalent:
   a) -1 is a square in $(\mathbb{Z}/p\mathbb{Z})$;
   b) there is an element of order 4 in $(\mathbb{Z}/p\mathbb{Z})^\star$;
   c) $4|p-1$.

   Solution: If $a^2 = 1 \mod p$, then $a^4 = 1$ and since a is not order two, it is order four. So a) implies b). Conversely, if $a^4 = 1$ then $a^2 = 1$ or -1 which are the only two roots of $X^2 - 1$. But if a is order 4, then $a^2 \neq 1$ so $a^2 = -1$. We have proved that b) implies a). Finally since $(\mathbb{Z}/p\mathbb{Z})^\star$ is cyclic of order $p-1$, b) and c) are equivalent.

3. Assume that $p = xy$ for some x, $y \in \mathbb{Z}[i]$. Show that $|x|^2 \in \{1, p, p^2\}$, here $|x|$ denotes the complex norm.

   Solution: We have $|p|^2 = |x|^2|y|^2$. Also, if $x \in \mathbb{Z}[i]$, then $|x|^2 \in \mathbb{Z}$, so $|x|^2$ divides p^2 in $\mathbb{Z}$. It follows that (since it is positive) $|x|^2 \in \{1, p, p^2\}$.

4. Show that the following are equivalent:
   a) $p = 2$ or $p \equiv 1 \mod 4$;
   b) p is reducible in $\mathbb{Z}[i]$;
   c) there exist a, $b \in \mathbb{Z}$ such that $p = a^2 + b^2$.

   Solution: Since $\mathbb{Z}[i]$ is a PID, p is irreducible if and only if p is prime, if and only if p is maximal, if and only if $\mathbb{Z}[i]/p \cong (\mathbb{Z}/p\mathbb{Z})[X]/(X^2+1)$ is a field, if and only if X^2+1 is irreducible in $(\mathbb{Z}/p\mathbb{Z})[X]$, if and only if X^2+1 has no root in $\mathbb{Z}/p\mathbb{Z}$. If $p = 2$, then $1^2 + 1 \equiv 2 \equiv 0 \mod p$. If $p \neq 2$, we saw in a previous question that -1 is a square in $\mathbb{Z}/p\mathbb{Z}$ if and only if $p \equiv 1 \mod 4$. We have just proved that a) and b) are equivalent.

   Let us now assume that p is reducible in $\mathbb{Z}[X]$. Then, $p = xy$ where, by the previous question, $|x|^2 \in \{1, p, p^2\}$. If $|x|^2 = 1$, then $x\overline{x} = 1$ and x is invertible in

$\mathbb{Z}[i]$. If $|x|^2 = p^2$, then $|y|^2 = 1$ and y is invertible in $\mathbb{Z}[i]$. If both x and y are not units in $\mathbb{Z}[i]$, then $|x|^2 = a^2 + b^2 = p$ where $x = a + ib$. So b) implies c).

Finally, if $p = a^2 + b^2$ for some a, $b \in \mathbb{Z}$, then $p = (a + ib)(a - ib)$ is reducible in $\mathbb{Z}[i]$. So c) implies b).

5. (Harder) Pick any $x = \varepsilon \prod_i p_i^{\alpha_i} \in \mathbb{Z}$ where $\varepsilon \in \{-1, 1\}$, $\alpha_i \in \mathbb{Z}_{>0}$ and the p_i are distinct primes. Show that there exists a, $b \in \mathbb{Z}$ such that $x = a^2 + b^2$ if and only if for all i such that α_i is odd, $p_i \not\equiv 3 \mod 4$.

   Solution: Let $\Sigma := \{a^2 + b^2 : a, b \in \mathbb{Z}\}$. Note that $(a^2+b^2)(c^2+d^2) = |a+ib|^2|c+id|^2 = |(a+ib)(c+id)|^2 = |(ac-bd) + i(ad+bc)|^2 = (ac-bd)^2 + (ad+bc)^2$. So Σ is closed under multiplication and, to answer the question, it suffices to show which prime powers are in Σ. Even prime powers are in Σ and so is 2 and any prime $p \equiv 1 \mod 4$, by the previous question. So a prime power is not in Σ if and only if it is an odd power of some $p \equiv 3 \mod 4$.