SOLUTION OF QUIZ 3, VERSION B, MATH100B, WINTER 2021

(Thanks to Alex Mathers for providing these solutions.)

1. (5 points) Suppose p is prime. Prove that $x^{p-1} + x^{p-2} + \cdots + 1 \in \mathbb{Q}[x]$ is irreducible.

   See Example 12.2.4 in the lecture notes.

2. (5 points) Suppose every ideal of a unital commutative ring A is finitely generated. Prove that A is Noetherian.

   See Lemma 12.3.5 in the lecture notes.

3. Suppose A is a subring of B, B is a unital commutative ring, $1_B \in A$, and I is an ideal of B.
   (a) (3 points) Prove that $f : A \to B/I,\ f(a) := a + I$ is a ring homomorphism and $\ker f = I \cap A$.

   Notice that f factors as $p_I \circ i$ where $i : A \to B$ is the inclusion map and $p_I : B \to B/I$ is the natural quotient map. Because i and p_I are both homomorphisms so is their composition f. For the kernel one has

$$\ker f = f^{-1}(0) = (p_I \circ i)^{-1}(0) = i^{-1}(p_I^{-1}(0)) = i^{-1}(I) = I \cap A.$$

   (b) (5 points) Prove that if I is a prime ideal of B, then $I \cap A$ is a prime ideal of A.

   Solution 1. Notice $I \cap A$ is an ideal of A because it equals the kernel of a homomorphism, as seen in part (a). We first need to show $I \cap A$ is proper, i.e. $I \cap A \neq A$: if $I \cap A = A$ then we have $1_B \in I \cap A \subseteq I$, but then because I is an ideal of B one deduces that $I = B$, which contradicts that I is a prime ideal of B (recall again prime ideals are proper).

   For the other condition, suppose $ab \in I \cap A$ for $a, b \in A$. Then $ab \in I$ and $a, b \in B$, so from the fact that I is a prime ideal of B we deduce that either $a \in I$ or $b \in I$. But in the former case we have $a \in I \cap A$ and in the latter case we have $b \in I \cap A$.

   Solution 2. Notice the map f in part (a) is in fact a unital ring homomorphism. Because $\ker f = I \cap A$ by part (a), one has by the first isomorphism theorem an isomorphism

$$A/(I \cap A) \simeq \operatorname{Im} f$$

   where the latter is a unital subring of B/I. But B/I is an integral domain because I is prime, so $\operatorname{Im} f$ is an integral domain as well, and then so is $A/(I \cap A)$ by the above isomorphism. From this we deduce that $I \cap A$ is a prime ideal of A.

   (c) (2 points) Provide an example where I is a maximal ideal of B, but $I \cap A$ is not a maximal ideal of A.

   Take $A = \mathbb{Z}$ and $B = \mathbb{Q}$. Then $I = \{0\}$ is a maximal ideal of $\mathbb{Q}$, but $I \cap A = \{0\}$ is not a maximal ideal of $\mathbb{Z}$.

4. Suppose p is prime and $f(x) := (x^p - x + 1)^2 + p$.

(a) (5 points) Suppose $f(x) = q(x)h(x)$ for some monic non-constant polynomials $q, h \in \mathbb{Z}[x]$. Prove that there are polynomial $q_1, h_1 \in \mathbb{Z}[x]$ such that

$$q(x) = x^p - x + 1 + p\, q_1(x), \text{ and } h(x) = x^p - x + 1 + p\, h_1(x).$$

(You are allowed to use a relevant result from HW assignment after you carefully state it.)

Notice in $\mathbb{Z}_p[x]$ we get the factorization $c_p(f) = c_p(q)c_p(h)$. But on the other hand notice that $c_p(f(x)) = (x^p - x + 1)^2$; thus we have

$$(x^p - x + 1)^2 = c_p(q(x))c_p(h(x))$$

in $\mathbb{Z}_p[x]$. Also notice that $c_p(q)$ and $c_p(h)$ are monic and non-constant, as q and h are monic and non-constant by assumption. From a homework problem, we know that $x^p - x + 1$ is irreducible in $\mathbb{Z}_p[x]$, and so by unique factorization in $\mathbb{Z}_p[x]$ we must have $c_p(q(x)) = c_p(h(x)) = x^p - x + 1$. From this one gets the result, for instance we have $q(x) - (x^p - x + 1) \in \ker(c_p)$, and so $q(x) - (x^p - x + 1) = p\, q_1(x)$ for some $q_1 \in \mathbb{Z}[x]$.

(b) (3 points) Suppose q_1 and h_1 are as in the previous part. Prove that

$$(x^p - x + 1)(q_1 + h_1) \equiv 1 \pmod p$$

and discuss why this is a contradiction.

We calculate

$$\begin{aligned}
(x^p - x + 1)^2 + p = f(x) &= q(x)h(x) \\
&= (x^p - x + 1 + p\, q_1(x))(x^p - x + 1 + p\, h_1(x)) \\
&= (x^p - x + 1)^2 + p(x^p - x + 1)(q_1 + h_1) + p^2 q_1 h_1.
\end{aligned}$$

From this we deduce that $(x^p - x + 1)(q_1 + h_1) + p\, q_1 h_1 = 1$ in $\mathbb{Z}[x]$, and reducing mod p gives the result. We obtain a contradiction by comparing degrees on both sides.

(c) (2 points) Prove that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Clearly f is nonzero and a non-unit. Because f is monic (hence primitive), we know that $f(x)$ is irreducible in $\mathbb{Q}[x]$ if and only if it is irreducible in $\mathbb{Z}[x]$. Suppose we have $f(x) = q(x)h(x)$ for $q, h \in \mathbb{Z}[x]$; parts (a) and (b) together show this cannot happen for q and h non-constant. But if, say, q is constant, then comparing leading terms in $f(x) = q(x)h(x)$ shows that q is a unit. The same logic applies if h is constant, so either q or h is a unit. Thus $f(x)$ is irreducible in $\mathbb{Z}[x]$.