HOMWORK 11, ONLY FOR STUDYING, NOT FOR SUBMISSION

(The scores are assigned to the problems only for information, not for grading.)
You must prove your answer to every question.

Problem 1 (Exercise 17.7 of Shoup). (5) Show that a polynomial \( f \in F[X] \) of degree 2 or 3 over
a field \( F \) is irreducible if and only if it has no roots in \( F \).

Solution. If \( f \) has a root \( a \) then it is divisible by \( X - a \), so it is reducible. On the other hand, if \( f \)
is reducible then it has a factor of degree 1, which is of the form \( aX + b \). Then \(-b/a\) is a root of \( f \).

Problem 2. Let \( f, g \) be two polynomials in \( F[X] \) over a field \( F \).

(a) (5) Show that if \( f, g \) are relatively prime then they have no common root.

Solution. If \( f, g \) have a common root \( a \) then \( X - a \) divides both \( f \) and \( g \), hence they are not
relatively prime.

(b) (5) Show that if \( F = \mathbb{C} \) then the converse of the above statement is also true.

Solution. If \( f, g \) have a common factor \( d(X) \) then, since every polynomial in \( \mathbb{C} \) has a root,
also \( d(X) \) has a root, and this root is common in \( f \) and \( g \).

(c) (5) Show an example with \( F \neq \mathbb{C} \) where the converse is not true.

Solution. \( f(X) = X^2 + 1 \) and \( g(X) = X^2 + 1 \) in \( \mathbb{R}[X] \) are not relatively prime (they are identical),
but they have no common root since they have no root at all.

Problem 3. Let \( p(X) \) be a polynomial over the field \( F \).

(a) (5) Show that \( p(X) \) has at least one root in the ring \( F[X]/(p(X)) \).

Solution. Let \( [X] \) be the image of the polynomial \( X \) under the natural homomorphism of \( F[X] \)
onto \( F[X]/(p(X)) \): in other words, let \( [X] \) be the residue class of \( X \). Then \( p([X]) = [p(X)] = 0 \)
in \( F[X]/(p(X)) \), since \( p(X) \equiv 0 \pmod{p(X)} \).

(b) (5) Show an example when it has more than one root.

Solution. The polynomial \( X^2 + 1 \) in \( \mathbb{C} = \mathbb{R}(X)/(X^2 + 1) \) has two roots: namely \( X \) and \(-X \),
 corresponding to \( i \) and \(-i \) in \( \mathbb{C} \).

Problem 4. (10) Over the field \( \mathbb{Z}_2 \), find an irreducible polynomial \( p(X) \) of degree 3 and describe
the field \( \mathbb{Z}_2[X]/(p(X)) \), as the set of all polynomials of degree 2, giving a complete multiplication
table modulo \( p(X) \). [Hint: To find an irreducible polynomial, list first all the composite
polynomials of degree 3. The rest are the irreducible ones.]

Solution. We will list only the polynomials of degree 3 having a constant term, since the ones
without a constant term are obviously composite. These polynomials are

\[ X^3 + 1, X^3 + X + 1, X^3 + X^2 + 1, X^3 + X^2 + X + 1. \]

All composite polynomials of degree 3 with a constant term are products of polynomials of
degree 1 and 2 with a constant term. The only degree 1 polynomial with a constant term is \( X + 1 \).
The only degree 2 polynomials with a constant term are \( X^2 + 1 \) and \( X^2 + X + 1 \). Therefore the
only composite degree 3 polynomials with a constant term are \((X + 1)(X^2 + 1) = X^3 + X^2 + X + 1\)
and \((X + 1)(X^2 + X + 1) = X^3 + 1\). Therefore the irreducible degree 3 polynomials are

\[ X^3 + X + 1, X^3 + X^2 + 1. \]
Let us choose \( p(X) = X^3 + X + 1 \). Then modulo \( p(X) \) we have \( X^3 \equiv X + 1 \). The elements of the field \( \mathbb{Z}_2[X]/(p) \) can be represented by all the polynomials
\[
0, 1, X, X + 1, X^2, X^2 + 1, X^2 + X, X^2 + X + 1
\]
of degree \( \leq 2 \). The multiplication is just polynomial multiplication as long as the degree of the result is at most 2. Otherwise, reduction modulo \( X^3 + X + 1 \) gives the following rules in the new field:
\[
\begin{align*}
X \cdot X^2 &= X + 1, \\
X \cdot (X^2 + 1) &= 1, \\
X \cdot (X^2 + X) &= X^2 + X + 1, \\
X \cdot (X^2 + X + 1) &= X^2 + 1, \\
(X + 1) \cdot X^2 &= X^2 + X + 1, \\
(X + 1) \cdot (X^2 + 1) &= X^2, \\
(X + 1) \cdot (X^2 + X) &= 1, \\
(X + 1) \cdot (X^2 + X + 1) &= X, \\
X^2 \cdot X^2 &= X^2 + X, \\
X^2 \cdot (X^2 + 1) &= X, \\
X^2 \cdot (X^2 + X) &= X^2 + 1, \\
X^2 \cdot (X^2 + X + 1) &= 1, \\
(X^2 + 1) \cdot (X^2 + X + 1) &= X^2 + X, \\
(X^2 + X) \cdot (X^2 + X + 1) &= X, \\
(X^2 + X) \cdot (X^2 + X + 1) &= X^2, \\
(X^2 + X + 1) \cdot (X^2 + X + 1) &= X + 1.
\end{align*}
\]
In particular, the inverse pairs are
\[
\begin{align*}
X \cdot (X^2 + 1) &= 1, \\
(X + 1) \cdot (X^2 + X) &= 1, \\
X^2 \cdot (X^2 + X + 1) &= 1.
\end{align*}
\]

**Problem 5.** (10) In an integral domain, we will say that an element \( \sigma \) is a root of unity of degree \( n \) if there is a positive integer \( n \) with \( \sigma^n = 1 \). Let \( \sigma \) be a root of unity of degree \( n \). Show that if \( \sigma \neq 1 \) then \( \sigma + \sigma^2 + \cdots + \sigma^n = 0 \).

**Solution.** Let \( \rho = \sigma + \sigma^2 + \cdots + \sigma^n = 1 + \sigma + \sigma^2 + \cdots + \sigma^{n-1} \), then
\[
\sigma \rho = \sigma + \sigma^2 + \cdots + \sigma^{n-1} + \sigma^n = \rho,
\]
hence \( (\sigma - 1)\rho = 0 \). If \( \sigma \neq 1 \) then this implies \( \rho = 0 \) since we are in an integral domain.
Problem 6. (15) If \( z = x + yi \) is a complex number then let \( \arg(z) \) denote the angle of the vector \((x, y)\) representing \(z\), as measured counterclockwise from the \(x\) axis. For nonzero complex numbers \(u, v\) show (you can look up the proof in a textbook) that \(\arg(uv) = \arg(u) + \arg(v)\).

Solution. For a complex number \(z\) and angle \(\alpha\), let \(U_\alpha(z)\) be the vector obtained from \(z\) by turning it clockwise with angle \(\alpha\).

Let \(|z| = \sqrt{z \overline{z}}\) be the absolute value of the complex number \(z\), and let us write \(u = |u|u'\), then \(|u'| = 1\) since we have seen that the norm \(|z|^2\) (and therefore the absolute value as well) is multiplicative. So, \(uv = |u|u'v\) and therefore \(\arg(uv) = \arg(u'v)\). Let \(\alpha = \arg(u) = \arg(u')\), we will show
\[
u'z = U_\alpha(z)
\]
for all \(z\). First note that \(u'(az_1 + bz_2) = au'z_1 + bu'z_2\) for all \(z_1, z_2 \in \mathbb{C}\) and \(a, b \in \mathbb{R}\). Then note that also \(U_\alpha(z_1 + z_2) = U_\alpha(z_1) + U_\alpha(z_2)\), and \(U_\alpha(cz) = cU_\alpha(z)\) for all \(z \in \mathbb{C}\) and \(c \in \mathbb{R}\). Now, it is easy to check that \(u' \cdot 1 = u' = U_\alpha(1)\) and \(u' \cdot i = U_\alpha(i)\). From this it follows for an arbitrary \(z = a + bi\) for \(a, b \in \mathbb{R}\):
\[
u'(a + bi) = au' \cdot 1 + b \cdot u' \cdot i = aU_\alpha(1) + b \cdot U_\alpha(i) = U_\alpha(a) + U_\alpha(bi) = U_\alpha(a + bi).
\]

Problem 7. For an integral domain \(D\), let \(S = \{(a, b) : a, b \in D, b \neq 0\}\). We introduce the relation \(\sim\) over \(S\) as follows: \((a, b) \sim (a', b')\) if and only if \(ab' = a'b\). (It is convenient to think of the pairs \((a, b)\) here as formal “fractions” \(a/b\).)

(a) (5) Prove that \(\sim\) is an equivalence relation.
(b) (5) We introduce the following operations on \(S\): \((a, b) + (a', b') = (aa', bb')\), and \((a, b) + (a', b') = (ab' + a'b, bb')\). Show that if \(u \sim u'\) and \(v \sim v'\) then \(u + v \sim u' + v'\) and \(u \ast v \sim u' \ast v'\).

Denoting the equivalence class of \(u\) by \([u]\) show that this allows the definition of the operations \(+, \ast\) over the set \(K\) of equivalence classes.
(c) (5) Prove that \(K\) with these operations turns into a field. Find an injection of \(D\) into \(K\).

Solution. The solution is described in Section 17.2 of Shoup.