MATH 7210 Homework 10

Andrea Bourque

November 2021

1 Problem 1

Let p be an odd prime.

a) Show that $2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}$.

Proof. $\square$

b) Show that 2 is a quadratic residue mod p iff $p \equiv \pm 1$ mod 8.

Proof. ($\rightarrow$) Let $x^2 \equiv 2 \bmod p$. Then $1 \equiv x^{p-1} \equiv 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \bmod p$. Thus $\frac{p^2-1}{8} = 2n$ for some n, or $p^2 \equiv 1$ mod 16. This gives $p \equiv 1, 7, 9, 15$ mod 16, which implies $p \equiv \pm 1$ mod 8.

($\leftarrow$) Let $p \equiv \pm 1$ mod 8. Then $p^2 = (8n \pm 1)^2 = 64n^2 \pm 16n + 1 \equiv 1$ mod 16, so that $(-1)^{\frac{p^2-1}{8}} = 1$. Thus $2^{\frac{p-1}{2}} \equiv 1 \bmod p$. In Homework 8 Problem 4, we showed that exactly half of $1, ..., p-1$ are quadratic residues. Furthermore, any nonzero square a^2 is a solution to $x^{\frac{p-1}{2}} - 1 \equiv 0 \bmod p$. This polynomial has no more than $\frac{p-1}{2}$ roots, but all $\frac{p-1}{2}$ quadratic residues are roots. Thus, since 2 is a solution, 2 is a quadratic residue. $\square$

c) Show that -2 is a quadratic residue mod p iff $p \equiv 1, 3$ mod 8.

Proof. ($\rightarrow$) Let $x^2 \equiv -2 \bmod p$. Then $1 \equiv x^{p-1} \equiv (-1)^{\frac{p-1}{2}} 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8} + \frac{p-1}{2}}$ mod p. Then $p^2 - 1 + 4(p-1) \equiv 0$ mod 16, or $(p+2)^2 \equiv 9$ mod 16, giving $p \equiv 1, 3, 9, 11$ mod 16, which implies $p \equiv 1, 3$ mod 8.

($\leftarrow$) Let $p \equiv 1, 3$ mod 8. If $p = 8n + 1$, then $\frac{p^2-1}{8} + \frac{p-1}{2} = 4n + 8n^2 + 2n$, which is even. If $8n + 3$, then $\frac{p^2-1}{8} + \frac{p-1}{2} = 4n + 1 + 8n^2 + 6n + 1$, which is also even. Thus $(-2)^{\frac{p-1}{2}} \equiv 1 \bmod p$. As in part b, a solution to $x^{\frac{p-1}{2}} - 1 \equiv 0$ mod p is a quadratic residue, so -2 is a quadratic residue. $\square$

2 Problem 2

a) Show that if p is an odd prime congruent to 5 or 7 mod 8, then p is irreducible in $\mathbb{Z}[\sqrt{-2}]$.

Proof. Consider the norm $N(a + b\sqrt{-2}) = a^2 + 2b^2$. If $p = xy$, then $N(p) = p^2 = N(x)N(y)$, implying $N(x) \in \{1, p, p^2\}$. Suppose further than neither x nor y is a unit. Let $x = a + b\sqrt{-2}$. $N(x) = 1$ implies $a^2 = 1$, since if $b \neq 0$, $N(x) \geq 2$. Then $x = \pm 1$ is a unit, which is a contradiction. $N(x) = p^2$ implies $N(y) = 1$, meaning y is a unit, which is also against our assumption. Thus $N(x) = p$; we have $p = a^2 + 2b^2$. If b is even, then $p \equiv a^2$ mod 8. The squares mod 8 are seen to be 0 or 1, which contradicts $p \equiv 5, 7$ mod 8. Thus suppose $b = 2c+1$. $p = a^2+2(2c+1)^2 = a^2+2(4c^2+4c+1) \equiv a^2+2$ mod 8. Since the squares are either 0 or 1, $a^2 + 2$ is either 2 or 3 mod 8, which again contradicts $p \equiv$ 5,7 mod 8. We have exhausted all possibilities from the assumption that p can be factored into a product of two non-units, so p is irreducible. □

b) Show that if p is an odd prime congruent to 1 or 3 mod 8, then p splits into 2 nonassociate irreducibles in $\mathbb{Z}[\sqrt{-2}]$.

Proof. □

c) Show that a complete list of the irreducibles in $\mathbb{Z}[\sqrt{-2}]$ up to associates is given by $\sqrt{-2}$, primes p where $p \equiv 5, 7$ mod 8, and $a_p \pm b_p\sqrt{-2}$ where p is prime and 1 or 3 mod 8, with $a_p^2 + 2b_p^2 = p$.

Proof. □

3 Problem 3

a) If I is a left ideal, show that R/I is simple iff I is maximal.

Proof. ($\leftarrow$) If I is maximal, R/I is a field, and we know fields are simple.

($\rightarrow$) If J is an ideal of R containing I, then J/I is an ideal of R/I. Since R/I is simple, $J/I = 0$ or R/I. $J/I = 0$ implies $J = I$, and $J/I = R/I$ implies $J = R$. Thus I is maximal. □

b) Show that every simple module is cyclic.

Proof. Any module has submodules Rm for $m \in M$. If $m \neq 0$, then $Rm \neq 0$ as a submodule. If M is simple, this implies $Rm = M$. □

c) Given $m \in M$, show that $\phi_m : R \to M$ given by $\phi_m(r) = rm$ is an R-module map with image Rm.

Proof. For $a, r, s \in R$, we have $\phi_m(ar+s) = (ar+s)m = arm+sm = a\phi_m(r)+\phi_m(s)$, so that ϕ_m is an R-module map. The image is clearly Rm by definition; $\phi_m(r) = rm \in Rm$ for all $r \in R$ and any $x \in Rm$ is equal to $rm = \phi_m(r)$ for some r. □

d) Show that every simple R module is isomorphic to R/I for some maximal left ideal I.

Proof. From part b, we know that a simple module is cyclic, say $M = Rm$. Then from part c, we know that Rm is the image of the map ϕ_m. Then M is isomorphic to $R/\ker\phi_m$. Suppose that $\ker\phi_m$ is not maximal, so that there is an ideal J strictly between $\ker\phi_m$ and R. Then R/J is a nontrivial submodule of $R/\ker\phi_m$, contradicting the fact that $R/\ker\phi_m$, being isomorphic to M, is simple. Thus $\ker\phi_m$ is maximal, and M is isomorphic to R/I, where $I = \ker\phi_m$ is maximal. □

e) What are the simple $\mathbb{C}[X]$ modules? Can you generalize to $F[X]$ modules for an arbitrary field F?

Proof. We must identify the maximal ideals I of $\mathbb{C}[X]$. Polynomial rings over a field are PIDs, so any non-trivial ideal $I = (p)$ for a monic polynomial $p(X)$. Furthermore, $\mathbb{C}$ is algebraically closed, meaning that p factors as a product $\Pi_i(X - r_i)$ over its roots r_i. But then I is contained in $(X - r_1)$, so it is not maximal. We can then see that the ideals $(X - r)$ are the maximal ideals. $\mathbb{C}[X]/(X - r) \cong \mathbb{C}[r] = \mathbb{C}$ since $r \in \mathbb{C}$. Thus, the simple $\mathbb{C}[X]$ modules are just isomorphic to $\mathbb{C}$.

This cannot be generalized to arbitrary fields since we have used the fact that F is algebraically closed. □

4 Problem 4

If M is a simple R-module, show that $\mathrm{End}_R(M)$ is a division ring.

Proof. For $\phi \in \mathrm{End}_R(M)$, $\ker \phi$ and $\mathrm{im}\phi$ are both submodules of M, so they are either 0 or M. If $\ker \phi = 0$, then $\mathrm{im}\phi = M$, and if $\ker \phi = M$, then $\mathrm{im}\phi = 0$. Thus ϕ is either the 0 map or an isomorphism. Therefore, the non-zero elements of $\mathrm{End}_R(M)$ are invertible, so $\mathrm{End}_R(M)$ is a division ring. $\square$

5 Problem 9.5.7

Prove that the additive and multiplicative groups of a field are never isomorphic.

Proof. If F is a finite field, suppose it has N elements. Then the additive group consists of all N elements, while the multiplicative group consists of the $N-1$ nonzero elements, so they cannot be isomorphic since they have different orders.

If F is infinite with characteristic p, then every element in the additive group satisfies $px = 0$. Thus, if the multiplicative group were to be isomorphic to the additive group, every non-zero element $x \in F$ would satisfy $x^p = 1$. We note that binomial coefficients ${}_pC_k$ for $k = 1, ..., p-1$ are divisible by p, by considering the fact that the denominator $k!(p-k)!$ has no factors of p. Then $1 = (x+1)^p = x^p + 1^p = 1+1 = 2$, implying $1 = 0$, which is never true in a field. Therefore, the multiplicative group and additive group are not isomorphic.

If F is infinite with characteristic 0, then $2x = 0$ implies $x = 0$, where as $x^2 = 1$ implies $x = 1$ or $x = -1$; the multiplicative group has an element of order 2, while the additive group does not. Thus, they cannot be isomorphic. □

6 Problem 10.3.2

Assume R is commutative. Prove that $R^n \cong R^m$ iff $n = m$.

Proof. ($\leftarrow$) If $m = n$, then obviously $R^n \cong R^m$.

($\rightarrow$) First we consider Exercise 10.2.12: $R^n/IR^n \cong R/IR \times ... \times R/IR = (R/IR)^n$. It suffices to show that $IR^n = (IR)^n$. Consider the standard basis $e_1, ..., e_n$ of R^n. Then IR^n contains $Ie_i \cong I$ for each $i = 1, ..., n$. By taking linear combinations, IR^n then contains any element of $(IR)^n$. Similarly, $(IR)^n$ is also generated by n linearly independent copies of I, so $(IR)^n = IR^n$. Thus $R^n/IR^n = (R/IR)^n$.

Now we apply the exercise with I maximal. R/I is then a field, say F, and $(R/I)^n = F^n$ can be considered as an n-dimensional vector space. Thus if $R^n \cong R^m$, $F^n \cong R^n/IR^n \cong R^m/IR^m \cong F^m$. From linear algebra, isomorphic finite dimensional vector spaces have the same dimension, so $n = m$. (Hint, use I maximal). $\square$