Math 7751, Fall 2009. Solutions to the Final exam.

1. (a) Let R and S be rings with 1. Prove that every ideal of $R \times S$ has the form $I \times J$ where I is an ideal of R and J is an ideal of S.

Note: A common mistake was the wrong assumption that every subring of $R \times S$ is equal to $A \times B$ for some subrings A of R and B of S. This is false – for instance, if $R = S$, the "diagonal subring" $\{(r, r) : r \in R\}$ is not representable in the above form.

Solution: Let L be an ideal of $R\times S$. Let $\pi_1 : R\times S \to R$ and $\pi_2 : R\times S \to S$ be the projections to the first and second coordinates. Since *surjective* ring homomorphisms send ideals to ideals (for instance this follows from the lattice isomorphism theorem) and π_1 and π_2 are surjective, we get that $\pi_1(L)$ is an ideal of R and $\pi_2(L)$ is an ideal of S. It is also clear that $L \subseteq \pi_1(L) \times \pi_2(L)$.

To prove the opposite inclusion take any $(r, s) \in \pi_1(L)\times\pi_2(L)$. By definition this means that there exist $r' \in R$ and $s' \in S$ such that $(r, s') \in L$ and $(r', s) \in L$. Since L is an ideal, we have $(r, 0) = (r, s')(1, 0) \in L$ and $(0, s) = (r', s)(0, 1) \in L$, whence $(r, s) = (r, 0) + (0, s) \in L$. Hence $L = \pi_1(L) \times \pi_2(L)$.

(b) Let G and H be finite groups of relatively prime orders. Prove that every subgroup of $G \times H$ has the form $A \times B$ where A is a subgroup of G and B is a subgroup of H.

Note: The assumption that $|G|$ and $|H|$ are relatiely prime is necessary – as in part (a), if we allowed $G = H$, the diagonal subgroup would not be of the desired form.

Solution: Let C be a subgroup of $G \times H$ and $\pi_1 : G \times H \to G$ and $\pi_2 : G \times H \to H$ be the projections to the first and second coordinates. As in part (a), we are reduced to showing that $\pi_1(C) \times \pi_2(C) \subseteq C$.

Take any $(g, h) \in \pi_1(C) \times \pi_2(C)$, so that $(g, h') \in C$ and $(g', h) \in C$ for some $g' \in G$ and $h' \in H$. Let $n = |G|$ and $m = |H|$. Since n and m are relatively prime, there exist $a, b \in \mathbb{Z}$ such that $an + bm = 1$. Then the element $(g^{bm}, (h')^{bm}) = (g, h')^{bm}$ also lies in C. On the other hand, by Lagrange theorem $(h')^{bm} = ((h')^b)^m = 1$ and $g^{bm} = g^{1-an} = g$. Thus, $(g, 1) = (g^{bm}, (h')^{bm}) \in C$, and similarly $(1, h) \in C$, whence $(g, h) = (g, 1)(1, h) \in C$.

2. Let G be a group in which any two conjugate elements commute with each other, that is, x and gxg^{-1} commute for any $x, g \in G$.
(a) Prove that G has a non-trivial abelian normal subgroup (possibly equal to G).

Note: As was correctly pointed out, we need to assume that the group G is non-trivial.

Solution: Recall that for a subset S of G we denote by $\langle S \rangle$ the subgroup generated by S. We shall use the following two facts, whose proofs are straightforward:

(i) If S is a commutative subset of G, that is, $xy = yx$ for any $x, y \in S$, then $\langle S \rangle$ is abelian;

(ii) If S is invariant under conjugation in G, that is, $gSg^{-1} = S$ for any $g \in G$, then $\langle S \rangle$ is normal in G.

Now take any non-identity element $x \in G$, and let $S = \{gxg^{-1} : g \in G\}$ be the G-conjugacy class of x. Then S is invariant under conjugation by the definition of the conjugacy class and S is commutative by the assumption in the problem. Thus, by (i) and (ii) $\langle S \rangle$ is a normal abelian subgroup which is non-trivial since $1 \neq x \in \langle S \rangle$.

(b) Prove that if G is also finite, then G must be solvable.

Solution: Let us say that a group G satisfies condition (CC) if any two conjugate elements of G commute. Thus, we need to show that any finite group with (CC) is solvable. We shall prove this by induction on $|G|$.
The base case $|G| = 1$ is trivial. Take $n \geq 2$, and suppose that all groups with (CC) of order $< n$ are solvable. Let G be a group of order n with (CC). By (a) G has a non-trivial abelian normal subgroup N. Since G has (CC), it is easy to see that any quotient of G also has (CC), so in particular, G/N has (CC). Since $|G/N| < |G|$, by induction hypothesis G/N is solvable. We also know that N is abelian, hence solvable. Thus, by a theorem from Lecture 14, G must also be solvable.

3. (a) Let R be a commutative ring with 1. The *Krull dimension* of R is the largest integer $n \geq 0$ such that R has an ascending chain of *prime* ideals $P_0 \subset P_1 \subset \ldots \subset P_n \subset R$ where all inclusions are strict. Suppose that R is a PID. What are possible Krull dimensions of R? **Hint:** There are only finitely many possibilities.

Solution: As we proved in class, in a PID all *nonzero* prime ideals are maximal. Thus, a strictly ascending chain of prime ideals of R can have at most two elements: we can take $P_0 = 0$, but P_1 would already have to be maximal. Thus, the Krull dimension of R can only be equal to 0 or 1. Clearly, both 0 and 1 are possible: if R is a field, then $\{0\}$ is the only proper ideal of R, so $KdimR = 0$. If R is any PID, which is not a field, then R has a nonzero maximal ideal (recall that any commutative ring with 1 has a maximal ideal), so $KdimR = 1$.

(b) Let R be a UFD, P a nonzero prime ideal of R and $S = R/P$. Determine which of the following statements is true:

(i) S is always a PID

(ii) S may not be a PID, but it is always a UFD

(iii) S may not even be a UFD

Solution: Statement (iii) is true. Let $R = \mathbb{Z}[x]$, which is a UFD by Theorem 23.1. Let $\varphi : R \to \mathbb{R}$ be the evaluation at $\sqrt{5}$ homomorphism: $\varphi(p(x)) = p(\sqrt{5})$. Clearly, $\varphi(R) = \mathbb{Z}[\sqrt{5}]$, and thus $\mathbb{Z}[\sqrt{5}] \cong R/P$ where $P = \text{Ker}\varphi$. The ideal P is prime since $R/P \cong \mathbb{Z}[\sqrt{5}]$ is a domain, being a subring of $\mathbb{R}$. On the other hand, $\mathbb{Z}[\sqrt{5}]$ is not a UFD by Problem 4 in Homework#9.

4. (a) Prove that for any integer $n \geq 2$ the ring $\mathbb{Z}[in] \subset \mathbb{C}$ is not a PID (here i is the complex number i)

(b) Now assume that $n \geq 2$ is odd. Prove that $\mathbb{Z}[in]$ is not a UFD.

Solution: We shall show that $\mathbb{Z}[in]$ is not a UFD for any $n \geq 2$ (which of course implies both (a) and (b)) – when I was assigning this problem, I did not realise there was a short argument proving this.

Let $R = \mathbb{Z}[in]$ and $N : R \to \mathbb{Z}_{\geq 0}$ be the square of the usual complex norm, that is, $N(a + bi) = a^2 + b^2$. We claim that the element $x = in$ is irreducible in R. First, x is not a unit since $N(x) \neq 1$ and N is multiplicative. If $x = yz$ with $y, z \in R$, then at least one of the elements y or z is non-real (WOLOG y is non-real). Then $y = a + bni$ with $b \neq 0$, whence $N(y) = a^2 + b^2n^2 \geq n^2$. Hence $N(z) = N(x)/N(y) \leq 1$, so we must have $N(z) = 1$, whence $z \in \{\pm 1\}$ must be a unit. Thus, in is indeed irreducible.

Now suppose that R is a UFD, so all its irreducible elements must be prime. Since in divides $n \cdot n$ in R (as $in \cdot (-in) = n^2$) and we assume that in is prime, it follows that in divides n in R, which is of course false. The obtained contradiction shows that R is not a UFD.

5. Prove that the polynomial $f(x) = 32x^6 + 4x + 1$ is irreducible in $\mathbb{Z}[x]$.

Solution: Clearly, $f(x)$ is not a unit in $\mathbb{Z}[x]$. Suppose that $f(x) = g(x)h(x)$ with g, h non-units. Since $cont(f) = 1$, both g and h must be non-constant. Now consider the equality $f(x/2) = g(x/2)h(x/2)$. Since g and h are non-constant, it implies that $f(x/2)$ is reducible in $\mathbb{Q}[x]$, and thus $2f(x/2)$ is also reducible in $\mathbb{Q}[x]$. But by Eisenstein criterion $2f(x/2) = x^6 + 4x + 2$ is irreducible in $\mathbb{Z}[x]$ (hence by Gauss lemma irreducible in $\mathbb{Q}[x]$).
The obtained contradiction shows that $f(x)$ must be irreducible in $\mathbb{Z}[x]$.

6. Let F be a field. Prove that the additive group of F and the multiplicative group of F are not isomorphic to each other.

Solution: We shall prove that the additive group $(F, +)$ and the multiplicative group F^* cannot have the same number of elements of order 2. We consider two cases:
Case 1: char $F \neq 2$. In this case $2 \neq 0$ in F, so the equation $2x = 0$ has only one solution $x = 0$. Thus, the additive group $(F, +)$ has no elements of order 2. On the other hand, the multiplicative group F^* does have an element of order 2, namely $x = -1$ (note that $-1 \neq 1$ again because *char* $F \neq 2$).
Case 2: char $F = 2$. In this case all nonzero elements of $(F, +)$ have order 2; in particular, there is at least one such element since $|F| \geq 2$. On the other hand, F^* has no elements of order 2: indeed $x^2 = 1$ implies that $(x-1)(x+1) = 0$, so $x = \pm 1$, but in a field of characteristic two we have $-1 = 1$.
Remark: We could immediately eliminate the case $|F| < \infty$ since then F^* and $(F, +)$ are finite groups of different orders and thus cannot be isomorphic. This observation would slightly shorten the argument in Case 2.

7. A group G is called *just-infinite* if G is infinite but all its proper quotients are finite (that is, G/N is finite for any non-trivial normal subgroup N of G). Prove that every infinite finitely generated group has a just-infinite quotient. You may use the following fact without proof:

Fact 1: If G is a finitely generated group and H is a subgroup of G of finite index, then H is also finitely generated.

Solution: Let X be the set of all normal subgroups of G of *infinite index*, ordered by inclusion. We claim that X has a maximal element. By Zorn's lemma, it is enough to show that any chain in X has an upper bound in X.
So, let $\{N_\alpha\}$ be a chain in X and $N = \cup N_\alpha$. It is straightforward to show that N is a normal subgroup of G, so we only need to check that the index $[G : N]$ is infinite. Suppose not and $[G : N]$ is finite. Then by Fact 1 the group N is generated by a finite set $S = \{s_1, \ldots, s_k\}$. For each $i = 1, \ldots, k$

we have $s_i \in N_{\alpha_i}$ for some i. Since $\{N_\alpha\}$ is a chain, one of the subgroups $N_{\alpha_1}, \ldots, N_{\alpha_k}$ contains all the others; WOLOG, assume that N_{α_k} has this property. Then N_{α_k} contains all elements of S, whence $N_{\alpha_k} \supseteq \langle S \rangle = N$, and so $N_{\alpha_k} = N$. This is impossible since N_{α_k} has infinite index in G (being an element of X), while N has finite index by assumption.

Thus, we proved that X has a maximal element K. This means that K is a normal subgroup of G which has infinite index, but any normal subgroup of G which strictly contains K has finite index. By the lattice isomorphism theorem this implies that the group G/K is infinite, but any non-trivial normal subgroup of G/K has finite index. Thus, the group G/K is a just-infinite quotient of G.

Remark: It appears that we never used the assumption that G is infinite, but of course, the assertion of the problem is false for finite G. Find a place in the proof where we implicitly used the fact that G is infinite.

8. Let p and q be primes such that p is a generator of the multiplicative group $\mathbb{F}_q^*$. Prove that the cyclotomic polynomial $\Phi_q(x) = \sum_{i=0}^{q-1} x^i$ is irreducible in $\mathbb{F}_p[x]$.

Solution: The following lemma will be proved in Algebra-II, but you should try to prove it yourself (it is not difficult).

Lemma: *Let F be a field and $f(x) \in F[x]$. Then $f(x)$ is square-free, that is, $f(x)$ is not divisible by the square of a non-constant polynomial if and only if $gcd(f(x), f'(x)) = 1$.*

Now let $f(x) = x^q - 1 \in \mathbb{F}_p[x]$. Since $f'(x) = qx^{x-1}$ and $q \neq 0$ in $\mathbb{F}_p$, the polynomials f' and f are relatively prime, so f is square free.

Thus, if $f = f_1 \ldots f_k$ is a factorization of f into a product of monic irreducibles, all the factors are distinct. Furthermore, we know that one of these factors is $x - 1$; WOLOG we assume that $f_1 = x - 1$. We will show that $deg(f_i) \geq q - 1$ for some i. Since $deg(f) = q$, this would necessarily imply that $k = 2$ and $f_2 = \Phi_q$, so Φ_q is irreducible, as desired.

Now consider the ring $R = \mathbb{F}_p[x]/(x^q - 1) = \mathbb{F}_p[x]/(f_1 \ldots f_k)$. Since $f_1, \ldots, f_k$ are distinct irreducibles, by the Chinese remainder theorem we have

$$R \cong F_1 \times \ldots F_k \qquad (***)$$

where $F_i = \mathbb{F}_p[x]/(f_i)$. As we proved in class each F_i is a field of order p^{n_i} where $n_i = deg(f_i)$.

Now take the multiplicative groups of both sides of (***). It is straightforward to show that $(A \times B)^* = A^* \times B^*$, and thus

$$R^* \cong F_1^* \times \ldots \times F_k^*. \tag{!!!}$$

Note that R^* has an element of order q, namely $\bar{x}$ (the image of x in R). Indeed, $(\bar{x})^q = 1$ since $\overline{x^q - 1} = 0$ and $(\bar{x})^i \neq 1$ for $0 < i < q$.
Since q is prime, (!!!) implies that F_i^* has an element of order q for some i. Since $|F_i^*| = p^{n_i} - 1$, we deduce that $q \mid (p^{n_i} - 1)$, whence $p^{n_i} \equiv 1 \mod q$. This means that the order of p in the group $\mathbb{F}_q^*$ does not exceed n_i. On the other hand, by our assumption in the problem p is a generator of $\mathbb{F}_q^*$, whence its order is equal to $|\mathbb{F}_q^*| = q - 1$. Thus, $deg(f_i) = n_i \geq q - 1$, which finishes the proof, as explained at the beginning.